The University Of Sheffield.

OCTAs, Cyberterrorism and International Law: Exploring the Legal Landscape of Operational Cyber Terrorist Activities

By:

Claire Ar Man Yau

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

The University of Sheffield
School of Law

March 2021

DECLARATION

I, the author, confirm that the Thesis is my own work. I am aware of the University's Guidance on the Use of Unfair Means (www.sheffield.ac.uk/ssid/unfair-means). This work has not been previously been presented for an award at this, or any other, university.

ABSTRACT

The last decade has witnessed the rise of cyber terrorist groups and their exploitation of cyberspace and cyber technologies to advance their interests and pursue their agendas. In particular, these groups exploit cyberspace for the purposes of recruitment, financing and propaganda, that is, operational cyber terrorist activities (OCTAs). With this in mind, this thesis examines whether and to what extent international law applies to OCTAs. It first examines conventional law in the form of regional treaties and UN resolutions to determine whether they afford states effective protection against OCTAs.

Concluding that conventional international law offers little protection against OCTAs, this thesis examines the degree of protection afforded by the customary international law obligation upon states to prevent their territory from being used to cause harm to the legal rights of other states. While this thesis shows that the obligation to prevent transboundary harm requires states to prevent certain types of OCTAs, not all OCTAs will fall within the scope of this obligation. Therefore, this thesis concludes that while customary law can, to some extent, protect states against certain OCTAs, states need to progressively develop international law in order to put in place legal measures that can combat the threat posed by OCTAs specifically and cyber terrorism generally.

ACKNOWLEDGEMENTS

It would not have been possible to write this doctoral thesis without the help and support of several individuals. Above all, I would like to thank both my supervisors Dr. Russell Buchan and Professor Nicholas Tsagourias for their unwavering patience, guidance and commitment towards me over the last four years. They have taught me to be tenacious, resilient and confident and for that, I will always be grateful. Without their scholarly advice and direct supervision, this thesis would not have been possible.

I would like to thank my parents, Brian and May Yau who have provided endless support mentally, emotionally and financially during the course of my PhD. They taught me the meaning of hard work and never failed to encourage me to succeed. To them, I am eternally grateful, and I hope I have made you proud. I would like to thank my friends Shazmin Majid and Emma Briant, for always uplifting and inspiring me to the best that I can be. Thank you for continuously believing in me and encouraging me every step of the way, your love and support will always be remembered. I would also like to thank all my family and my friends for their unconditional love and infinite support over these last four years.

During my PhD, I have been fortunate enough to meet incredible friends who have been a critical part of this amazing journey. For that, I would first like to thank Eray Sinan Demirhan for being a brilliant friend and a wonderful mentor. I am always grateful for your intellectual insights, academic input and for proofreading my work. Another thank you is owed to Louisa McMahon who has been a constant stream of support during the PhD. Thank you for always knowing the answers, being a wonderful friend, and for sharing the stress with me. Likewise, I wish to thank Isabel Simonsen Carrascal for her continuous encouragement and reassurance. I am grateful I got to share this challenging but worthwhile experience with you both from the beginning. I am also grateful to Fiona Davies, who has been a great friend and ally during these last few years. I wish to share my gratitude for my PhD cohort from Sheffield Law School (2016-2021) for their peer support, long office lunches and for sharing the woes of being a PhD student. Without you all, this would not have been possible. Thank you for showing me that I am not alone in this journey.

Finally, I would like to offer my thanks to the University of Sheffield School of Law, which I have been a part of for the last decade. I am grateful for their financial support in funding this PhD and for giving me the opportunity to accomplish this research.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS /ACRONYMS

ARSIWA	Articles on Responsibility of States for Internationally Wrongful Acts
AU	African Union
CTC	Counter-Terrorism Committee
CTED	Counter-Terrorism Committee Executive Directorate
DRC	Democratic Republic of Congo
EU	European Union
EU IRU	European Union Internet Referral Unit
EUROPOL	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
GA	General Assembly
ICJ	International Court of Justice
ICT	Information Communication Technologies
ILA	International Law Association
ILC	International Law Commission
ISIS	Islamic State of Iraq and Syria
ISIL	Islamic State of Iraq and the Levant
ITLOS	International Tribunal on the Law of the Sea
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organisation
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
OCTAs	Operational Cyber Terrorist Activities
SC	Security Council
UN	United Nations
UN GGE	United Nations Group of Governmental Experts
UNODC	United Nations Office on Drugs and Crime
VCLT	Vienna Convention on the Law on Treaties

INTRODUCTION

I. Introduction to Research

This thesis examines whether and to what extent international law can be called upon to prevent and suppress operational cyber terrorist activities (hereinafter, referred to as 'OCTAs'), that is, the exploitation of cyberspace by terrorist groups for the purposes of recruitment, financing and propaganda. The recruitment of individuals, the training of recruits and the funding of malicious operations are activities that are essential to enabling terrorist groups to further their political and ideological goals.[1] Presented in this way, OCTAs facilitate, underpin and support the commission of violent terrorist acts and therefore jeopardise the maintenance of international peace and security, which is widely recognised as the overriding objective of the international community.[2] Critical to the suppression of OCTAs – and therefore international terrorism – is the taming influence of international law. In light of this, this research will analyse the adequacy of current international law in addressing OCTAs. This will include an examination of various regional international law regimes as well as the efforts of the United Nations and in particular, the Security Council and General Assembly in this regard. Finding these existing regimes unable to adequately suppress OCTAs, this research will assess the utility of the obligation to prevent transboundary harm in preventing OCTAs. In short, by imposing an obligation upon states to prevent harmful activities from occurring within their territory and which interfere with the legal rights of other states, this research explores the potential for the obligation to prevent transboundary harm to act as an effective legal mechanism in suppressing OCTAs.

II. Problematising the Thesis

2.1 The Threat of Non-State Actors

Traditionally, states are considered as the primary subjects of international law. This means that international legal rules apply only to states in order to govern state-to-state relations. As such, it is overwhelmingly the case that violations of international law can only be committed by states and thus, only states can be held responsible. However, when non-state actors operate among states to engage in violent activities that affect the legal rights of other states, they can trigger international conflicts

[1] This is affirmed by the Security Council in its resolutions pertaining to terrorist group ISIS and its exploitation of the internet. See United Nations Security Council Resolutions S/RES/2129 of 17 December 2013 at para 13 and 14; S/RES/2133 of 27 January 2014 at para 1 and 7; S/RES/2170 of 15 August 2014 at paras 2, 7, 9, 11 and 18; S/RES/2178 of 24 September 2014 at para 7; S/RES/2253 of 17 December 2015 at para 22; S/RES/2322 of 12 December 2016 at para 14; S/RES/2368 of 20 July 2017 at para 23.

[2] Article 1(1) of the Charter of the United Nations, 1945.

and violate international norms.[3] In other words, they can endanger international peace and security but also undermine international law. Yet, the scope for non-state actors to be held legally accountable for its actions is limited. Unless it can be shown that the state has effective control over the non-state group, by which the state is held legally responsible for those harmful acts, the non-state terrorist group exists in a vacuum which allows them to evade legal accountability.[4] As a result, establishing attribution can be challenging, particularly in cyberspace where its transient nature creates an abundance of anonymity for non-state actors operating maliciously.[5]

State-sponsored terrorism, however, is not the only threat when it comes to transborder terrorist activities.[6] Particularly since the events of 9/11, there has been an emergence of non-state terrorist groups on the international scene capable of engaging in political violence.[7] In the words of Tal Becker:

> these groups operate outside state control… they endanger human security on a global scale but offer no fixed global address towards which principles of legal accountability, reciprocity or deterrence can be directed.[8]

The proliferation of non-state terrorist groups is a rising phenomenon in the 21st century and, coupled with the advent of technology and its potential to be used for malicious purposes, poses a serious threat to international peace and security. With this in mind, the Islamic State (ISIS)[9] is a good example to demonstrate how terrorist groups can use cyber technology to further their violent objectives and endanger international peace and security but also international law.

ISIS is the most prolific terrorist group of the 21st century, notorious for its exploitation of social media. From 2014, ISIS' online presence and media strategy played a central role in its rise and dominance until its recent downfall. The volume of ISIS propaganda disseminated through the use of

---

[3] Under international law, non-state actors have traditionally been referred to as 'any actor on the international plane other than a sovereign state'. In this research, however, the use of the term 'non-state actors' refers explicitly to terrorist groups and organisations operating on the international legal scene. See for example Mary Ellen O'Connell, 'Enhancing the Status of Non-State Actors Through a Global War on Terror?', *43 Columbia Journal of Transnational Law* 435 (2004-2005). The author distinguishes between different non-state actors and identifies terrorist groups as an emerging and dominant non-state actor on the international scene.

[4] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I. C. J. reports 1986, p. 14, at p. 54 – 55. The ICJ found in Nicaragua that the acts of the Contra rebels fighting in Nicaragua were not attributable to the United States because the United States did not exercise "effective control" over the rebels.

[5] Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict and Security Law,* 21 (3), pp. 429 – 453 (2016), at p. 430 – 432.

[6] See Tal Becker, *Terrorism and the State: Rethinking the Rules of State Responsibility*, (Hart Publishing, 2006); Cedric Ryngaert, 'Non-State Actors: Carving Out a Space in a State-Centred International Legal System', *Netherlands International Law Review* 63: 183-195 (2016).

[7] See for example Michael Scharf, 'How the War Against ISIS Changed International Law', *Case Western Reserve Journal of International Law* 48 (2016); Nicolò Bussolati, "The Rise of Non-State Actors in Cyberwarfare", at p. 102, in eds. Jens David Ohlin, Kevin Govern and Claire Finkelstein, *Cyber War: Law and Ethics for Virtual Conflicts*, (OUP, 2015).

[8] Becker, supra note 6, at p. 252.

[9] The author acknowledges that there are various monikers used to refer to Islamic State including ISIL, Daesh and IS. While these terms are also correct and widely used, this research refers to Islamic State exclusively as 'ISIS', which means the Islamic State in Iraq and Syria.

Twitter, Facebook, YouTube among other social media platforms has enabled ISIS to attract millions of followers and recruit thousands of individuals worldwide. Equally, ISIS exploit social media platforms and cyberspace to engage in the illicit acquisition of funds to support their malicious activities. With this, ISIS followers are increasingly inspired and equipped with the means necessary to commit terrorist acts in and against Western states, thus posing a threat to the maintenance of international peace and security.

Since 2015, ISIS has lost much of its territories across Iraq and Syria as a result of US-led coalition offensives to recapture parts of the country.[10] Despite this, the global appeal of ISIS has continued and it has inspired many terrorist attacks in foreign cities including the suicide bombings in Paris in 2015,[11] the airport and subway attacks across Brussels in 2016,[12] and the Manchester Arena attack in 2017.[13] Notwithstanding declarations to the opposite, ISIS remains a powerful terrorist group.[14] There are fears over its resurgence following the current global pandemic of COVID-19, and reports that weakened security enforcement across the world has allowed the group to continue operations in Afghanistan, Africa, Egypt and other states.[15] ISIS is allegedly continuing to build its caliphate, which no longer concentrates on the control of territory. Instead, ISIS is reportedly exploiting the current circumstances and intensifying social media efforts to distribute propaganda and engage in the recruitment of young people who spend more time online.[16]

Given this, the reality of terrorist groups utilising cyberspace for terrorist activities poses a serious threat to international peace and security and international law, which is the core theme of this research. Absent or underinclusive of legal regulation, non-state terrorist actors will continue to exploit the lacunas in the law and operate independently or alongside states on the international

[10] BBC News Online, Islamic State and the Crisis in Iraq and Syria in Maps, March 2018. Available at https://www.bbc.co.uk/news/world-middle-east-27838034 (accessed 1 May, 2020).
[11] BBC News Online, 'Paris Attacks: What Happened on the Night', December 9, 2015. Available at https://www.bbc.co.uk/news/world-europe-34818994 (accessed May 1, 2020); Claire Phipps and Kevin Rawlinson,'Paris Attacks Kill More Than 120 People – As It Happened', *The Guardian Online*, November 14, 2015. Available at https://www.theguardian.com/world/live/2015/nov/13/shootings-reported-in-eastern-paris-live (accessed May 1, 2020).
[12] Matthew Weaver, Haroon Siddique, Raya Jalabi, and Claire Phipps, 'Brussels: Islamic State Launches Attack on Airport and Station – As It Happened', *The Guardian Online*, March 23, 2016. Available at https://www.theguardian.com/world/live/2016/mar/22/brussels-airport-explosions-live-updates (accessed 1 May 2020).
[13] BBC News Online, 'Manchester Attack: What We Know So Far', June 2, 2017. Available at https://www.bbc.co.uk/news/uk-england-manchester-40008389 (accessed May 1, 2020); Vikram Dodd et al., 'At Least 22 Killed, 59 Injured in Suicide Attack at Manchester Arena', *The Guardian*, May 23, 2017. Available at https://www.theguardian.com/uk-news/2017/may/22/manchester-arena-police-explosion-ariana-grande-concert-england (accessed May 1, 2020).
[14] Michael Safi and Martin Chulov, 'Abu Bakr al-Baghdadi Killed in US Raid, Trump Confirms', *The Guardian*, October 27, 2019. Available at https://www.theguardian.com/world/2019/oct/27/abu-bakr-al-baghdadi-isis-leader-killed-us-donald-trump (accessed May 1, 2020).
[15] Joseph Hincks, 'With the World Busy Fighting COVID-19, Could ISIS Mount A Resurgence?', *Time Online*, April 29, 2020. Available at https://time.com/5828630/isis-coronavirus/ (accessed May 1, 2020).
[16] Orla Guerin, 'ISIS in Iraq: Militants 'Getting Stronger Again', *BBC News Online*, December 23, 2019. Available at https://www.bbc.co.uk/news/world-middle-east-50850325 (accessed May 1, 2020).

scene to threaten peace and security. Accordingly, states and the international community must take measures and address this threat in order to prevent and suppress acts of cyber terrorism and to maintain international peace and security as well as international law.

2.2 Emergence of New Technologies: Cyberterrorism and OCTAs

As the evolution of ISIS has shown, modern terrorism has evolved. Today, terrorism 'tend[s] to function more as movements or social networks, than as hierarchical organisations.'[17] The advent of new technologies is largely responsible for this dynamic shift of the structural organisations of contemporary terrorism. Instead of relying on conventional rankings of a terrorist organisation where leaders dictate from above, modern terrorism consists of a matrix of members that share responsibilities in miscellaneous ways. Members utilise their individual skillsets to contribute to the operational functions of the organisation, potentially working thousands of miles away from each other on different continents. It can be said then that terrorist groups are no longer constrained to operating from bases of central command in conflict zones and forming strategies using pen and paper. New age terrorism removes the need for physical proximity of its members. Instead, operations can be carried out remotely from any location requiring only access to the internet and a device that has access to the internet.

With this in mind, modern terrorism that exploits cyber technologies has a much greater potential to further political violence and disrupt international peace and security. As such, one of the aims of this thesis is to reveal how cyberspace and cyber technologies facilitate new age terrorism, particularly because cyberspace is an arena that affords various advantages to terrorist groups. One such incentive for using cyber technology is the 'reliance on global networking and the abandoning of the physical domain in favour of the virtual domain of the Internet [which] has maximised its potential for success, while minimising the risks involved'.[18] In addition, its interconnected nature, accessibility and the anonymity it affords makes cyberspace the ideal environment for terrorist groups to conduct malicious activities.[19] Therefore, this research explores the use of cyberspace by terrorist groups to facilitate their wider terrorist objectives.

[17] Becker, supra note 6, at p. 253.
[18] Demetrius Delibasis, 'Cybersecurity and State Responsibility: Identifying a Due Diligence Standard for Prevention of Transboundary Threats', in Joanna Kulesza and Roy Balleste, ed. *Cybersecurity and Human Rights in the Age of Cyberveillance,* (Rowman & Littlefield, 2015), at p. 20.
[19] Gabriel Weimann, 'www.terror.net How Modern Terrorism Uses the Internet', *United States Institute of Peace, Special report* 116, March 2004, at p. 3.

2.3 The Prevalence of OCTAs

OCTAs are operational cyber terrorist activities, referring specifically to recruitment, financing and propaganda. They are acts of political violence that contribute towards the effective functioning of terrorist organisations and have the potential to contribute towards acts of violent terrorism. Through recruitment, terrorist groups can increase members and divide functions of the organisation allowing critical operations to be carried out. Recruits can go on to engage in terrorist conflict, train other recruits and promote terrorism.[20] Funding enables terrorist groups to carry out such activities and operations. Thus, terrorist groups source funds through donations, solicitation, exploitation of online platforms as well as other criminal activities.[21] Finally, terrorist groups rely on propaganda to share their ideological and political goals, publicise extremist views and incite violence. Propaganda is used to encourage new members to join their causes and share their beliefs.[22] As such, OCTAs are powerful tools that are essential to terrorist groups and contribute towards their effective functioning.[23]

In this research and for heuristic purposes, OCTAs are categorised into two distinct types; activities that form part of the core definition of terrorism and activities that fall within the wider definition of terrorism. In respect of the former, there are some OCTAs that are so intimately related to the final act of political violence that they are almost indistinguishable from the terrorist act itself. A prime example in this context is the incitement of terrorism. On the other hand, some OCTAs are much further removed from the final act of violence that, while they are essential for terrorist groups to engage in terrorism, they do not form part of the core definition of terrorism. An example in this regard is the recruitment of individuals through internet chat rooms or the showing of support for terrorism by sharing social media posts. As we shall see as this thesis progresses, the extent to which international law can be called upon to prevent and suppress cyberterrorism differs depending upon how closely tied the OCTA is to the final act of violent terrorism. In other words, the further removed the OCTA is from the commission of political violence, the less likely it is to fall within the regulatory purview of international law.

In light of the above, this research presents OCTAs as an area of enquiry that must be studied separately from other uses of cyberspace for terrorist purposes. This is because, while state obligations concerning cyber terrorist activities resulting physical injury and harm are well established,

[20] Shima Keene, 'Terrorism and the Internet: A Double-Edged Sword', *Journal of Money Laundering Control*, Vol. 14, Issue 4, pp. 359-370, (2011)
[21] Financial Action Task Force Report, Financing of Recruitment for Terrorist Purposes, January 2018, FATF Paris.
[22]Daniel Milton, 'Fatal Attraction: Explaining Variation in the Attractiveness of Islamic State Propaganda', *Conflict Management and Peace Science* 1 – 21 (2018).
[23] United Nations Office on Drugs and Crime (UNODC), The Use of the Internet for Terrorist Purposes, (United Nations, 2012).

international law does little to regulate the use of cyberspace for activities that are preparatory and that support the commission of terrorist violence with the possibility of resulting in physical injury and harm. Yet, terrorism remains a prevalent threat to the maintenance of international peace and security and states must be subject to rules of prevention that apply to OCTAs emanating on or from their territories because these are the activities that form the foundation to terrorist violence. In order to prevent terrorism, international legal rules must first prohibit the foundational activities that perpetuate terrorist violence, and this must begin with OCTAs. Only if and when international law is ready to impose legally binding obligations on states specifically to prevent cyber terrorist recruitment, financing and propaganda activities can this threat to international peace and security be adequately addressed.

This research distinguishes between different types of OCTAs to recognise their role within terrorism and how terrorist groups utilise cyberspace for different purposes. Whilst OCTAs are generally malicious activities that necessitate legal address, this research examines the different types of OCTAs that require prohibition under international law. In doing so, this research recognises the threat that OCTAs pose towards the achievement of international community values, that is international peace and security, and the necessary measures that must be taken to prevent and suppress such activities. Accordingly, this research explores the prevention and suppression of OCTAs under international law.

III. Primary Research Question and Subsidiary Research Questions

As said, the purpose of this thesis is to analyse the prevention and suppression of operational cyber terrorist activities under international law. This thesis will seek to answer the following research question: How does international law apply to OCTAs? In order to answer this question, this thesis presents OCTAs as a threat to international peace and security; examines existing treaties and UN outputs that try to prevent or suppress OCTAs and then investigates the duty of states to prevent and suppress OCTAs as a matter of customary international law according to the obligation to prevent transboundary harm. As such, the following subsidiary research questions have been formulated:

i) What are OCTAs, how do they relate to terrorism and how do they impact upon the maintenance of international peace and security?
ii) How does conventional international law apply to OCTAs, namely, treaty regimes such as the UN Charter and the Budapest Convention?
iii) Does the obligation to prevent transboundary harm apply in cyberspace? How does the standard of due diligence condition the obligation to prevent transboundary harm? To

what extent can the obligation to prevent transboundary harm prevent and suppress OCTAs under international law?

In addressing the first subsidiary research question, this research aims to draw attention to the most prevalent forms of OCTAs. As will be discussed in Chapter 1, this research examines only cyber terrorist recruitment, financing and propaganda. The purpose of coining the term OCTAs is to abbreviate and shorten the understanding of specific cyber activities that are core to terrorist groups. This is in part because the Security Council and General Assembly identify recruitment, financing and propaganda as the most prevalent terrorist activities.[24] This said, there is scope to contend that OCTAs should incorporate other activities such as incitement, radicalisation, training, planning, and supporting of terrorist acts in cyberspace given that the Security Council and the General Assembly have also referred to such activities in resolutions and meetings.[25] The interconnected nature of terrorism means a broad interpretation of OCTAs can in fact encompass other activities. For example, training and radicalising of individuals cannot be done without the recruitment of members. The planning of terrorist acts is not possible without the supply of funds to acquire equipment, materials or weapons. Similarly, supporting or inciting terrorism is enabled through the use of propaganda. While OCTAs can extend to include activities beyond that of recruitment, financing and propaganda, this thesis focuses on these three core activities because they are central to the functioning of terrorist groups.

Chapter 2 contextualises the thesis by providing a theoretical chapter which presents OCTAs and terrorism as a threat to international peace and security. The discussion aims to bring attention to a principal theory of peace and to determine whether and how OCTAs affect the achievement of peace. By exploring the impact of OCTAs on the maintenance of international peace and security, the thesis determines the need for OCTAs to be subject to rules of international law.

As was said, this thesis intends to address the prevention of OCTAs in depth as a matter of public international law. Accordingly, one of the subsidiary research questions of this thesis is to examine how existing legal frameworks of international law apply to OCTAs. In order to do this, the research aims to examine regional treaties and UN resolutions to determine the applicability of international law in the prevention and suppression of OCTAs. The objective of Chapter 3 is to examine three

[24] E.g. S/RES/2322 of 12 December 2016; A/RES/72/284 The United Nations Global Counter-Terrorism Strategy Review of 2 July 2018. See Chapter Four.

[25] United Nations Security Council Resolution 1373, S/RES/1373 of 28 September 2001; United Nations Security Council Resolution 2178, S/RES/2178 of 24 September 2014; United Nations Security Council Resolution 2253, S/RES/2253 of 17 December 2015; United Nations General Assembly Resolution 68/276, A/RES/68/276 of 24 June 2014; United Nations General Assembly Resolution 72/194, A/RES/72/194 of 23 January 2018; United Nations Security Council, United Nations Security Council 7587th Meeting, S/PV.7587 of 17 December 2015; United Nations Security Council, United Nations Security Council 8560th Meeting, S/PV.8460 of Feb. 11, 2019.

regional treaties relating to cyber offences and cyber security; the Convention on Cybercrime (2010),[26] the Arab Convention (2010)[27] and the African Union Convention (2014)[28] to determine their applicability to OCTAs. The analysis of these treaties intends to discover whether there are provisions that can be interpreted to have application to cyber terrorist recruitment, financing or propaganda activities. The chapter intends to bring to light the current landscape of international law and to understand how it deals with OCTAs. In order to deduce whether there is applicable international law, an exposition of current provisions contained in regional treaties is a good place to start. Therefore, this chapter makes in depth analysis on the meaning of the rules and whether they can be construed to have application to OCTAs.

Note, however, that there are three other regional treaties that were omitted from the analysis: Shanghai Cooperation Organisation Agreement (2009),[29] The Organisation of American States (OAS) Comprehensive Inter-American Cybersecurity Strategy (2004)[30] and The Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information (CIS Agreement) (2001).[31] Despite the fact they concern information security and terrorism, the discussion and analysis does not consider these three regional conventions due to the focus of the thesis and time constraints. This chapter intends to examine a set of regional treaties that are reflective of the current status of international law as far as it concerns cyberspace and terrorism. As such, this thesis engages with the most pertinent treaties concerning the regulation of OCTAs under international law.

This analysis continues into Chapter 4, where the objective of this chapter is to evaluate UN outputs and to determine whether they can be applied to OCTAs. As the primary organs responsible for international peace and security, the Security Council and the General Assembly are principal to the discussion of counter-terrorism and to assess whether OCTAs can be found within its resolutions, meetings and other related documents. Therefore, this chapter seeks to review resolutions pertaining to terrorism and to discuss whether the wording of particular provisions can be interpreted to have application to OCTAs. This involves an analysis into the semantic use of certain words and the connotation of specific expressions that can shape the way a resolution impacts on the legal duties of states. This chapter thus intends to show how the Security Council deals with OCTAs through legal

[26] Council of Europe, Convention on Cybercrime, ETS No. 185 (November 23, 2001).
[27] The Arab Convention on Combating Information Technology Offences (2010).
[28] The African Union Convention on Cybersecurity and Personal Data Protection (2014).
[29] The Shanghai Cooperation Organisation Agreement (2009).
[30] The Organisation of American States (OAS) Comprehensive Inter-American Cybersecurity Strategy (2004).
[31] The Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information (CIS Agreement) (2001).

instruments and the significance of language in the determination of legal responsibilities as it relates to UN resolutions.

As regards the final subsidiary research question concerning the obligation to prevent transboundary harm, this thesis turns to customary international law to determine whether this legal framework is capable of preventing and suppressing OCTAs. The purpose of Chapters 5 and 6 is to set out the nature and scope of the obligation to prevent transboundary harm in cyberspace and to apply this principle to OCTAs. In doing so, this thesis shines a light on customary international law and its utility in the prevention and suppression of OCTAs. In light of the paucity of relevant treaty law, customary law is well equipped to deal with OCTAs as a contemporary issue. State practice underpins the development of customary international law and is expected to develop as it addresses the issue of OCTAs. Therefore, the aim of these chapters is to determine whether customary law can offer a tentative solution to the problem of OCTAs.

To a certain extent, OCTAs have been left to individual states to deal with under national laws. In turn, this research aims to present OCTAs as an international problem because they routinely implicate multiple states and jeopardise their international legal rights. The harm suffered by one state often originates from malicious acts emanating from the territory of another state, and on certain occasions, may also involve a third state. Thus, Chapter 6 in particular, intends to demonstrate whether and to what extent the obligation to prevent transboundary harm can be used to deal with OCTAs by triggering state responsibility when it comes to transboundary cyber harm. This chapter aims to bring attention to the use of an existing legal framework of international law to deal with a contemporary problem of terrorism. In doing so, this thesis hopes to determine the applicability of international law to OCTAs.

IV. Originality

This thesis addresses the issue of operational cyber terrorist activities, state responsibility and the obligation to prevent transboundary harm in international law. In particular, this thesis focuses on OCTAs that do not rise to the level of force, an area of research that has not attracted much attention from the international legal community and is a distinct emerging legal issue. This thesis focuses on issues related to legal obligations of states in relation to OCTAs under international law. The originality of this research lies in utilising the customary obligation to prevent transboundary harm to prevent and suppress OCTAs under international law. There have been very limited attempts to integrate the obligation to prevent transboundary harm within the context of cyberterrorism to provide a regulatory framework for the prevention of OCTAs. In other words, the thesis provides a different legal

framework according to which OCTAs can be assessed, underlining the contribution and originality of this research.

Among the literature surrounding cyberterrorism and international law, there has been limited commentary on OCTAs under international law which is something that this thesis addresses. The ILA Study Group on Cybersecurity, Terrorism and International Law (2016) focuses on international legal issues surrounding the use of cyberspace for violent terrorist attacks.[32] The report makes insightful analysis on how international law responds to cyberterrorism through treaties and the Security Council's mandate on peace and security. The report explicitly recognises that there is a need to undertake further legal research examining how international law deals with terrorists' use of cyberspace for terrorist activities and for purposes other than cyber-attacks.[33] This is particularly interesting because the report acknowledges the use of cyberspace for OCTAs as a prevalent issue that deserves commentary exclusively as a study of its own.

To add to this, in his article 'Cyberspace, Terrorism and International Law' (2016), David Fidler writes about OCTAs as well as violent cyber terrorist attacks and highlights the paradox as it concerns their regulation under international law.[34] OCTAs, while an abundant issue described as a 'crisis', nevertheless lacks 'credible options' for international legal action.[35] In contrast, there are 'plausible options' regarding the regulation of cyber terrorist attacks, despite the fact these attacks have not yet occurred. Fidler therefore draws attention to this dichotomy and underlines the need for counterterrorism in cyberspace to 'focus on the root causes of this problem', that is, tackling OCTAs.[36] Therefore, it seems that prevailing literature does not concern OCTAs but instead, prioritises discussion of cyber terrorist attacks despite the scarcity of the latter.

Likewise, Heather Harrison Dinniss, in her article 'The Threat of Cyberterrorism and What International Law Should (Try to) Do About It' (2017),[37] recognises that ISIS has made 'great strides in utilizing information and communication technologies (ICTs) for encrypted communications, recruitment, propaganda and fundraising'.[38] Though, Dinniss pertinently points out that there lacks an international framework for states to address acts of cyber terrorism, the analysis does not elaborate

[32] International Law Association (ILA), Study Group on Cybersecurity, Terrorism and International Law, Study Group Report (July 31, 2016).
[33] Ibid, at p. 8. The report states that 'it recommends the ILA establish another study group to focus on the international legal issues associated with terrorist use of ICTs and the Internet for purposes other than cyber-attacks.'
[34] David Fidler, 'Cyberspace, Terrorism and International Law', *Journal of Conflict & Security Law,* Vol. 21, No.3, 475-493, (2016).
[35] Ibid, at p. 493.
[36] Ibid.
[37] Heather A. Harrison Dinniss, 'The Threat of Cyber Terrorism and What International Law Should (Try To) Do About It', *Georgetown Journal of International Affairs,* Vol. 19 (Fall 2018), pp. 43 – 50.
[38] Ibid, at p. 43.

on the regulation of OCTAs or their status under international law despite their significance to cyberterrorism. Instead, the primary focus of this analysis concerns violent cyber terrorist attacks and even discussion on the state involvement of such attacks by reference to the 2010 Stuxnet malware attack. From these studies, it can be said that there is little commentary on the regulation of OCTAs under international law.

There is some commentary on general issues of non-state actors under the obligation to prevent transboundary harm and due diligence. Another ILA Study Group on Due Diligence in International Law (2016) discusses due diligence and its applicability to different areas of international law.[39] This report examines due diligence as a standard of conduct and the obligations attached to this duty, providing some insight into how due diligence can be applied in the context of cyberspace. The Study Group report does not, however, mention OCTAs or cyberterrorism as it relates to the duties of states under the due diligence standard.

In Christopher E. Lentz's article on 'A State's Duty to Prevent and Respond to Cyberterrorist Acts' (2010), he emphasizes the role of the state in the prevention of cyberterrorism and refers in particular to the obligations set forth in Security Council Resolution 1373 (2001).[40] While this article alludes to terrorist financing as it appears in Resolution 1373, it considers only violent attacks as necessary of prevention when it comes to violent acts of cyberterrorism. Similarly, in his article titled 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016),[41] Russell Buchan made analysis exploring the content of the obligation and its application to non-state actors in cyberspace. Nonetheless, Buchan's work focuses on destructive transboundary harm that resembles cyberattacks and does not address the issue of cyber terrorism or OCTAs.

Furthermore, Irene Couzigou's paper on 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations' (2018) is useful for analysis concerning the obligation to prevent transboundary harm and how it applies to cyberspace and cyber operations.[42] In her discussion, Couzigou comments on state responsibility over the acts of terrorist groups launching transboundary cyber operations from the territory under its exclusive control and considers how rules of international law apply in light of such terrorist acts.[43] Like many other studies, however, Couzigou's

[39] Tim Stephens and Duncan French, 'ILA Study Group on Due Diligence in International Law', *International Law Association,* Second Report, (July 2016).
[40] Christopher E. Lentz, 'A Study's Duty to Prevent and Respond to Cyberterrorist Acts', *Chicago Journal of International Law,* Vol. 10, No.2, (2010).
[41] Buchan, supra note 5.
[42] Irene Couzigou, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations', *International Review of Law, Computers & Technology*, 32:1, 37 – 57.
[43] Ibid, at p. 46. On discussing the obligation for a state to act in response to transboundary cyber harm, Couzigou identifies knowledge as a trigger to the obligation to prevent transboundary harm and that states are bound by this obligation where the harm emanates from or transits through territory under its exclusive control. She hypothesizes that 'such would be the

work centres around violent cyber-attacks. The discussion does not extend its focus to OCTAs that do not reach a sufficiently high threshold of harm but instead, concentrates on cyber conduct that causes serious or significant harm.

These legal studies shed light on the general area of the obligation to prevent transboundary harm and are useful to inform the general discussion. However, commentary on the customary obligation to prevent transboundary harm as it concerns OCTAs is very limited and what exists lacks analytical depth. It can thus be said with reason that current international legal literature has not explicitly focused on terrorist groups exploiting cyberspace for the specific purposes of recruitment, financing and propaganda activities and on how international law can address this issue of OCTAs. To add to this, counter-terrorism mechanisms have been more focused on internal policies and increasing national security, rather than on the behaviour of states and their role in suppressing OCTAs below the level of force.[44]

Still, Ben Saul and Kathleen Heath recognise that states 'bear a long-standing, general international law obligation to diligently prevent and repress terrorist activities emanating from their territory and directed towards harming other states'.[45] Despite this, there has not yet been any academic literature that has engaged specifically with the legality of OCTAs, state responsibility for OCTAs and how the relationship between the two should be addressed under international law. Equally, there seems to be no comprehensive analysis on the implications of OCTAs at an international scale and how this issue can be addressed by rules of international law. In light of this, this thesis intends to fill these gaps identified in the literature.

With this in mind, this thesis makes an original, significant and important contribution to the academic literature for the following reasons. First, this thesis reconceptualises how OCTAs endanger international peace and security by discussing cyberterrorism as OCTAs under international law. The thesis identifies two types of OCTAs and shows how terrorist groups exploit cyberspace for terrorism. Second, this thesis reconsiders how international law can be interpreted to apply to OCTAs through the analysis of regional treaties, UN resolutions and customary international law. Third, this thesis reinterprets the obligation to prevent transboundary harm by applying it to a new area of cyberspace and specifically cyberterrorism. Fourth, this thesis re-evaluates the utility of due diligence as a

case if the intelligence services of a State were to discover that a terrorist organisation had installed destructive malware in the gas pipeline control system of another State that it is about to activate'.

[44] See for example UK National Cyber Security Strategy 2016-2021 which lays out a policy guideline for the government to adopt in order to defend the state against cyber threats. The policy distinguishes between terrorist use of the Internet and cyber terrorism, considering the latter as an attack. The threats that are warned of in the policy refer to cyber-attacks against the critical national infrastructure. The policy does not address OCTA's specifically, if at all.

[45] Ben Saul and Kathleen Heath, "Cyber Terrorism", in eds., Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace*, (Edward Elgar, 2015), at p. 148.

standard conditioning the obligation to prevent transboundary harm regarding OCTAs. By examining the tenets of the due diligence and assessing elements including knowledge and material capacity, the thesis aims to provide new knowledge on the application of due diligence to OCTAs, establishing a legal trajectory to prevent and suppress acts of cyberterrorism.

V. Methodology

This thesis employs a legal doctrinal method of research in order to achieve the intended research aims and objectives. Doctrinal research involves the combination of a range of different techniques serving three main purposes: to describe, to prescribe and to justify.[46] Therefore, this thesis will begin by presenting the law to determine its relevancy to OCTAs. Since legal doctrine seeks to explore 'legal precedent and legislative interpretation',[47] this research intends to make substantive evaluations of existing legal apparatuses to evaluate whether international law is currently equipped to deter OCTAs. This will involve the review of primary sources of law including international and regional treaties on cyber technology and terrorism. Analysis will also include documents from the United Nations, analysing resolutions from the Security Council and the General Assembly. This will lead to a 'systematic exposition'[48] of legal rules which is necessary to determine the applicability of current international law to OCTAs.

Upon analysing the relationship between these rules, and 'with a view to solving…gaps in the existing law',[49] the research then prescribes the use of an existing principle of international law but to a new set of facts. It will present the customary obligation to prevent transboundary harm as a pragmatic solution to the legal problem, justifying the utility of this legal mechanism. Legal rules have been described as 'normative in character', reflecting the way in which subjects of the law should act or behave.[50] In light of this, this research intends to prescribe the law and articulate how the law should apply as it concerns the prevention of OCTAs and cyberterrorism. The research therefore places the legal system at the subject of inquiry, providing the normative framework for analysis. In doing so,

[46] Jan Smits, 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research', *M-EPLI Working Paper*, No. 2015/06, (Sept. 2015) at p. 8
[47] Terry Hutchinson, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law', *Erasmus Law Review* Vol. 8 No.3, (Dec 2015) at p. 131
[48] Dennis Pearce, Enid Campbell and Don Harding, 'Categorizing Legal Research', *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission,* (1987).
[49] Smits, supra note 45, at p. 5
[50] Paul Chynoweth, 'Legal Research', in ed. Andrew Knight and Les Ruddock, *Advanced Research Methods in the Built Environment*, (Wiley-Blackwell, 2008) at p. 30. The author explains a feature of doctrinal research which posits 'how individuals ought to behave' in accordance with the law.

the research adopts an 'internal perspective'[51] to make assumptions about the law, and subsequently provides an alternative measure in response to the outcome reached from the analysis of the law.

Using a doctrinal method of research thus enables the exploration of legal rules and principles of international law and to determine how they apply to OCTAs. As such, the doctrinal method is essential to answering the central research question of 'How does international law apply to OCTAs' and to achieving the subsidiary research aims and objectives of this thesis.

VI. Thesis Overview

Chapter 1 is a definitional chapter providing a discussion of the meaning of terrorism, cyberterrorism and OCTAs. Since there is no formal definition of terrorism under international law, the chapter begins by identifying the common characteristics of international terrorism. The chapter explains why OCTAs form part of the definition of cyberterrorism. This discussion is important, as the current interpretation of cyber terrorist recruitment, financing and propaganda hinders its legal address under international law. Terrorist groups primarily use cyberspace for the purposes of conducting OCTAs, and the prevalence of OCTAs are far greater than the use of cyberspace for terrorist attacks. As such, this research assesses how international law addresses OCTAs and identifies a gap in the law that necessitates legal attention. Chapter 1 finishes by exploring each individual OCTA, identifying the features of each terrorist activity and delineating a working definition of each in order to establish the scope of the research.

Chapter 2 contextualises the research and provides it with a theoretical background. In particular, this chapter situates OCTAs within the framework of international peace and security. The chapter explores the theory of international peace and security, specifically through Johan Galtung's theory of peace, which embodies both a negative and positive concept. The chapter emphasizes the importance and the role of international law in maintaining international peace and security. It then discusses the nature and evolution of terrorism and emphasizes the threat of terrorism against both concepts of peace. Chapter 2 then assesses the impact of OCTAs on international peace and security and does so through the theoretical lens of Galtung's theory of peace.

Chapter 3 discusses international and regional treaty law relating to cyber technology and counterterrorism and examines whether these instruments can be interpreted to apply to OCTAs. In order to determine whether current international law is effective in deterrence against OCTAs, Chapter 3 is significant because it evaluates existing legislation to determine the adequacy of

[51] Ibid.

international law as it stands. Three regional treaties are subject to examination according to the general rule of interpretation under Article 31(1) VCLT 1969: the Convention on Cybercrime (2010), the African Union Convention on Cybersecurity and Personal Data Protection (2014) and the Arab Convention on Combating Information Technology Offences (2010). The chapter examines each OCTA within the context of each convention and its supplementary documents and evaluates the utility of current legislation using reported cases of cyberterrorism as a means of analysis. This chapter demonstrates that whilst there are varying degrees of relevant application of regional treaties to deter OCTAs, the conventions are constrained by regional limitations or the provisions are reserved for cyber terrorist acts that produce sufficiently severe consequences amounting to cyber-attacks. Chapter 3 emphasizes the further need for rules of international law to address OCTAs.

Chapter 4 continues with the discussion regarding applicable international law to OCTAs by examining the United Nations collective security system through counter-terrorism resolutions of both the Security Council and the General Assembly. This chapter serves to demonstrate the role of the Security Council and the General Assembly in addressing matters of international terrorism and the enforcement of peace and security in relation to terrorism. Chapter 4 distinguishes between the Security Council's use of executive and legislative resolutions as well as interpreting its use of binding and non-binding language through using the general rule of interpretation enshrined in Article 31(1) VCLT 1969. This issue is discussed in depth to demonstrate to the reader how the Security Council chooses to address matters of international terrorism that concern OCTAs, revealing a lack of binding obligations that specifically prevent cyber terrorist recruitment, financing and propaganda activities. This chapter builds on the discussion in Chapter 3 to emphasize that the UN's collective security system places greater importance on preventing cyber terrorist attacks that are rare and sporadic rather than suppressing OCTAs that are prolific and routine. In addition, this chapter stresses the significance of states to steer the fight against terrorism and the need for compelling norms of international law to impose upon them obligations in order to prevent OCTAs.

Chapter 5 explores the tenets of the customary obligation to prevent transboundary harm conditioned by the standard of due diligence. The chapter first begins by exploring the legal status of the obligation and its formation through custom, identifying the core concept as the state's obligation not to allow knowingly its territory to be used for acts injurious to the rights of other states. Chapter 5 demonstrates to the reader that such obligation has application in cyberspace, and thus applies to cyber activities. The chapter explores the content of the obligation, identifying that only those activities that are internationally wrongful and give rise to sufficiently serious consequences for the legal rights of the victim state, are subject to the obligation to prevent transboundary harm. The

chapter then discusses the standard of due diligence as the criterion used to assess the state's performance of its customary obligations, examining issues including the state's knowledge and technical capacity as well as other factors affecting the performance of its obligations include the effectiveness of state control, the likelihood of harm and the importance of the interest requiring protection. This discussion regarding the different factors to trigger obligations demonstrates the flexibility of the due diligence standard when imposing duties on the state to prevent harmful activities. Finally, the chapter discusses the specific duties of prevention that states must take in the face of transboundary harm and applies them in the context of cyberspace to demonstrate additional means of holding states responsible for harmful activities in cyberspace.

Chapter 6 develops the discussion by applying the customary obligation to prevent transboundary harm to OCTAs. The chapter presents OCTAs as harmful activities that interfere with the legal rights of other states, having the potential to violate rules of international law. This chapter stipulates that where a terrorist group launches an OCTA, that if committed by a state would amount to an internationally wrongful act and where that OCTA gives rise to sufficiently serious consequences, the state must prevent the OCTA in question. As such, this chapter argues that states are under a legal obligation to engage in specific measures to prevent and suppress OCTAs once they learn of such harm emanating on or from its cyber territories. This chapter is important because it demonstrates that customary international law of state responsibility may adapt and respond to emerging cyberterrorism and reiterates the role of the state in suppressing OCTAs as a means of combating terrorism and maintaining international peace and security.

Finally, the conclusion provides a summary of the research. The conclusion outlines the key findings of the thesis and discusses the contributions made to the field of cyberterrorism and international law. Lastly, this thesis will make recommendations for areas of future research as it relates to OCTAs and international law.

Chapter One

DEFINING TERRORISM, CYBERTERRORISM AND OCTAS

I. Introduction

Cyberterrorism has become a prominent threat during the 21st century with terrorist groups such as ISIS increasingly exploiting cyberspace to engage in terrorist acts and OCTAs, that is, cyber terrorist recruitment, financing and propaganda. OCTAs are essential to the effective functioning of terrorist groups by enabling them to pursue their political objectives. Given this, OCTAs must be subject to prevention and suppression in order to fight against global terrorism and maintain international peace and security.

This chapter explores the definition of cyberterrorism and OCTAs and in doing so frames the research scope of the thesis. Section II examines the definition of terrorism, whereas Section III explores the definition of cyberterrorism and identifies the conceptual and legal difficulties that this definition encounters. Section IV presents OCTAs as an integral part of cyberterrorism. Section V identifies different types of OCTAs and explores their defining features. Finally, Section VI offers concluding thoughts.

II. Defining International Terrorism

The problem of defining terrorism under international law has been a source of controversy for many years because the international community has not been cohesive in its interpretation of terrorism. Differing national agendas in a decentralised community have led to diversity when it comes to defining terrorism. Generally, international law has concerned itself directly with the modus operandi of terrorism whilst circumventing the need for a more general definition. On account of this, there is no single and uniform definition in international law but instead, particular acts such as hijacking, the taking of hostages and suppressing terrorist bombings and so forth have been outlawed by international conventions.

While there is no specific definition of terrorism, certain approaches to terrorism will nevertheless be considered because they are necessary and helpful to understanding OCTAs and their legal treatment. According to Rosalyn Higgins, 'terrorism is a term without legal significance' and is 'merely a convenient way of alluding to activities, whether of states or of individuals, widely disapproved of and in which either the methods used are unlawful, or the targets protected, or both'.[1] For her, a

[1] Rosalyn Higgins, 'The General International Law of Terrorism', in Rosalyn Higgins and Maurice Flory, *International Law and Terrorism* (London Routledge, 1997) 13 (28).

general definition of terrorism does not assist in our understanding of the term, particularly because those acts commonly referred to as terrorism 'would most likely be prohibited by other international legal norms'.[2] In other words, terrorism is widely understood through the common elements that form its various definitions across a multitude of legal instruments. Thus, in the words of Helen Duffy, 'the absence of a generic definition of terrorism leaves no gaping hole in the international legal order'.[3]

On the other hand, some scholars have contended that 'a common definition is necessary and indispensable to any serious attempt to combat terrorism'[4] and that in the absence of this, 'the struggle over the representation of a violent act is a struggle over its legitimacy'.[5] The view that terrorism should be understood universally and legally is one that has carried some weight when it comes to defining the concept and what it means in precise terms. In light of increasing international terrorism and especially the events of 9/11 and the emergence of ISIS, the international community has started to craft a more general definition of international terrorism that broadens its scope beyond the use of weapons to commit political violence.

There are a number of international instruments that regulate terrorism. The United Nations has made a significant contribution to the debate on international terrorism. Whilst the UN has not provided a definition of terrorism, both the Security Council and the General Assembly have recognised the type of activities that are terrorist in nature. In 1994, under Resolution 49/60, the General Assembly adopted a Declaration on Measures to Eliminate International Terrorism, where a number of armed activities were considered acts of terrorism. The General Assembly specifically condemned:

> Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstances unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.[6]

Under this resolution, the General Assembly also condemned 'all acts, methods and practices of terrorism' irrespective of 'wherever and by whoever committed'.[7] By stipulating that these criminal acts are 'unjustifiable', this interpretation makes explicit reference to certain criminal acts as acts of terrorism that do not differentiate between state sponsored terrorism and terrorism perpetrated by national liberation movements during the 1990s. Similarly, in 1999 the International Convention for

[2] Ibid.
[3] Helen Duffy, *The 'War on Terror' and the Framework of International Law* (Cambridge University Press, 2005), at p. 44.
[4] Gerhard Hafner, "The Definition of the Crime of Terrorism", in Nesi, G., ed, *International Cooperation in Counter-Terrorism: The United Nations and Regional Organisations in the Fight Against Terrorism* (Ashgate, 2006), at p. 33.
[5] Ben Saul, *Defining Terrorism in International Law* (Oxford University Press, 2006), at p. 3.
[6] United Nations General Assembly A/RES/49/60 of 17 February 1995, para 3.
[7] Ibid.

the Suppression of the Financing of Terrorism made no reference to state terrorism or the possible perpetrators of terrorism. Thus, international instruments have emphasised that there is no difference between state terrorism or any other forms of it but instead, recognise that all forms of terrorism must be condemned by international law.

As one of the first attempts to draft a general definition of terrorism, the Convention defined terrorism as:

> any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in hostilities in a situation of armed conflict, when the purpose of such an act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.[8]

As part of measures in response to the events of 11 September 2001, another attempt of a general definition of terrorism was provided by the General Assembly Ad Hoc Committee on Terrorism. Article 2(1) of the Draft Comprehensive Convention on International Terrorism stipulates that:

> (1) Any person commits an offence within the meaning of this Convention if that person, by any means, unlawfully and intentionally, causes:
> (a) Death or serious bodily injury to any person; or
> (b) Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure, facility or the environment; or
> (c) Damage to property, places, facilities, or systems referred to in paragraph 1(b) of this article, resulting or likely to result in major economic loss, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing an act.[9]

Though the Convention remains in draft form, the definition of terrorism shares similar common elements to that found in the definition of both the General Assembly and the International Convention mentioned above.

Further efforts to define terrorism are equally provided by the Security Council. In particular, after the events of 9/11 the Security Council adopted various resolutions condemning 'any act', 'all acts' and 'all forms' of terrorism.[10] One of the closest definitions of terrorism has been provided by the Security Council in Resolution 1566 (2004). The Security Council characterises international terrorism by condemning:

> criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or

[8] International Convention for the Suppression of the Financing of Terrorism opened for signature 9 December 1999, 2178 ILM 229 (entered into force 10 April 2002), Article 2 (1)(b).
[9] United Nations General Assembly, Letter dated 3 August 2005 from the Chairman of the Sixth Committee addressed to the President of the General Assembly A/59/894 (12 August 2005), Appendix II, Article 2 (1).
[10] United Nations Security Council Resolution 1516 (2003) para 1; Resolution 1530 (2004) para 1; Resolution 1515 (2003), preamble; Resolution 1516 (2003) para 4; Resolution 1526 (2004), preamble; and Resolution 1530 (2004) para 4.

> in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.[11]

From this definition, there are certain components that have been recognised as integral to an act of terrorism. In this way, the Security Council does not only consider what consequences must flow from an act in order to qualify as terrorism, but also focuses upon the object, nature and purpose of the act.

An equally important definition of terrorism is made by the Appeals Chamber of the Special Tribunal for Lebanon in an interlocutory decision in 2011. Interestingly, the Appeals Chamber turned to two main sources of international law to aid its interpretation: the Arab Convention for the Suppression of Terrorism (to which Lebanon was signatory) and customary international law on terrorism.[12] Using these references, the Appeals Chamber defined terrorism as:

(i) The volitional commission of an act;

(ii) Through the means that are liable to create a public danger; and

(iii) The intent of the perpetrator to cause a state of terror.[13]

In formulating this definition, the Appeals Chamber referred to Article 314 of the Lebanese Criminal Code and expanded the means capable of constituting terrorism so as to not restrict terrorism on the basis of the kind of weapon or means used to carry out a terrorist attack.[14] In this sense then, the Appeals Chamber considered it necessary to interpret the 'means' by which terrorism can create danger in light of contemporary forms of terrorism. This definition of terrorism identifies the elements of terrorism as the act, the method and the motive. By referring to both domestic and international law, the Appeals Chamber incorporates both objective and subjective elements into its interpretation. Whilst this interpretation of terrorism is not binding on courts other than the Special Tribunal for Lebanon, it can nevertheless serve as a useful guide when formulating a definition of terrorism.

Certainly, there are some minor discrepancies between the different definitions provided by United Nations bodies, international conventions and the Special Tribunal for Lebanon. This being

[11] United Nations Security Council Resolution 1566, S/RES/1566, (8 October 2004) at para 3.
[12] Matthew Gillett and Matthias Schuster, 'Fast-track Justice: The Special Tribunal for Lebanon Defines Terrorism', *Journal of International Criminal Justice* 9 (2011), 989 – 1020.
[13] Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging (STL-11-01/I), Appeals Chamber, 16 February 2011, p. 88 at para 147.
[14] Ibid, at p. 80, paras 124 – 129.

said, it is clear there are common elements concurrent through these characterisations of terrorism. One of the defining characteristics of terrorism is the use of intentional violence for political purposes. In short, terrorism is an act of political violence that can be committed wherever and by whomever, seeking to create fear not just for its victims but among a population for the purposes of pursuing the political aims of a given terrorist group. The various definitions above lead to a generic definition of international terrorism which can be understood as *an act of violence for political purposes with the intent to cause death or serious bodily harm or used to threaten violence with the provocation of a state of terror used to intimidate the public or the government of the state which are under no circumstances justifiable*. These elements form the conditions *sine qua non* of terrorism and, where they are present, they serve to distinguish terrorist violence from other criminal and violent acts under international law.

III. Defining Cyberterrorism

The previous section provided a working definition of terrorism that can be used to guide our analysis of international law. This section deals with the definition of cyberterrorism as a contemporary form of terrorism. Cyberterrorism is an act of terrorism that has taken place in, via or through cyberspace and that produces violent consequences sufficient enough to warrant the response of states. Definitions of cyberterrorism generally allude to threats that affect the security of the state and the cyber infrastructure and services it provides. Notably, Dorothy Denning provides a definition of cyberterrorism to mean:

> unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[15]

While technological advances have evolved the way in which terrorism is now carried out, the political objectives of cyberterrorism remain fundamentally the same as conventional terrorism. The harmful act of violence must be conducted for the purposes of intimidating or coercing the state or its population and used for political objectives. Cyberterrorism must also produce some degree of harm in order to constitute an act of terrorist violence. In other words, 'cyberterrorism can be understood as a development of 'traditional' terrorism with different means but similar political and ideological

[15] Dorothy Denning, "Cyberterrorism", Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services, *U.S. House of Representatives* (May 23, 2000). Available at https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm (accessed 3 June 2020).

agendas.'[16] This new and novel platform has developed contextually to involve computers, information technology, data and networks. According to Denning, a defining element of cyberterrorism appears to be the harmful effects that are inflicted on a physical component related to electronic means or information belonging to the critical national infrastructure of the state for political purposes.

The objective of cyber terrorist operations is to inflict violence, which may be part of an operation or the objective of an entire cyber operation. Certain instances of violence can result in physical damage to hardware. Though there has not yet been a cyber terrorist operation that has caused physical harm in this sense, certain incidents have demonstrated that physical damage can be a serious result. For example, the Stuxnet operation in 2010 caused physical destruction to centrifuges in Iran, which was one of the first times that a computer virus or worm was known to cause damage beyond that of targeted hijacking of computers and stealing information.[17] In 2011, the Sony PlayStation Hack resulted in the network being shut down for 23 days as well as the hackers committing credit card fraud and stealing details of 77 million PlayStation Network users.[18] The WannaCry Ransomware in 2017 resulted in critical national infrastructure being disrupted causing severe hindrance to the services of the UK's National Healthcare System.[19] While these examples are not of a terrorist nature, they nevertheless demonstrate that physical damage and disruption is certainly a possible consequence of transboundary cyber operations that is characterised by violence.

[16] Roland Heickerö, 'Cyber Terrorism: Electronic Jihad', *Strategic Analysis*, Vol. 38, 38:4, 554-565, 2014, at p. 564.
[17] See e.g. Kim Zetter,'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', *Wired* (3rd November 2014). Available at https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed 3 March 2020); BBC News, 'Stuxnet 'Hit' Iran Nuclear Plans', 22 November 2010. Available at https://www.bbc.co.uk/news/technology-11809827 (accessed 3 March 2020).
[18] See e.g. Ben Quinn and Charles Arthur, 'PlayStation Network Hackers Access Data of 77 Million Users', *The Guardian Online*, (26 April 2011). Available at https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data (accessed 3 March 2020); BBC News Online, 'PlayStation Outage Caused by Hacking Attack', 25 April 2011. Available at https://www.bbc.co.uk/news/technology-13169518 (accessed 3 March 2020); Jason Schreier, 'Sony Estimates $171 Million Loss from PSN Hack', *Wired* (23 May 2011). Available at https://www.wired.com/2011/05/sony-psn-hack-losses/ (accessed 3 March 2020).
[19] See e.g. National Audit Office, 'Investigation: WannaCry Cyberattack and the NHS', *NAO Department of Health* (25 April 2018); BBC News Online, 'NHS Cyber-Attack: GPs and Hospitals Hit by Ransomware', 13 May 2017. Available at https://www.bbc.co.uk/news/health-39899646 (accessed 3 March 2020); Alex Hern and Samuel Gibbs, 'What is WannaCry Ransomware and Why Is It Attacking Global Computers?', *The Guardian Online* (12 May 2017). Available at https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20 (accessed 3 March 2020).

To add to this, scholars such as Gabriel Weimann,[20] Dorothy Denning,[21] and Susan Brenner[22] share the view that an act of cyberterrorism is a terrorist operation that inflicts a certain level of violence resulting in consequential effects on an intended target. Weimann believes that the threat of cyberterrorism is 'the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)'.[23] His understanding of cyberterrorism is influenced by Denning, who articulates that when considering the threat of cyberterrorism, one must explore the vulnerabilities of targets such as vital infrastructures that could be subject to terrorist violence.[24] Targets susceptible to cyberterrorism are identified as power grids and emergency services, which form part of critical national infrastructures belonging to the effective functioning of the state. It seems then that Weimann and Denning's interpretations of cyberterrorism concerning the nature of the target are comparable to the cyber operations (of a non-terrorist nature) previously discussed.

Furthermore, Brenner contends that cyberterrorism can be executed through the use of different types of weapons; weapons of mass destruction, weapons of mass distraction and weapons of mass disruption.[25] Brenner identifies these categories to range in their levels of severity, with mass destruction imposing the gravest level of harm and the remaining two categories imposing a distinct and significant level of violence on its intended targets. Weapons of mass distraction are described as psychological manipulation that can result in death, injury and property damage. Brenner hypothesizes this type of cyberterrorism whereby 'terrorists hacked the government computer system and sent credible, fake messages, which the local officials reasonably believed'.[26] For weapons of mass disruption, Brenner explains this as the use of computer technology to inflict systemic damage on one or more target systems. Importantly, in Brenner's categories of cyberterrorism, it seems that there must be a minimum level of violence inflicted that results in damage to computer systems or interference with essential systems, with the potential of causing 'personal injury or even death (along with property damage)' in order to constitute cyberterrorism.[27] This distinction is important because

[20] See for example Gabriel Weimann, 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict & Terrorism*, 28:129 – 149, 2005; Gabriel Weimann, *Terrorism in Cyberspace; The Next Generation*, (Columbia University Press, 2015); Gabriel Weimann, 'Cyberterrorism: How Real is the Threat?', *United States Institute of Peace Special Report* 119 (December, 2004).
[21] See for example Dorothy Denning, 'Cyberterrorism: The Logic Bomb Versus the Truck Bomb', *Global Dialogue*, Oct. 2000 p.29; Dorothy Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', *Global Problem Solving Information Technology and Tools*, Dec. 10, 1999).
[22] See for example Susan Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare', *Journal of Criminal Law and Criminology*, Vol. 97 Iss. 2 (2007); Susan Brenner, 'Cyberterrorism: How Real is the Threat?', *Media Asia*, 29:3, 149 -154 (2002).
[23] Weimann, 'Cyberterrorism: The Sum of All Fears?', supra note 20, at p. 130.
[24] Denning, 'Cyberterrorism: The Logic Bomb Versus the Truck Bomb', supra note 21, at p. 34.
[25] Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare', supra note 22, at p. 386 – 400.
[26] Ibid.
[27] Ibid, at p. 398.

not only does it differentiate between the levels of violence, it also demarcates the boundaries as to the minimum level of violence that can constitute an act of cyberterrorism.

In the context of certain rules then, an act of cyberterrorism must cross the threshold of violence to become more than a mere or minor inconvenience in order to fall within the scope of its definition.[28] This interpretation is supported by the Tallinn Manual 2.0, a soft law document concerning the applicability of international legal rules in cyberspace. The Manual presents cyberterrorism as an act conducted by a terrorist group through the use of a state's cyber infrastructure on its territory that affects a right of, and produces serious adverse consequences for, other states. Specifically, those cyber terrorist acts imposing some tangible level of violence resulting in destruction on physical hardware of computer systems or data. For instance, under Rule 7 regarding the principle of due diligence, the Tallinn Manual hypothesizes examples of terrorist groups violating international law through the use of 'destructive malware'.[29] Similarly, under Rule 9 concerning territorial jurisdiction, the Manual uses an example of a terrorist group launching 'cyber operations against the electrical distribution grid of another state, thereby causing a widespread blackout'.[30] In this sense then, the requisite is for a terrorist act to impose some quantifiable level of violence in order to be characterised as cyberterrorism.

From the discussion above, it can be concluded that an act of cyberterrorism can be determined based on two factors: by the violence it inflicts and the nature of its intended target. It is important to point out however, that the view that cyberterrorism must produce physical consequences is somewhat outdated given the progressions of contemporary terrorism.[31] Rather, the level of violence inflicted can be measured based on what is comparable to that of physical effects resulting from traditional terrorism. This understanding of cyberterrorism is shared by Brenner. In an article published in 2012, she asserts that 'for a politically-motivated cyber-attack to be considered an act of cyber-terror, it would have to be serious enough to actually incite terror on a par with violent, physical acts of terrorism such as bombings… Attacks that merely disrupt access to a public website do not'.[32] The distinction made between what is considered an act of cyberterrorism and what is not relies on assessing the level of violence inflicted on the intended target of which must cross a certain threshold of violence and impose sufficiently serious consequences.

[28] Not all rules of international law contain a de minimis threshold i.e. the use of force.
[29] Michael Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereinafter, Tallinn Manual 2.0) (Cambridge University Press, 2017) at 43, paras 2 – 4 and para 6.
[30] Ibid at 56, para 6.
[31] This issue is explored later in Chapters 5 and 6.
[32] Dorothy Denning, 'Stuxnet: What Has Changed?', *Future Internet,* 4, 627 – 687, (2012), at p. 678.

Cyberterrorism, given its violent nature, is becoming a critical threat in the modern world. Indeed, 'the threat of terrorist cyberattack[s] became more plausible after the 2009 discovery of Stuxnet' and subsequent violent cyber operations.[33] Thus, the prevailing narrative surrounding the term cyberterrorism is that despite the lack of an actual cyberterrorist attack, there is a genuine and pervading threat that one will in fact occur. Furthermore, 'many believe it is not a question of 'if' but 'when''.[34] To this end, the following section identifies how OCTAs are integral to cyberterrorism and have the potential to materialise the threat of terrorist violence, in cyberspace or otherwise, necessitating legal attention under international law.

IV. OCTAs as an Integral Part of Cyberterrorism

Cyberspace is used both as a weapon and tool by terrorist groups. Contemporary terrorism sees terrorist groups exploiting cyberspace for the purposes of conducting operational activities that provide sustenance to the organisation. Acronymized as OCTAs, operational cyber terrorist activities, refer specifically to cyber terrorist recruitment, financing and propaganda activities. Recruitment increases membership and divides responsibilities of the group to carry out essential tasks including training recruits, radicalizing members and collecting funds. Terrorist financing equips the organisation with the means necessary to conduct operations and carry out tasks such as providing materials, hiring recruits, producing propaganda, supplying equipment and so forth. Propaganda exposes supporters and the world audience to terrorist ideology that can entice marginalized individuals to join terrorist organisations and give them a sense of belonging. It can be said then that OCTAs are essential to the effective functioning of terrorist groups because they enable the organisation to perform tasks that bring them closer to their political and ideological goals.

OCTAs support the commission of serious terrorist violence, allowing terrorist groups to thrive and prosper. In this sense then, OCTAs can and do lead to violent terrorism where their continued proliferation increases the threat of terrorist violence, whether in cyberspace or on the ground. The current discourse surrounding the use of cyberspace for cyber terrorist attacks or cyberwarfare can then be described as 'overrated'.[35] Cyberterrorism does not reflect the current reality where terrorist groups exploit cyberspace to conduct OCTAs that are low intensity but equally calamitous by way of catalysing violent terrorism. Therefore, the prevailing problem is the continued exploitation of

[33] Weimann, *Terrorism in Cyberspace; The Next Generation*, supra note 20, at p. 134.
[34] Denning, supra note 21.
[35] See Gabriel Weimann, 'www.terror.net How Modern Terrorism Uses the Internet', *United States Institute of Peace, Special Report 116*, (March 2004) at p. 2. The author highlights the mainstream focus of terrorist use of technology; 'when policymakers, journalists and academics have discussed the combination of terrorism and the Internet, they have focused on the overrated threat posed by cyberterrorism or cyberwarfare (i.e., attacks on computer networks, including those on the Internet) and largely ignored the numerous uses that terrorists make of the Internet every day'.

cyberspace for preparatory activities that are conducted by terrorist groups and that form an integral part of cyberterrorism. If achieving violent ends is the definitive triumph for terrorist groups such as ISIS, then the prevention and suppression of OCTAs is paramount in the fight against terrorism to ensure international peace and security. Accepting this, the prohibition of OCTAs is a matter of public international law.

The term 'terrorist use of the internet' has often been used to describe a range of terrorist activities that include those defined under OCTAs. Terrorist use of the internet is used by the United Nations Office on Drugs and Crime (UNODC) in its comprehensive publication to help identify 'the legislative areas in which the United Nations can assist in the implementation by Member States of the Global Counter-Terrorism Strategy in combating the use of the Internet for terrorist purposes'.[36] The UNODC identifies the specific means by which the internet is utilised by terrorists as propaganda, recruitment, incitement, radicalisation, financing, training, planning, execution of terrorist acts and cyberattacks.[37] This term is also employed most notably by scholars Maura Conway and Gabriel Weimann, who use this category to define terrorist groups using the internet as a tool to achieve their aims. Conway identifies the five core uses of the internet by terrorist groups: information provision, financing, networking, recruitment and information gathering.[38] Similarly, Weimann recognises that 'terrorists are using the internet to raise funds, recruit, incite violence, and provide training'.[39]

Whilst terrorist use of the internet recognises several different activities for which terrorist groups employ the internet, OCTAs refer specifically to cyber terrorist recruitment, financing and propaganda activities as the core activities necessary for the effective functioning of terrorist groups.[40] By delineating these specific activities, the term OCTAs allows a wider scope of application when it comes to defining cyber terrorist activities. This is because any other terrorist activities such as training, incitement and networking for instance, can be seen as a composite activity to one of the three core activities defined under OCTAs. For instance, to provide training means to prepare individuals through coaching, teaching, educating or instructing them with the knowledge or skills required to carry out a certain task through the use of cyber technology for the purposes of terrorism.[41] This terrorist activity

[36] United Nations Office on Drugs and Crime (UNODC), *The Use of the Internet for Terrorist Purposes*, United Nations New York (September 2012).
[37] Ibid, at p. 3 – 11.
[38] Maura Conway, 'Terrorism and the Internet: New Media – New Threat?', *Parliamentary Affairs*, Vol. 59, No. 2, 2006, 283-298.
[39] Gabriel Weimann, 'Virtual Disputes: The Use of the Internet for Terrorist Debates', *Studies in Conflict & Terrorism*, 29:623 – 639 (2006), at p. 623.
[40] The rationale for such delineation is a matter further addressed in Chapter 4, in light of the Security Council's recognition and condemnation of these terrorist activities in its resolutions.
[41] This interpretation of training is formulated by reference to UNODC and Oxford English dictionary definition. See UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p. 72. See also Lexico Oxford Dictionary definition 'training'. Available at https://www.lexico.com/definition/training (accessed 1 February 2012).

is part of the recruitment process into the terrorist organisation, and thus constitutes cyber terrorist recruitment. Similarly, networking involves building relationships, interacting with others to exchange information and to develop contacts for the purposes of terrorism, which again falls under the broader activity of cyber terrorist recruitment.[42] In light of this, OCTAs is a broad term that can be used to embody the core functions of terrorist groups.

To explain, OCTAs exist on a spectrum. On one end of the spectrum, there are some OCTAs that are integral to terrorism. OCTAs of this kind are so intimately related to an act of political violence that, if attributed to a state, would amount to an act of terrorism in and by itself i.e., an incitement to violence.[43] This is because there is a close relation between an incitement to violence and a resulting act of political violence, which has been described as a 'pre-stage of terrorism'.[44] For example, a series of Tweets praising and encouraging violent acts of terrorism against a state is an OCTA that amounts to an act of political violence, that if committed by a state, would violate international law. At the other end of the spectrum, there are some OCTAs that form part of the wider general definition of terrorism. These activities are considered functions of terrorist groups that pave the way for the commission of terrorist violence. For example, setting up a Just Giving page to encourage donations to a terrorist group provides support and enables it to function, and further materialises the possibility of political violence. Though these types of OCTAs are essential to the sustenance of the organisation, they do not have sufficiently close proximity to an act of political violence that would otherwise amount to an act of terrorism in and by itself, if it were to be committed by a state.

It can be said then that the characterisation of OCTAs exists on a scale that is defined by context and circumstance relative to the act of terrorism in question. The extent to which OCTAs may become integral to terrorism and form part of the definition of terrorism relates directly to their proximity to the political violence. Thus, OCTAs can be acts of cyberterrorism in and by themselves and they can also be the building blocks that pave the way for violent terrorist acts to materialise. These two categories of OCTAs are distinguished by their level of violence. This distinction is key because, as we shall see later on in the thesis, certain OCTAs necessitate further international legal attention whereas others do not.

In light of the above discussion, OCTAs are integral to cyberterrorism. OCTAs should be defined under cyberterrorism for at least two reasons. First and foremost, OCTAs are part and parcel of

[42] This interpretation of networking is formulated by reference to UNODC and a dictionary definition. See Lexico Oxford Dictionary definition 'networking'. Available at https://www.lexico.com/definition/networking (accessed 1 February 2021).
[43] 'Incite' means to 'encourage or stir up' (violent or unlawful behaviour). Oxford English Dictionary definition of 'incite'. Available at https://www.lexico.com/definition/incite (accessed 11 January 2021).
[44] Ezekial Rediker, 'The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union', *Michigan Journal of International Law*, Vol. 36, Iss. 2 (2015), at 326.

terrorism without which terrorist violence could not materialise. The functioning of terrorist groups relies on cyber terrorist recruitment, financing and propaganda as the preparatory activities that provide the means for terrorism to manifest and enable terrorist groups to orchestrate violent ends, whether in cyberspace or on the ground. In other words, OCTAs facilitate the optimal performance of terrorist groups to ensure that their ideological aims of political violence can be achieved. Terrorists' use of cyberspace as a tool has a genuine and real threat to develop into the use of cyberspace as a weapon.[45] Thus, the threat of cyberterrorism is exacerbated by OCTAs and their role within the effective functioning of terrorist groups is *sine qua non*. Given this, OCTAs must form part of the definition of cyberterrorism because they are linked to violence which is the essence of terrorism; they too are acts of violence characterised by cyber technology and terrorism.

Second, incorporating OCTAs within cyberterrorism is an attempt to elevate the significance of operational terrorist activities which is important in a normative sense. By stressing the indispensable nature of preparatory activities in the wider discourse surrounding cyberspace and cyberterrorism, OCTAs can gain importance through its legal status and meaning. As the building blocks to violent terrorism without which, an act of terrorism could not materialize, the prevention of OCTAs is imperative in the fight against terrorism. Using cyberspace to plan and conduct terrorist activities is now a commonality that is used to achieve 'short-, medium- and long-term objectives, both strategic and operational.'[46] Given that terrorist groups exploit cyberspace to carry out activities that contribute towards the routine functioning of the organisation, cyberterrorism discourse should reflect this predominant use of cyberspace, especially given that OCTAs perpetuate the presence of terrorism. OCTAs are invaluable to the success of terrorist organisations and they have a significant role within cyberterrorism that must be reflected in the normativity of international legal rules. Accordingly, the current approach to dealing with cyberterrorism must account for OCTAs in order to close the normative gap in the legal protection of states.

For these reasons, the international community, academics and policy makers alike must define cyberterrorism to include OCTAs in order to ensure their suppression and prevention under international law.

[45] Jeffrey Thomas Biller, 'Cyber Terrorism: Finding a Common Starting Point', *Journal of Law, Technology & The Internet*, Vol. 4, No. 2, (2013) at p. 319. Biller states that *'using information systems as a tool to further an organization's objectives is distinctly different from using those information systems as a weapon of terror'.*

[46] Shima Keene, 'Terrorism and the Internet: A Double-Edged Sword', *Journal of Money Laundering Control*, Vol. 14, Issue 4, pp. 359-370, (2011), at p, 360.

V. Defining OCTAs

In this section, OCTAs are defined and explored through the lens of the terrorist group ISIS because it developed a significant online presence during the height of its reign.

5.1 Cyber Terrorist Recruitment

Online recruitment is a core operation of terrorism that is fundamental to the functioning of terrorist groups such as ISIS. Cyber terrorist recruitment is defined in this thesis as:

> the process of actively seeking out, finding and enlisting individuals to join a terrorist organisation or to support terrorism through cyberspace or via the use of cyber technology.

With technology developing at a rapid pace, terrorist organisations are using cyberspace to recruit, train and communicate with their followers. Cyberspace is a cheap, fast and effective method of communication where information is available in abundance and the formation of covert networks can evolve seamlessly, making this platform an ideal breeding ground for malicious activities.

Terrorist recruitment typically involves encouraging supporters to participate in pro-terrorism dialogue and publicising support for terrorism through online platforms.[47] This is direct recruitment where terrorists solicit support from online users by fostering relationships with individuals who share and support the same ideologies in a bid to increase their headcount of members in the terrorist organisation. Other tactics may include seeking out individuals with specialist skills such as IT specialists, engineers or native speakers of different countries required to perform certain terrorist functions.[48] This includes but is not limited to financing, propaganda, training of recruits, planning of attacks, and executing attacks.[49] Recruitment can also be indirect where terrorist groups distribute online media campaigns to a non-specific audience with the objective of reaching out to as many people as possible.[50] Cyber terrorist recruitment involves gathering information about supporters, reaching out to potential recruits, exchanging information such as recruitment manuals and ultimately recruiting people to become part of a terrorist network.[51] The purpose is to radicalise people with the objective of finding 'individuals and groups who are willing to sacrifice themselves in the future'.[52] It seems that with the growth of terrorist campaigns and the heavy use of cyber technology, both direct and indirect methods of recruitment are abundant within terrorist agendas.

---

[47] Heickerö, supra note 16, at p. 561.
[48] FATF Report, Financing of Recruitment for Terrorist Purposes, January 2018, at p. 6.
[49] UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p, 3 – 11.
[50] See FATF Report, Financing of Recruitment for Terrorist Purposes, January 2018, at p. 6-7.
[51] See e.g. Maura Conway, 'Terrorism and the Internet: New Media – New Threat?' *Parliamentary Affairs,* Vol. 59, No. 2, 2006, 283-298).
[52] Heickerö, supra note 16, at p. 554.

Social media platforms are a feature of cyberspace which are exploited by terrorist groups. The use of social networking sites such as Facebook and Twitter, which are host to hundreds of millions of accounts, are considered 'powerful tools for mobilisation and recruitment'.[53] The interactive nature of social media allows members to engage in debate, share ideas, and discuss with one another all things related to terrorism. Such platforms are thus used as a propaganda mill and as a recruitment tool.[54] Through Twitter and Facebook, ISIS have been known to openly spread their extremist views and encourage violence against its opposition.[55] Online recruitment campaigns are launched through a variety of different outputs with the production of high-quality videos, images and magazines that are released in many languages including English, Dutch, French, German, Turkish, Spanish and Russian.[56] The panoply of these online materials casts a wide net over potential recruits and strives to appeal to masses of young people through a range of relatable multimedia formats.

The content of terrorist recruitment campaigns often consists of engaging visuals to appeal to its target audience. Propaganda aimed at recruiting young children may take the form of cartoons, video games, comic books, popular music videos, and adverts that invite and incite viewers to participate in extremism. Video games are made intentionally to attract the attention of children, typically requiring the player to claim victory against its enemies which are often portrayed as Western or international forces. Other similar content includes combining children's stories and cartoons with a narrative that promotes and glorifies terrorism and the use of violence, whilst at the same time condemning enemies and encouraging a divisive stance through singing songs of praise to celebrate triumphs of jihad. The nature of targeted terrorist content is aimed at indoctrinating the minds of young children with values of the terrorist organisation as a way to introduce them to life as a militant foreign fighter. These contents are tools that encourage and inspire young people to join terrorist groups.[57]

The volume of terrorist materials surfacing online has led to private companies of social media platforms being urged to moderate content to ensure that violent propaganda for the purposes of recruitment is not being disseminated from their sites. This includes employing technological means such as Artificial Intelligence methods, predictive analysis of social media posts and surveillance practice to detect and suppress pro-terrorism dialogue, particularly removing materials that incite

[53] Javier Argomaniz, 'European Union Responses to Terrorist Use of The Internet', *Cooperation and Conflict,* Vol. 50 (2), 250-268, (2015), at p. 253.
[54] Gabriel Weimann, 'The Emerging Role of Social Media in the Recruitment of Foreign Fighters, in ed. Capone, et al., *Foreign Fighters under International Law and Beyond,* T.M.C. Asser Press, (2016), at p. 80.
[55] Lisa Blaker, 'The Islamic State's Use of Online Social Media', *Military Cyber Affairs*, Vol. 1, Iss. 1, Article 4, (2015), at p. 2.
[56] Weimann, supra note 35.
[57] Blaker, supra note 55, at p. 1. The author points out National Security Council staff Hillary Mann Leverett states that '90,000 pro-ISIS messages were posted on social media' in February 2015.

violence or instigate acts of terrorism.[58] Twitter, Facebook, YouTube and other social media platforms are responsible for ensuring that content is moderated in order to improve on identification and monitoring of terrorist related materials. This means that certain uploads located on these platforms will violate the user's terms of service agreements and will then be subject to deletion if they are found to contain unacceptable content.[59] The analysis of materials involves establishing themes, patterns and trends related to terrorist violence by using algorithms that identify and block terrorist content with the decisive removal of content given to human reviewers at the final stage of the content removal process.[60]

Whilst content moderation has become a controversial part of the global counterterrorism regime in recent years due to its contravention against freedom of expression and human rights, social media platforms nonetheless remain a vital part of the recruitment campaign for terrorist groups. In 2018, EU proposals ordered social media platforms such as Facebook and Twitter to remove terrorist content from their sites within an hour of publications or face extreme financial penalties for the spread of ISIS recruitment propaganda.[61] In the same year, RAND published a report for the United Nations Development Program that found ISIS (and other terrorist groups) were using social media platforms such as Twitter, Facebook and other propaganda magazines to recruit, radicalise and coordinate attacks in Africa.[62] It seems that despite efforts to curtail the efforts of terrorist groups to use the internet for recruitment purposes, they continue to successfully use these platforms to connect with, radicalise and recruit young people from all around the world and it remains a primary method of terrorist engagement. In light of this, cyber terrorist recruitment must be addressed by rules of international law.

The process of recruitment is accomplished over a long period of time where a relationship of trust is fostered between the recruiter and the recruited before an individual is induced into the terrorist organisation. This results in the forming of a bond between what the Islamist religion refers to as the 'Da'wa' and the 'Da'ee', the preacher and the preaching of Islam. The value of culminating a significant relationship is to ensure the da'ee commits themselves wholly to the terrorist organisation, where they can continuously increase their support and solidify their unison to the terrorist

[58] See for example Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', *Chatham House Research Paper* International Security Department (August 2019).
[59] See e.g. Stuart Macdonald, Sara Giro Correia, Amy-Louise Watkin, 'Regulating Terrorist Content on Social Media: Automation and the Rule of Law', *International Journal of Law in Context,* Vol. 15, 183 – 197 (2015).
[60] Ibid.
[61] EUROPOL, 'Europol and Telegram take on Terrorist Propaganda Online', Press Release (25 November 2019). Available at https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online (accessed 5 August 2020).
[62] United Nations Development Program (UNDP) Regional Centre for Africa, 'Social Media in Africa: A Double-Edged Sword for Security and Development', Research Report, 5 November 2018.

organisation and its ideology. One significant tool used for jihadi's recruiting and radicalising individuals is the handbook 'A Course in the Art of Recruiting', where the importance of the da'wa role is explained:

> Statistically speaking, if you make da'wa to one person every year, and this person makes da'wa to one person every year, then after 30 years the number will be 1 billion…[63]

This manual equips jihadis with instructions on how to radicalise individuals effectively, setting out guidelines on appropriate techniques to successful indoctrination. The manual is a directive, and places great emphasis on the jihadi recruit to abide by certain rules, for example 'you must occupy as much of his time as you can', and 'don't remind him of his previous behaviour'.[64] This is simply one example of the type of materials that terrorist groups make readily available online to supporters in their efforts to recruit. With multiple sites granting access to this handbook online, the circulation of terrorist materials is facilitated by the sharing of information through technology. Not only does this have the potential of exposing the public to terrorist content, but it also supports the incitement of terrorism through extreme radicalisation employed to indoctrinate the minds of others.

The UNODC recognises terrorist recruitment as 'a way to develop relationships with, and solicit support from, those most responsive to targeted propaganda'.[65] Thus, a large proportion of terrorist content is exclusively directed towards vulnerable and marginalised groups in society. The process of recruitment and radicalization 'commonly capitalises on an individual's sentiments of injustice, exclusion or humiliation',[66] which makes young people an ideal target for terrorist recruitment. This is particularly the case for individuals that struggle to find a sense of belonging within their own communities and turn to online platforms to seek acceptance, finding comfort in joining and being a part of a terrorist organisation. As a result, there is a plethora of terrorist materials in the form of cartoons, music videos, and computer games to attract young people.[67] By promoting and glorifying acts of terrorism, online content is deliberately designed to influence and inspire minors to join the cause for terrorism.

Whilst the number of male recruits is significantly higher, there is an increase in the percentage of young women joining groups such as ISIS.[68] The same recruitment tactics are employed for women

---

[63] Abu Amru Al Qa'idy, 'A Course in the Art of Recruiting – Revised July2010' available at https://archive.org/stream/ACourseInTheArtOfRecruiting-RevisedJuly2010/A_Course_in_the_Art_of_Recruiting_-_Revised_July2010_djvu.txt (accessed 1 May 2017).
[64] Ibid.
[65] UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p. 5.
[66] Ibid.
[67] Ibid.
[68] See Joanna Cook, and Gina Vale, 'From Daesh to 'Diaspora': Tracing the Women and Minors of Islamic State', *International Centre for the Study of Radicalisation* (2018). The report states that 41, 490 citizens from 80 different countries joining ISIS in Iraq and Syria, of which 13% were recorded to be women.

where they are often targeted through Facebook, Twitter or other recruitment propaganda and presented the opportunity to live an idyllic life as 'ISIS brides' in conflict zones such as Syria.[69] Young girls and women tend to perform supportive roles such as preparing food, gathering materials, providing medical treatment to fighters, and maintaining the camps where terrorist groups are based.[70] Notoriously, women are recruited to contribute towards the mission of terrorist organisations by producing children or raising children with terrorist fighters and indoctrinating these children with the militant group's values in order to create child soldiers ready for life in terrorism.[71] This is because women are typically perceived as non-violent and they arouse less suspicion than men when travelling and bypassing through checkpoints and border controls making them the ideal asset for terrorist groups.[72] A study at London's International Centre for the Study of Radicalisation and Political Violence projected several European women in Iraq and Syria who have either accompanied their jihadist husbands or have travelled to the region with the intention to marry members of ISIS or other militant groups.[73]

However, women are increasingly seen to engage in more violent roles, as well as being exposed to violence as a tactic of terrorism. Women are recruited as suicide bombers, fighters, and militants or that their role evolves to taking on such positions within the organisation. Young girls may be subjected to violence, sexual slavery and marriage upon their recruitment into terrorist organisations to the extent that it becomes normalised for them. The recruitment of women and young girls is thus a vital part of effectuating terrorist organisations and the fulfilment of specific roles is a strategic measure employed by terrorist groups. The active contribution to and participation in violence exhibited by young girls and women indicates that the means of recruitment for terrorist groups such as ISIS is no longer restricted to age or by gender-based roles. Accepting this, online recruitment for terrorist organisations is a matter that requires international legal attention.

The success of terrorist groups relies significantly on increasing their headcount of membership through the radicalisation and recruitment of minors and women. In addition to this, creating and maintaining an effective terrorist organisation that is well equipped for the commission of ultimate terrorist violence is facilitated by both the provision of finances and the dissemination of information via propaganda materials online, as we shall see next.

---

[69] See for example, Amanda N. Spencer, 'The Hidden Face of Terrorism: An Analysis of Women in Islamic State', *Journal of Strategic Security* Vol. 9, No. 3, Special Issue: Emerging Threats (Fall 2016), pp. 74-98.
[70] Jessica Trisko Darden, 'Tackling Terrorists' Exploitation of Youth', *American Enterprise Institute*, May 2019, at p. 5.
[71] Weimann, supra note 54, at p. 84 – 85.
[72] See Kara Anderson, '"Cubs of the Caliphate" The Systematic Recruitment, Training and Use of Children in the Islamic State', *International Institute for Counter-Terrorism*, January 2016.
[73] See Cook, and Vale, supra note 68.

5.2 Cyber Terrorist Financing

Financial acquisition is crucial to the prosperity and sustenance of terrorist groups. Cyber terrorist financing is defined in this thesis as:

> the provision of funds or providing financial support to individual terrorists or terrorist groups through cyberspace or via the use of cyber technology for the purposes of terrorism or for terrorist causes.

The acquisition of finances enables a terrorist group to carry out certain tasks related to recruitment and propaganda, as well as the training of recruits, the purchasing of materials and weapons, the travel costs of recruits to conflict zones, and the launching of terrorist offensives both on the ground and in cyberspace.[74] Expenses of a terrorist organisation can be extremely high and it was revealed that, in 2014, ISIS required around $5 million per month to operate.[75] It seems that the more money that can be attained, the more a terrorist group can prosper and develop in various facets, ultimately supporting the commission of violent acts of terrorism. Typically, the acquisition of funds is a three-stage process, involving the raising, moving and storing of funds.[76] The raising of funds has changed significantly for terrorist groups that were once restricted to physical means of procuring funds. Since the threat of terrorism has become far more decentralised, 'Al-Qaeda's central command is not funding operations as it once did'.[77] Facilitated by the advent of cyberspace and cyber technology, terrorist groups today can raise funds in a multitude of different ways.

The UNODC identifies four categories of terrorist financing: direct solicitation, e-commerce, the exploitation of online payment tools and charitable organisations.[78] Direct solicitation is where terrorist groups, through the use of social media platforms and websites, distribute emails and targeted communications, and actively request donations from supporters. E-commerce involves the setting up of websites to facilitate the transfer of funds in the form of online stores for the purchase of propaganda materials, such as magazines, books, videos and audio recordings. Online payment tools are available through specific websites or platforms used to make the transfer of funds easier through electronic means. For instance, transfers are typically made through wire transfers, credit cards, or other online payment facilities such as PayPal or Skype.[79] Whilst online payment tools can be used willingly between parties, it is equally common for terrorist groups to acquire funds fraudulently through identity theft, credit card fraud and other forms of intellectual property crimes. Lastly, the

[74] Conway, supra note 38, at p. 284 – 286.
[75] Wes Cooper, 'The Dark Side of the Economy: A Comparative Analysis of the Islamic State's Revenue Streams', *Journal of Terrorism Research*, Vol. 8 (1), 34 – 42.
[76] Financial Action Task Force (FATF) Report, *Terrorist Financing Risk Assessment Guide*, FATF Paris, July 2019.
[77] Michael Jacobson, ''Terrorist Financing and the Internet', *Studies in Conflict & Terrorism* 33:353-363, (2010) at p. 347.
[78] UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p. 7.
[79] Ibid.

use of charities is a widely used method of acquiring finances for terrorism. Charities are easy, accessible avenues for terrorist organisations to collect funds or donations to support their activities and simultaneously, conceal the nefarious movement of funds. Terrorist organisations are known to exploit charities by using them as front organisations that appear to support humanitarian causes whilst instead, diverting funds for illicit purposes. Given that 'banned or exposed charities tied to terrorism can…shut down one day and reopen the next under a new name,' it seems that cyberspace is an ideal platform to acquire funds for terrorism.[80]

Cyber technology facilitates the efforts of terrorist groups to raise funds effortlessly, removing the barriers that were once limited by geographical and territorial boundaries.[81] Affording a 'virtual bridge' for terrorists to engage in malicious activities across borders, cyberspace allows financing operations to be conducted at a larger scale and for greater return.[82] As a result, the threat of cyber terrorist financing is significant and remains a prevalent terrorist threat, particularly in the context of cyber terrorism. Yet, in the words of Jacobson, terrorists' exploitation of cyberspace 'is only likely to increase as the scope and scale of the Internet expands, and with other related technological development.'[83] The benefits of using cyberspace to acquire terrorist financing is considered two-fold, where the 'dual objectives of raising finances and disrupting national economic infrastructure can be achieved in one operation'.[84] As a virtual operation, cyber terrorist financing can cause direct impacts on critical national infrastructure and subsequently threaten the security of a state without necessitating any physical proximity or physical element for its execution, making cyberspace an extremely appealing platform for terrorists. For this reason, terrorist activities conducted through cyberspace is a matter that should fall within the regulatory purview of international law.

The type of funding source that terrorist groups are able to acquire will depend on the group's size, capabilities, opportunities, member's skills and expertise, start-up costs, ideological and political considerations as well as geography.[85] The more members of a terrorist group, the more capable it is of performing malicious tasks and advancing the strength of the organisation. ISIS is notorious for its sophisticated propaganda campaigns and violent extremism that has resulted in thousands of deaths, casualties and calamities around the world. Aside from its traditional methods of financing which includes oil revenues, taxation in controlled territories (though this has come to a halt following the

[80] Jacobson, supra note 77, at p. 356
[81] Ibid. The author recognises that using the Internet is now an integral part of terrorist activities, and '*to raise and transfer funds is also part of a broader global shift toward the use of technology in international commerce*'.
[82] Paul Carroll, and James Windle, 'Cyber as an Enabler of Terrorism Financing, Now and in the Future', *Journal of Policing, Intelligence and Counter Terrorism*, 13:3, 285 – 300 (2018).
[83] Jacobson, supra note 77, at p. 359.
[84] Ibid, at p. 288.
[85] Cooper, supra note 75, at p. 286.

defeat of ISIS caliphate in Syria and Iraq), and illicit antiquities trading, ISIS reap billions of US dollars through cyber hacking, fraudulent schemes and cybercrimes such as malware and ransomware attacks.[86] The success of ISIS in acquiring funds is attributed to the group's recruitment, with its membership including tens of thousands of individual from across the world, which enables ISIS to gain a steady stream of income.

Both large-scale fraudulent schemes and piecemeal financing operations are continually launched worldwide to secure the provision of funds for terrorist operations. ISIS' growing use of cyberspace to expand its revenue through criminal activity online has led to its financing operations targeting an array of victims ranging from individuals to corporate and state entities. Terrorist groups operate as large criminal networks and exploit online users through identity theft and credit card fraud schemes to launder money, and to obtain and produce valuable goods and services such as false identification documents to produce passports, airline tickets for travel and cell phones for untraceable communications. Often, identity theft and credit card fraud schemes target users of specific websites, forums or chat rooms, or more recently, users of online payment systems, mobile-banking, and digital currencies.[87] In addition, terrorist groups also target private and state-owned financial institutions to conduct isolated, though extensive, operations to acquire funds. This typically involves skilled individuals hacking into bank systems through the use of malware or viruses, gaining access into bank institutions and stealing large amounts of cash. In either case, there is no question that terrorist organisations exploit cyberspace for the provision of funds targeting the government, private businesses and individuals to further their terrorist agenda.

A key element of cyber terrorist financing is the movement of funds to avoid traceability and detection from authorities. To facilitate this, terrorists are turning to the Dark Web to move funds through digital cryptocurrencies to use services as well as to buy and sell contraband. The Dark Web is a secure, encrypted part of the internet that is intentionally hidden from search engines and masks IP addresses of its users. Consisting of networks that are 'decentralised and anonymous',[88] the Dark Web has since 'turned into a major platform for global terrorism and criminal activities.'[89] The Dark Web is made up of marketplaces similar to consumer platforms eBay and Amazon, where listings are made for the sale of products, services or contrabands, typically illegal goods like firearms, credit card frauds schemes, drugs as well as counterfeits. The transaction of these goods and services are through

[86] Patrick Blannin, 'Islamic State's Financing: Sources, Methods and Utilisation', *Counter Terrorist Trends and Analyses*, Vol. 9, No. 5 (May 2017), pp. 13 – 22.
[87] See Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnson, 'Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats', *RAND Corporation* (2019).
[88] Ibid at p. 197.
[89] Gabriel Weimann, 'Going Dark: Terrorism on the Dark Web', *Studies in Conflict &Terrorism*, 39:3, 195-206, (2016) at p. 202

the use of Bitcoin, among other emerging cryptocurrencies (such as Ethereum, Monero and Blackcoin etc.), that provide the secure storing and transmitting of virtual tokens.[90] Though not impossible to track, terrorist groups often convolute the traceability of its digital money path by continuously moving money through different Bitcoin transactions. Thus, a major benefit of using cryptocurrencies is the difficulty for law enforcement to trace transactions due to the anonymity of user identities.

Consequently, the evolution of technologies has provided and continues to provide terrorist organisations with different avenues to raise and move funds whilst evading law enforcement. From carrying out organisational tasks to recruiting foreign terrorist fighters to the orchestration of violent terrorist acts, money is essential to support terrorist groups. Tackling the financing of terrorism is a global issue that many states face. Since the proliferation of ISIS' online terrorist campaigns in 2014, measures to counter terrorist financing among other terrorist activities, has become a priority for certain states. The UK has adopted specific counter-terrorist financing and anti-money laundering legislation to minimise the vulnerabilities in combating terrorist financing.[91] Equally, the US has introduced a national strategy that counters existing and emerging terrorist funding methods through robust targeted actions against terrorist financing networks.[92] In addition to this, efforts on a European and international level see the EU's anti-money laundering and counter terrorist financing regimes, as well as the Financial Action Task Force being launched as regional and global efforts on addressing terrorist financing.[93] These measures are manifest and the fight against the financing of terrorism is an international issue that remains a primary concern of many sovereign states. This said, multilateral action by all states, especially through primary rules of international law, is significant and necessary for the prevention and suppression of cyber terrorist financing.

5.3 Cyber Terrorist Propaganda

International terrorism relies on the use of propaganda to inspire its supporters, incite violence and spread terrorist ideology to all corners of the world. Cyber terrorist propaganda is defined in this research as:

> an act of political violence that can take the form of information or communication, which includes but is not limited to text, images, videos, articles, magazines, audio and visual files, video games and websites, used to promote terrorism or support terrorist causes through cyberspace or via the use of cyber technology.

[90] See Dion-Schwarz, Manheim, Johnson, supra note 87.
[91] UK Statutory Instruments, The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 No. 1511. Available at https://www.legislation.gov.uk/uksi/2019/1511/contents/made (accessed 11 August 2020).
[92] The White House National Strategy for Counterterrorism of the United States of America, October 2018. Available at https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf (accessed 11 August 2020).
[93] European Commission, 5th Anti-Money Laundering Directive (Directive (EU) 2018/843); FATF, Terrorism Financing Risk Assessment Guidance, FATF, Paris, July 2019.

Empowered by cyberspace, terrorist propaganda can take various formats including videos, graphic images, articles, magazines, audio and visual files, as well as video games.[94] The varying formats enable terrorist groups to spread extremist messages in different ways that can be distributed for the general population or targeted to a specific audience.[95] Propaganda allows terrorists to have direct control over the content of their messages and to manipulate the narrative sent out to both their supporters and enemies.[96] Disseminating propaganda is thus a pivotal part of modern terrorism where 'publicity and media are considered a necessity in the world of cyberterrorism'.[97] Given the advancement of emerging technologies exploited by terrorist organisations like ISIS, engaging in online discussions, reacting to social media posts and participating in violent discourse via the internet is 'the new political activism'.[98] As such, propaganda is an essential feature that allows terrorist groups to raise awareness of the cause to engage in recruitment, to inject fear into its enemies, to increase group cohesion, as well as to execute terrorist operations which is further facilitated through the use of cyber technology.[99]

The advent of cyberspace allows terrorist propaganda to reach even the most marginalised communities. ISIS's cyber jihad campaign is the modern channel for targeting young and vulnerable individuals to join the terrorist group.[100] For individuals that are more susceptible to extremist ideology, ISIS tactically utilises propaganda to create a support network for potential recruits to feel accepted.[101] Through the use of Facebook, Twitter, YouTube and other social media platforms, ISIS is exploiting communicative services as a means to sell the ISIS brand and act as a recruitment tool to acquire more members.[102] Thus, terrorist propaganda is designed to appeal to a wide range of audiences whether that is 'direct or indirect victims of acts of terrorism or to the international community or a subset thereof'.[103] There are no specific requirements for an ideal recruit of terrorism.

---

[94] UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p. 3.
[95] See e.g. Argomaniz, 'European Union responses to terrorist use of the Internet', *Cooperation and Conflict*, Vol. 50 (2), 250-268, (2015); Rudner, '"Electronic Jihad": The internet as Al-Qaeda's Catalyst for Global Terror', *Studies in Conflict and Terrorism*, (2016); Conway, 'Terrorism and the Internet: New Media – New Threat?' *Parliamentary Affairs*, Vol. 59, No. 2, 283-298, (2006).
[96] Weimann, supra note 35, at p. 6.
[97] Elizabeth Minei and Jonathan Matsuitz, 'Cyberspace as a New Arena for Terroristic Propaganda: An Updated Examination', *Poiesis Prax* (2012) 9:163 -176, at p. 168.
[98] Imran Awan, 'Cyber Extremism: ISIS and the Power of Social Media', *Social Science and Public Policy* 54: 138 – 149 (2017), at p. 141.
[99] Daniel Milton, 'Fatal Attraction: Explaining Variation in the Attractiveness of Islamic State Propaganda', *Conflict Management and Peace Science* 1 – 21 (2018), at p. 2.
[100] J.M Berger, 'How ISIS Games Twitter', *The Atlantic* (2014), available at https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/ (accessed 1 February 2021).
[101] Awan, supra note 98.
[102] Ibid at p. 147.
[103] UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p. 4.

Rather, supporters that become recruits of a terrorist organisation are 'young and old, educated and uneducated, new to the organisation and veterans of jihadi conflicts.'[104]

Within ISIS' online propaganda campaign, Twitter dominates as the primary tool used to spread propaganda and to recruit new members. In 2014, ISIS began interacting with supporters and members to promote religious, political and military agendas online.[105] A primary feature of ISIS' Twitter use is the reposting and sub-tweeting of extremist views through ISIS-related accounts and mentions to generate more followers and increase the number of supporter accounts. Part of ISIS' social media strategy is also to hijack dormant Twitter accounts to further spread and increase the dissemination of extremist views. Research has also shown that ISIS creates content to 'fit the aesthetic of [a] particular region' in order to appeal to those members and increase the effectiveness of their Twitter campaigns at generating support.[106]

Primarily, through spreading violent materials and extremist views, ISIS is 'able to create a climax of fear and anxiety… [which] allows them to reinforce their messages and use social media sites like Twitter to act as an echo chamber'.[107] By using this platform to trend a provocative narrative, ISIS actively and forcibly promotes violent attitudes and implements extremism through the encouragement and use of violence. Specifically, ISIS made use of 'hashtag hijacking' where they were 'using the hashtag #WorldCup with the accompanying words: "This is our ball…it has skin on it"'.[108] In making threats to the World Cup through the posting of pro-ISIS messages, ISIS actively broadens their audience through posting unrelated trending hashtags. Secondly, and according to Awan, 'Twitter therefore acts as a megaphone by which ISIS are able to send out live updates of fighters tweeting about what is feels like to be in Syria'.[109] Supporters and followers of ISIS on Twitter are able to experience an online extremist community without needing to be in the region of conflict. Twitter as a global platform thus enables ISIS to have an expansive reach and radicalises a population without the need for proximity to achieve such goals. The use of social media platforms thus enables cyber terrorist propaganda and is a matter of international law that must be suppressed in the fight against terrorism.

After losing control of territory in Syria and Iraq, ISIS' presence on Twitter began to decline after 2018. Instead, 2019 saw ISIS begin to exploit social media app TikTok as a recruiting tool targeted at

[104] Milton, supra note 99, at p. 8.
[105] Berger, supra note 100. The author discusses an app used by ISIS that at its height, posted 40, 000 Tweets in one day.
[106] Majid Alfifi, Parisa Kaghazgaran, James Caverlee, and Fred Morstatter, 'Measuring the Impact of ISIS Social Media Strategy', *Stanford Network Analysis Project* (2018).
[107] Awan, supra note 98, at p. 142.
[108] Ibid.
[109] Ibid.

young people. TikTok is a popular application that has over 1.5 billion active users, many of them children and teenagers and it is used to upload, watch and browse 60 second video clips with a range of creative and interactive features.[110] Given the breadth of audience on this platform, TikTok is increasingly being exploited to share 'far-right' ideology and this includes videos containing violence.[111] Content promoting ISIS videos began surfacing on TikTok, showing footage of ISIS fighters with guns and corpses being paraded through streets, as well as videos of beheadings.[112] Videos reportedly focused on recruitment efforts targeting potential foreign fighters, with the glorification of militants singing to ISIS songs. ISIS also shared videos targeting young girls and women to join the organisation as wives and lovers to jihadist fighters. Though, the identification and removal of ISIS accounts has been relatively minor (reportedly two dozen ISIS related accounts on TikTok), the growing popularity of this platform for young people is indicative that ISIS are making continued efforts to disseminate violent extremism and recruitment efforts via social media.[113]

Aside from social media, the production of online-only magazines was first produced by Al-Qaeda in 2010 under the name Inspire. The magazine's thematic focus centred on inspiring and instructing homegrown terrorist attacks, as well as covering both religious and political discourse situated within the Western world.[114] From 2014, ISIS followed in the same footsteps and created its own magazine issues under the name Dabiq. Whilst covering much of the same themes, Dabiq reinstates the fight against 'enemies of Allah' with a 'goal to empower Muslim youth'.[115] Both magazines, although having ceased in production, are still widely available online to inform supporters, young Internet users, and the rest of the world on Islamic State terrorism. The loss of the Syrian town Dabiq then saw ISIS relaunch a new online publication under the name Rumiyah, continuing to praise terrorist attacks and deprecate the opposition.[116] Made professionally to compliment ISIS' social media campaign, both Dabiq and Rumiyah are made with exceptional visuals and produced in various languages for ease of accessibility.

---

[110] See Gabriel Weimann, and Natalie Masri, 'Research Note: Spreading Hate on TikTok', *Studies in Conflict & Terrorism* (2020).
[111] Ibid at p. 2.
[112] Sam Shead, 'TikTok Used by Islamic State to Spread Propaganda Videos', BBC News, (22 October 2019). Available at https://www.bbc.co.uk/news/technology-50138740 (accessed 14 August 2020).
[113] Adi Robertson, 'TikTok Removes Two Dozen ISIS Propaganda Accounts', *The Verge Online*, (21 October 2019). Available at https://www.theverge.com/2019/10/21/20925416/tiktok-islamic-state-terrorist-propaganda-recruitment-account-videos (accessed 14 August 2020).
[114] Julian Droogan, and Shane Peattie, 'Reading Jihad: Mapping the Shifting Themes od Inspire Magazine', *Terrorism and Political Violence*, 30:4, 684 – 717.
[115] Inspire, 'Shattered: A Story About Change', (Issue 12, Spring 2014) at p. 32. Available at https://azelin.files.wordpress.com/2014/04/inspire-magazine-issue-12.pdf (accessed 2 May 2017).
[116] Adam Withnall 'ISIS Loses 'Prophesied' Town of Dabiq to Syrian Rebels After Short Battle', *The Independent* (16 October 2016) available at http://www.independent.co.uk/news/world/middle-east/isis-dabiq-loses-apocalyptic-prophesy-town-of-dabiq-to-syria-rebels-short-battle-a7363931.html (accessed 2 May 2017).

There are many different types of violence portrayed by terrorist propaganda ranging from pro-ISIS messages that show political support to videos of terrorist attacks that contain bloodshed and gore. Though not all terrorist materials are violent, 'the promotion of violence is a common theme in terrorism-related propaganda'.[117] In fact, according to Daniel Milton, research shows that the most viewed terrorist propaganda is typically material containing 'retribution violence against the group's enemies'.[118] In his own words, this is 'violence designed to evoke emotions toward the idea that it can defeat enemies and punish non-believers'.[119] A reason for this is that retribution propaganda contains extreme levels of violence, for instance in beheading videos, and viewers often satisfy their curiosity by viewing either all or part of a video clip.[120] Research also shows that people watch graphic videos due to fear of terrorism, where individuals pay more attention to visual stimulation that they find frightening.[121] It seems then that the more provocative the material, the more views it tends to gather online, perpetuating the dissemination of terrorist propaganda.

Terrorist propaganda is described by the ITU as 'illegal content',[122] and previous discussion on regional legislation surrounding terrorist propaganda has established that such content is indeed condemned by the international community.[123] This is because terrorist propaganda is disseminated with the objective of negatively influencing its viewers and for that visual content to inspire vulnerable individuals to become part of terrorist organisations as well as to generate fear among the rest of the population. More importantly, since 'propaganda is a mode of communication aimed at swaying the attitude of people toward some cause',[124] its dissemination via the internet has had and continues to have a profound impact on the social behaviour of its audience.[125] ISIS' social media campaign is evident of success in recruiting young people as foreign terrorist fighters and young women to become jihadi brides. This is attributed to the use of thematic language in ISIS content to create a divisive narrative between ISIS and its opponents and to shape perceptions and manipulate thoughts in order to achieve the desired response of its supporters. As a result, ISIS has been particularly effective at using social media sites such as Twitter and Facebook to create a 'them vs. us narrative' and foster a community of supporters that perpetuate this divide.[126]

---

[117] UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p. 4.
[118] Milton, supra note 99 at p. 2.
[119] Ibid at p. 7.
[120] See Sarah Redmond et al., 'Who Watches an ISIS Beheading – and Why', *American Psychologist,* Vol. 74, No. 5, 555 – 568 (2019).
[121] Ibid.
[122] Marco Gercke, 'Understanding Cybercrime: Phenomena, Challenges and Legal Response', *ITU Publication* (September 2012), at p. 222.
[123] See Chapter 3 which discusses regional legislation in light of OCTAs.
[124] Minei, and Matsuitz, supra note 97, at p. 167.
[125] Awan, supra note 98, at p. 141.
[126] Ibid at p. 147.

As a matter of fact, one of the most common types of terrorist propaganda used by ISIS is material that encourages and incites unlawful violence. Distinct from propaganda that shows passive support for ISIS, a large part of the group's propaganda focuses on inspiring supporters to carry out political violence. Whilst there is no fixed definition of incitement, it is often understood as consisting of 'public provocation to commit terrorism or public praise for terrorist acts, dehumanisation of the victims of terrorist attacks, or mere understanding for the underlying reasons for terrorist acts.'[127]

ISIS has been prolific in its use of language within propaganda to incite violence. For instance, images and videos that contain high levels of gore, bloodshed and violence reflects their capacity and willingness to inflict harm and the desire for terrorist groups to incite violence against its enemies. At the same time, these materials have the intention of provoking others to do the same. When terrorist groups produce propaganda that incites violence, they justify this behaviour as necessary for the purposes of terrorism. Not only does this create a deeper commitment to life as a terrorist, but inciting violence also becomes part and parcel of terrorism that is recognised as an achievement for its members. The more extreme the violence that is celebrated within the terrorist community, the greater the marginalisation of terrorist members from the conventional society.[128] As a result, there has been an increase in 'lone wolf terrorism' associated with ISIS where supporters of terrorism act alone in committing violence.[129] The terrorist attacks in San Bernardino (2015), Orlando (2016) and Manchester (2017) are exemplar of individuals committing violent acts on behalf of ISIS. Though there are other factors that contribute towards lone wolf terrorism, such as social isolation, ideological justifications and mental health among others, ISIS-inspired individuals are led to commit attacks through bombing materials, operational manuals as well as videos that incite violence.[130] By advertising and promoting violence, the objective is for viewers and supporters to sympathise with and support the ideology behind extreme terrorism and provide motivation for launching future attacks.

---

[127] Bibi Van Ginkel, 'Incitement to Terrorism: A Matter of Prevention or Repression?', *International Center for Counter-Terrorism Research Paper* 3 (August 2, 2011).

[128] See Sarabeth A. Smith, 'What is Old is New Again: Terrorism and the Growing Need to Revisit the Prohibition on Propaganda, *37 Syracuse J. Int'l L. Com*. 299, 303 (2010), at p. 101.

[129] This research focuses on terrorists and terrorist groups that are linked to a terrorist organization i.e. Islamic State. This might include lone wolf terrorists that conduct activities associated with a terrorist network by pledging allegiance whilst operating alone. Whilst the multi-faceted approach to conducting OCTAs means they typically involve more than one member to perform activities, this may not necessarily be the case. For instance, cyber terrorist recruitment involves hiring others to join a terrorist network and participate in terrorist activities. However, cyber terrorist financing may be carried out by a lone wolf terrorist, where they raise funds through illicit donations and then carry out a terrorist attack alone. Similarly, cyber terrorist propaganda can easily be distributed by a lone wolf terrorist and requires no support by a terrorist network or other terrorists. As such, the potential for a lone wolf terrorist and a terrorist group to conduct OCTAs is comparable. Though, it seems there is often a pledge of allegiance by lone wolf terrorists to an established terrorist group.

[130] See Paul Gill, John Horgan, and Paige Deckert, 'Bombing Alone: Tracing the Motivations and Antecedent Behaviours of Lone-Actor Terrorists', *Journal of Forensic Sciences*, March 2014, Vol. 59, No. 2.

In 2012, the UNODC recognised that the prevention of incitement for the protection of national security justifies limitations to the freedom of expression but that any such limitation must be both necessary and proportional to the threat posed. Curbing the freedom of one's speech is vindicated only if that speech constitutes an incitement of terrorism and therefore a threat to national security and public order.[131] The UNODC makes specific reference to distinguishing between terrorist materials that contain incitement as opposed to those considered as 'mere propaganda'. The differentiation that numerous Member States agreed with is that 'a showing of the requisite intent and a direct causal link between alleged propaganda and an actual plot or execution of a terrorist act is required'.[132] For the UNODC, this means that the prohibition of terrorist propaganda is enforced only if it can be linked to a planned terrorist attack or operation. Absent of this direct nexus, mere propaganda, that is materials that do not incite violence linked to an actual terrorist plot, is not considered unlawful. The UNODC thus considers only terrorist propaganda that presents a certain level of threat within its content as prohibited propaganda.

During the height of its online campaign between 2014 - 2017, ISIS has also increasingly used propaganda featuring children as a tactic to incite violence. This is because children have 'higher attachment to ideology and require more exhaustive efforts to counter their indoctrination', making their recruitment essential and easier to maintain for terrorist groups.[133] Children are easily influenced, and upon recruitment they become even more susceptible to terrorists' control and indoctrination, making them ideal recruits.[134] Notoriously, a terrorist video was subject to much media scrutiny when a video of a four year old with a detonator in his hand purportedly blowing up a vehicle with three ISIS prisoners inside circulated online.[135] The presence of children within terrorism serves as the 'second generation of mujahideen conditioned and taught to be a future resource for the group'.[136] Therefore, it is clear that there is no exception for children in terrorism. This has become a

---

[131] UNODC, *The Use of the Internet for Terrorist Purposes,* supra note 36, at p.6, paragraph 12. The report states that *'preventing and deterring incitement to terrorism in the interest of protecting national security and public order are legitimate grounds for limiting freedom of expression, as provided under article 19, paragraph 3, of the International Covenant on Civil and Political Rights…any restrictions on the exercise of this right must be both necessary and proportional to the threat posed'.*

[132] Ibid.

[133] Darden, supra note 70, at p. 5.

[134] Ibid, at p.4.

[135] See e.g. Jack Sommers, 'Islamic State Propaganda Video Shows British Boy, believed to be Isa Dare, Blowing Up 'Car of Spies', The Huffington Post UK, 11 February 2016. Available at https://www.huffingtonpost.co.uk/2016/02/11/islamic-state-propaganda-isa-dare_n_9207036.html (accessed 18 March 2020); Nigel Morris and Lizzie Dearden, 'ISIS Video 'Showing British Child Blowing Up Car With Prisoners Inside' Shows Jihadists are in Retreat, says PM', The Independent, 11 February 2016. Available at https://www.independent.co.uk/news/uk/home-news/isis-video-showing-british-child-blowing-up-car-with-prisoners-inside-shows-jihadists-are-under-a6867131.html (accessed 18 March 2020); Gordon Rayner, ''Jihadi Junior' Confirmed to be Isa Dare, son of female British fanatic with links to Lee Rigby killers', The Telegraph, 4 January 2016. Available at https://www.telegraph.co.uk/news/worldnews/islamic-state/12080134/Jihadi-Junior-son-of-female-British-fanatic-with-links-to-Lee-Rigby-killers.html (accessed 18 March 2020).

[136] Noman Benotman and Nikita Malik, 'The Children of Islamic State', *Quilliam International*, March 2016, p. 28.

progressively successful tactic to recruit support for the terrorist organisation and thus, propaganda involving young children has become rife.[137]

From the propaganda materials examined above, it is clear that an integral part of spreading propaganda is to ultimately lead to the radicalisation of its viewers. Whilst it can be said that propaganda is a commonplace task required for the self-promotion of terrorist ideology and its production is widespread and omnipresent, the menacing nature of extreme online content has a threatening potential to stimulate and encourage the commission of violent acts of terrorism, which otherwise, would not have been possible absent of such. Given this, the presence of cyber terrorist propaganda cannot and must not be undermined, and its prevention and suppression under international law remains paramount in the fight against terrorism.

VI. OCTAs and Human Rights

The discussion of OCTAs (and terrorism more generally) cannot be broached without recognising the conflict between the obligations identified by this study and human rights. This is particularly the case with respect to measures tackling propaganda, which may infringe upon freedom of expression, for example. The task of striking a balance between enforcing counter-terrorism mechanisms and the preservation of freedoms through human rights engenders considerable difficulty, and thus warrants significant attention from law enforcement regimes. Although this conflict between tackling OCTAs and the protection of human rights naturally offers scope for important analysis to be undertaken, this is better reserved for future study. The justification for this is as follows: the main objective of this research project is to examine the extent to which international law can be called upon to dampen and suppress the use of the Internet for terrorist related activities. Given the state-centric nature of international law, the aim of this project is to examine what, if any, obligations international law imposes upon states to prevent the occurrence of OCTAs. States are of course subject to (conventional and customary) obligations under international law to protect human rights and must thus tackle the threat of OCTAs in compliance with these international legal rules. How international human rights law restricts the ability of states to address the threat of OCTAs is important, not least because the general benefits of supressing OCTAs would be lost if this activity was conducted in a manner contrary to human rights. But, fundamentally, the question of whether international law requires states to suppress OCTAs, and question of whether states can achieve this aim within the requirements laid

[137] See e.g. Vale, 'Cubs in the Lions' Den: Indoctrination and Recruitment of Children Within Islamic State Territory', *International Centre for the Study of Radicalisation* (2018); Almohammad, 'ISIS Child Soldiers in Syria: The Structural and Predatory Recruitment, Enlistment, Pre-Training Indoctrination, Training, and Deployment', *ICT Research Paper,* February 2018; Darden, 'Tackling Terrorists' Exploitation of Youth', *American Enterprise Institute*, May 2019.

down by international human rights law, are different and can be assessed separately. This project disentangles these questions and focuses upon the former.

VII. Conclusion

The lack of a universal definition of terrorism has not prohibited a general understanding of the term neither has it hindered legal approaches to tackle terrorism. This is because international legal instruments have provided interpretations of terrorism that have allowed for a common understanding through its core elements. In turn, this has allowed for an interpretation of cyberterrorism to develop. The advances in technology means that cyberterrorism has evolved in unprecedented ways that now sees terrorists use of cyberspace as both a tool and a weapon to cause serious political violence. This is particularly the case for ISIS and its tactical and prolific use of social media campaigns to further its ideological goals. In light of this, terrorists' exploitation of cyberspace for the purposes of conducting OCTAs is a matter that necessitates international attention.

This chapter has presented OCTAs as the preparatory activities necessary for the effective functioning of terrorist groups that can and do lead to acts of political violence. This chapter has sought to provide a general definition of cyber terrorism and present OCTAs as an integral part of cyber terrorism. This chapter has also identified two types of OCTAs, one of which triggers international legal action of states. In doing so, this chapter acts as a frame for the legal analysis that follows. As this chapter has shown, OCTAs are not only indispensable to the sustenance of terrorist groups, but the conduct of these malicious activities is also conditional upon each other. OCTAs are the core contributors to ultimate acts of terrorist violence, and which catalyse terrorist attacks. As a matter of international peace and security, it is vital to ensure that cyberterrorism prioritises the prevention and suppression of OCTAs in the fight against global terrorism under existing rules of international law. Following this, the next chapter situates OCTAs within the framework of international peace and security.

Chapter Two

OCTAS WITHIN THE FRAMEWORK OF INTERNATIONAL PEACE AND SECURITY

I. Introduction

The primary aim of the international legal system is to achieve and maintain international peace and security. The notion of international peace and security is defined in positive and negative terms and these different dimensions illustrate the broad range of threats faced by the contemporary international society. Terrorism is one such threat, and it endangers international peace and security in both its positive and negative conception. The threat posed by terrorism is amplified by cyber technology, particularly through OCTAs, that is, cyber terrorist recruitment, financing and propaganda activities.

Accordingly, the purpose of this chapter is to situate OCTAs within their broader theoretical context and in particular within the context of international peace and security. Section II explores the meaning of international peace and security and gives meaning to the normative values of positive and negative peace. Section III explores the role of international law in maintaining international peace and security. Section IV explores the contemporary threat that modern terrorism poses to international society. Section V then presents OCTAs as a threat to international peace and security.

II. Theory of International Peace and Security: Negative and Positive Peace

Within the context of international relations, the maintenance of peace implies the absence of inter-state disputes which threaten violence and conflict. There are two sides to the peace theory, which includes a negative and a positive concept.[1] Johan Galtung describes negative peace as the 'absence of personal violence' and positive peace as the 'absence of structural violence'.[2] His definitions of peace are interpretations of violence, for the latter (violence) is one certain and defining feature that characterises the former (peace).[3] In light of this, the following section explores peace in both negative and positive terms and also discusses the concept of security within international law.

2.1 Negative Peace

Negative peace reflects the lack of conflict or violence for states.[4] Creating negative peace concerns ways at reducing and eliminating violence and this is most significantly accomplished through the prevention of war or other forms of large-scale violence. Negative peace is described using the terms

[1] Johan Galtung, 'Violence, Peace and Peace Research', 6 *Journal of Peace Research* (1969), at p. 183.
[2] Ibid.
[3] Ibid, at p. 168.
[4] Nicholas Tsagourias and Nigel White, *Collective Security: Theory, Law and Practice*, (CUP, 2013), at p. 41.

'personal violence' and 'direct violence' characterising this threat with a degree of certainty to its objects. Used synonymously, both connotations describe consequences of violence which 'can be traced back to concrete persons as actors.'[5] In other words, personal and direct violence can be understood as the result of a person directly harming another person. As such, personal violence presents itself as an overt form of violence that generates tremendous fluctuations over time.[6] This is because direct violence is reflected in periods of war that are not consistent but instead impose violence on its objects in varying waves. Where there is a state of war within society, it is a visible effect of violence. Given this, personal violence is easier to identify because it 'shows'.[7] Though, the relationship between direct violence and its object does not have to produce destruction or death per se. Rather, personal or direct violence tends to result in manifest physical violence, and it is the threat of physical violence against the object that characterises the violence and gives it meaning under the theory of peace.

Tsagourias and White explain that threats to achieving negative peace are dealt with by the collective security system as the referent object of the international peace and security mandate. Whilst 'war is waged between states and affects the security of states and is limited to states as actors',[8] the primary threat to achieving negative peace can also be seen as the state. War is a mechanism for states to display and exercise military power on the international scene for the purposes of creating peace. Thus, war can be described as a 'legal condition' through which norms and ideals, that is ensuring peace and security, can be achieved through the use of force.[9] In this sense then, the concept of negative peace can, to some extent, be seen as paradoxical. Whilst achieving negative peace requires the absence of violence and conflict, states engage in violence and conflict, at least in some part, for the purpose of creating peace and security. On the one hand, states must manage international conflicts in order to control, contain and reduce actual and potential violence. On the other, states engage in violence and conflict to 'create spheres of political order and balances of power [that plays] a vital role in underpinning long periods of peace'.[10] Negative peace thus faces the paradox of requiring the achievement of a condition that is threatened by the same primary object responsible for creating this condition

This said, creating negative peace is not without detriment to the state. Whilst engaging in war has the ultimate objective of achieving peace, states expose themselves to the possibility of danger

[5] Galtung, supra note 1, at p. 170 – 171.
[6] Ibid.
[7] Ibid, at p. 173.
[8] Tsagourias and White, supra note 4, at p. 24.
[9] John Bassett Moore, *Digest of International Law*, (Vol. 7, 1906), at p. 153.
[10] Barry Buzan, 'Peace, Power and Security: Contending Concepts in the Study of International Relations', *Journal of Peace Research*, June 1984, Vol. 21, No. 2, Special Issue on Alternative Defense, pp. 109 – 125, at p. 117.

and harm in the process. By participating in conflict, states' risk their national sovereignty and the protection of its civil society at the hands of violence. Depending on the intensity, the consequences of war can be catastrophic and irreparable, affecting states and impeding the recovery of its internal structure for generations. Despite this, states engage in war with the overriding intention of establishing order in what can be described as the state of anarchy. Barry Buzan presents anarchy as the fragmented political condition necessary for war which results from the absence of any principal political authority governing the international society.[11] Anarchy reflects the assertion of each sovereign territorial state as the ultimate source of political authority within its own domain. As such, anarchy facilitates the outcome of war because the system within which anarchy exists requires states to struggle to preserve their own survival. Conflict and war are thus a product of an anarchic system that breeds competition among states.

Today, however, war is no longer the principal danger to negative peace and ensuring security. After the end of the Second World War, inter-state wars were no longer the core of international conflict, with anarchy between states diminishing upon the collapse of empires. Obstructions to achieving peace have increasingly seen the rise of armed conflicts, military coups, and civil wars as part of the peace-building process.[12] Given this, the contemporary world has seen a fundamental shift in threats to security with intra-state conflicts occurring within the borders of states taking precedence as a prevailing threat to international peace and security.

2.2 Positive Peace

Positive peace is presented by Galtung as the absence of structural violence. It is often characterised as 'social injustice' because it is built into the structure of a system and 'shows up as unequal [powers] and … unequal life [chances]'.[13] These threats are 'structural defects of the international or national system', which have the potential to incite structural, or indirect violence and cause instability within the state.[14] Unlike personal violence, structural violence is not visible within the society. Structural violence is experienced by humanity through the social structure which groups exist within, persisting silently and often static. Galtung further emphasises structural violence as 'inequality',[15] where societies are subject to certain unequal distributions of power. For instance, the condition of poverty can cause society to experience an imbalance of power where there is a lack of institutional

[11] Ibid, at p. 113.
[12] See e.g. Emily Crawford, 'From Inter-State and Symmetric and Intra-State and Asymmetric: Changing Methods of Warfare and the Law of Armed Conflict in the 100 Years Since World War One', *Yearbook of International Humanitarian Law*, Vol. 17, No. 2014, pp. 95 – 118 (2006), Sydney Law School Research Paper No. 16/44; Muzaffer Ercan Yilmaz, 'Intra-State Conflicts in the Post-Cold War Era', *International Journal on World Peace,* Vol. 24, No. 4, (December 2007), pp. 11- 33.
[13] Galtung, supra note 1, at p. 171.
[14] Tsagourias and White, supra note 4, at p. 24.
[15] Galtung, supra note 1, at p. 175.

mechanisms available to support people that are struggling. The concept of positive peace thus places the 'integration of human society' as core to achieving this condition.[16]

Despite this, Galtung contends that the absence of personal violence 'does not lead to a positively defined condition' simply because direct violence in the form of war does not exist.[17] Whilst negative peace identifies the referent object as the state itself, positive peace concerns the individuals that make up the state.[18] The qualities that form positive peace focus on the growth of social values to progress the survival capacity via the equal distribution of power in one's society. Galtung's theory of positive peace thus emphasizes the need for society to develop in a manner that reduces inequality and progresses to cultivate humanity and promotes humane conditions for people to thrive and prosper. By promoting egalitarianism within the social system, the absence of structural violence can then be seen as a condition that can sustain peace for civil society with longevity.[19] As such, structural violence is characterised by the conditions in a society, which are often the root causes of violent conflict. Structural violence is therefore the antithesis to direct violence; such that positive peace is parallel to negative peace.

Structural violence captures violence within the society that can amount to violations of international law. Violence in the structural system can include the 'exploitation, repression and exclusion' of individuals whom 'may die or be held in a permanent state of misery, including malnutrition and illness'.[20] It can also take the form of political conflict, which Galtung has alluded to as 'a revolution brought about by means of a highly hierarchical military organisation'.[21] Such revolutions include political uprisings to reform government institutions in the form of an apartheid, for example.[22] Other forms of structural violence can include social injustice, poverty, and terrorism, though they are not limited to these forms. The purpose of structural violence seeks to distinguish different phenomena of violence within a social structure that can produce equal measures of harm as negative peace. The attributes of a structure can then impose violence in the society which ultimately results in victims of the state, or put simply, the number of persons killed. The difference between direct violence and structural violence is that for the former, the number of persons killed is a result of violence inflicted upon them, whereas, for the latter, the number of persons killed is caused

[16] Johan Galtung, 'An Editorial', *Journal of Peace Research* (1964), 1(1): 1-4.
[17] Galtung, supra note 1.
[18] See e.g. Barbara van Tigerstrom, *Human Security and International Law: Prospects and Problems*, (Hart Publishing, 2007).
[19] Ibid at p. 184. Galtung believes that *'the short-term costs of personal violence appear as small relative to the costs of continued structural violence'.* He further explains that this does not limit the gravity of personal violence but identifies the tendency of personal violence to incorporate physical violence as exampled by large-scale violent revolutions.
[20] Ige F. Dekker, 'Reconsidering the Legal Relevance of Structural Violence' in eds. P. J. I. M., De Waart, Erik Denters, Nico Schriver, *Reflections on International Law from the Low Countries*, (Martinus Nijhoff Publishers, 1998) at p. 326.
[21] Galtung, supra note 1, at p. 172.
[22] Dekker, supra note 20.

by the lack of necessities. In any case, the presence of negative peace and positive peace produce the same output as one another, that is, fatalities.

Yet, given that structural violence is not easily visible within society and cannot be quantified to a singular act of violence, its effects are arguably less obvious than the consequences of direct violence. Moreover, the lack of a specific and direct actor in structural violence makes establishing positive peace a more complex task. In this sense then, the cause and effect of structural violence is less vigorous in nature and does not appear at first-hand as violence in the traditional sense. However, the tranquillity of structural violence should not appear less threatening than the volume of warfare and there is no reason to assume that structural violence amounts to less suffering than personal violence.[23] That is to say, war does not necessarily produce more catastrophes than that of structural violence. Rather, the stability and silence of structural violence can seep into society without much notice because it is 'about as natural as the air around in us.'[24] The indiscernibility of structural violence is, in any case, menacing to the stability of the state for its consequences are accepted as the norm of society within which those tragedies manifest. To this end then, the concept of positive peace becomes even more vital to understanding current threats to the modern world.

Key findings of the Positive Peace Report 2015 reveal consistency with Galtung's theory of peace and his analysis in statistics.[25] The report determines a number of key findings. Positive peace has steadily increased since 2005, with 73% of countries ranked in the Positive Peace index having shown an improvement to 2015. There is a direct correlation with positive peace and civil resistance campaigns: the higher the levels of positive peace, the fewer and less violent these campaigns. The majority of all violent movements (91%) that took place were situated in countries with the lowest levels of positive peace. Furthermore, findings show that democracies consistently have the strongest level of positive peace, but represent the minority of countries.[26] Among other findings, the report indicates that positive peace is generated by the creation and sustaining of peaceful societies, which correlates with Galtung's conception of peace through both negative and positive conditions.

Both positive and negative peace emphasise the absence of violence as necessary to both the safeguarding of a civil society and the existence of the state itself. According to Tsagourias and White, 'only the achievement of both negative and positive peace will ensure the minimum of human survival

[23] Galtung, supra note 1, at p. 173.
[24] Ibid.
[25] Institute for Economics and Peace, 'Positive Peace Report 2015: Conceptualising and Measuring the Attitudes, Institutions and Structures That Build A More Peaceful Society', *Vision of Humanity* (2015). Available at http://visionofhumanity.org/app/uploads/2017/04/Positive-Peace-Report-2015.pdf (accessed 21 August 2020).
[26] Ibid, at p. 22.

and will also enable human flourishing'.[27] This interpretation of peace further emphasises the protection of the state domain to be synonymous with the prosperity of the society within it. Structural violence shows that the existence of violence within a structure has the same potential to disrupt peace and security in the same, if not, potentially more destructive manner than direct violence. The absence of structural violence and indeed the absence of direct violence are attained only through the creation of both positive and negative peace as necessary conditions to limiting the presence of violence.[28]

2.3 Definitions of Security

Peace and security may be seen as conjugal values in the broader sense of explicit international legal principles. The achievement of peace, however, does not guarantee a state of security. A state that faces no threat of violence does not necessarily make its environment secure for civilization. Instead, it is fair to assume that achieving peace can be seen as the impetus for achieving security of the state and indeed, vice versa. International law identifies the importance of the state and human survival as objectives of state security.[29] States are responsible for guaranteeing their own survival through the protection of its sovereign territories by investing and developing in their military strength. The competitive pursuit of military capability is therefore the state's responsibility to ensure its own welfare, security and internal political structure can be protected and defended from external aggression in the face of conflict with other states. Equally, the state must guarantee the human survival of its civilisation in the developing international world by fostering a secure environment without the threat of violence.[30] After all, the ultimate objective for states is to guarantee security for its territory and for its citizens. One may ask then, what is the meaning of security? And how is security relevant to Galtung's theory of peace? These two issues are explored in turn next.

There are various interpretations of security. Williams describes security as 'the alleviation of threats to acquired values',[31] and similarly, White interprets this concept to mean 'the absence of existential threats to states, peoples and individuals'.[32] Meanwhile Kelsen claims security is 'the condition of being protected against or not exposed to, a danger'.[33] Whilst these definitions differ in

[27] Tsagourias and White, supra note 4, at p. 42.
[28] See Peter Lawler, 'Peace Studies', in ed. Paul Williams, Security Studies: An Introduction (Routledge, 2nd Ed, 2013) at p. 86. Lawler posits that *'the extrapolation of the capacity to limit recourse to violence would only produce the condition of negative peace, whereas the extrapolation of the human capacity to cooperate would realise a condition of positive peace'.*
[29] See e.g. Vaughan Lowe, *International Law*, (Clarendon Law Series, 2007), p. 100-104.
[30] See e.g. Russell Buchan, *International Law and the Construction of the Liberal Peace*, (Hart Publishing, 2013).
[31] Paul Williams, 'Security Studies, 9/11 and The Long War', in A.J. Bellamy et al. eds, *Security and the War on Terror*, (Routledge, 2008) at p. 9.
[32] Nigel White, *Keeping the Peace*, (Manchester University Press, 1997) at p. 45.
[33] Hans Kelsen, *Collective Security Under International Law*, (Washington, DC, Naval War College, 1957) (New Jersey, Lawbook Exchange, 2011) at p. 1.

their wording and articulation, it is clear that there are common elements to the meaning of security that provide a general understanding of the term. From the definitions above, the meaning of security can be understood as the prevention of a threat or danger which has the potential to cause harm to a protected interest of a state, persons or individual. It seems that the epitome of security is the state of being free from a threat or danger and thus, to achieve that state is to ensure the protection of valued interests from such threat or danger.

Interestingly, Arnold Wolfers offers a more dynamic view of security whereby he describes the condition of security as both objective, where there is an absence of threat, and subjective, denoting the absence of fear.[34] This interpretation implies that security has both a practical and conceptual aspect to it, in that the assessment of security can be measured by both fact and feeling. The absence of a threat is proved by evidence and the absence of fear is expressed by the feeling of safety. However, this understanding of security does not imply that objective security automatically infers subjective security. For example, it is possible that the perception of a threat may not necessarily incur fear, and vice versa. Rather, the relationship between both aspects is to some extent binary. In international law, state security is quantified on the basis of reducing fear for those affected by potential threats and eliminating uncertainties that obstruct the quest for a secure environment in the territory of that state. It can then be understood that security as a concept is both a condition and a value prioritised by states to fortify their chance of survival and to ensure the peaceful coexistence with other states in the international community.[35]

Much like the theory of peace, security correlates directly with the achievement of certain conditions through negation. In other words, only will the absence of certain conditions achieve security, and likewise peace, as distinct concepts. The absence of fear and threat creates security, and the absence of direct and structural violence creates the conditions for peace. Security, however, is not synonymous with peace. That is to say, the achievement of security does not by default equate to peace. The absence of fear or threat is quantified by a material concept such as war. This, in turn, indicates that the creation of security requires at least the negative condition of peace to be achieved. Security can then be understood as a 'very limited aspect of peace' that encompasses but is not limited to the concept of war.[36] Therefore, in spite of their differences, the relationship between peace and security is intimately correlated and can be understood in harmony with each other. Only when there

[34] Arnold Wolfers, "National Security as an Ambiguous Symbol", in: Arnold Wolfers (Ed.): *Discord and Collaboration. Essays on International Politics* (Baltimore: John Hopkins University Press): 147−165.
[35] See Matthew Bourne, *Understanding Security*, (Palgrave Macmillan 2014) at p. 1-9.
[36] Johan Galtung, 'Theory and Practice of Security'*, Instant Research on Peace and Violence*, 1972, Vol. 2, No. 3, European Co-operations (1972), pp. 109 – 112, International Peace Research Institute, Oslo, at p. 109.

exists no threat or fear of direct violence and of structural violence can the conditions of peace and security be achieved in absolute.

Conditions to both peace and security are achieved through the enforcement of international legal rules imposing obligations upon states to shape their behaviour. Accordingly, the next section explores the role that international law plays in achieving international peace and security.

III. The Role of Law in Maintaining International Peace and Security

International law was founded upon relations between states 'operating horizontally…between those entities recognised as possessing personality on the international plane, such as states and international organisations.'[37] As such, the international legal system provides states with a structure to govern inter-state relations in times of war and peace.

International law is composed of principles, values and rules that determine how peace and security can be achieved through normative regulations. Legal norms set the parameters within which states may act and determines the extent to which they can do so. Law has a normative function, governing states to behave in ways that will secure peace for the international community. These legal rules are described as norms because they are standards which must be fulfilled by states in order to meet certain objectives and to achieve international peace and security. As an 'aggregate of the legal norms', these rules come in various forms with the core focus of achieving international peace and security.[38] Weil describes these norms as prescriptive, prohibitive and permissive denoting what states must do, must not do, and may do respectively.[39] For example, states have an obligation to respect the sovereign territory of other states and this norm is prescribed by international law through state practice.[40] Likewise, states are prohibited from the use or threat of force against other sovereign territories and this is enshrined in Article 2 (4) of the UN Charter.[41]

Among the range of normative objectives that must be achieved, the prevailing purpose of implementing rules is to maintain a functioning legal order. International law prescribes legal rules on

[37] James Crawford, State Responsibility: The General Part, *Cambridge Studies in International and Comparative Law*, (CUP, 2014), at p. 79.
[38] See Prosper Weil, 'Towards Relative Normativity in International Law?', *The American Journal in International Law*, Vol. 77, No. 3, (July 1983) pp. 413-422.
[39] Ibid at p. 413.
[40] Island of Palmas case (Netherlands v. United States), Permanent Court of Arbitration (Huber), 2 Reports of International Arbitral Awards (1928), p. 829: *'Territorial sovereignty… involves the exclusive right to display the activities of a state. This right has as a corollary a duty: the obligation to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and war, together the rights which each state may claim for its nationals in foreign territory. Without manifesting its territorial sovereignty in a manner corresponding to the circumstances, the state cannot fulfil this duty'*; see also ICJ, Corfu Channel Case (Merits), ICJ Rep., 1, at p. 35: *'between independent states, respect for territorial sovereignty is an essential foundation of international relations'.*
[41] Article 2(4) of the Charter of the United Nations, 1945.

how states should behave in conducting inter-state relations as a means of achieving international peace and security. The purpose of international law is to ensure 'peaceful relations between states and [it] should be regarded from the perspective as a technical discipline, providing the tools for statesmen'.[42] In this sense then, international law enables states to navigate relations between other states and acts as an instrument for which states can implement certain norms and values. Legal rules prescribe responsibilities to states and determine how peace can be achieved as an international community. As long as states observe the values and principles that are protected by international law, their behaviour can shape international peace and security in a way that guarantees the achievement of these norms and serves to safeguard the rights of sovereign states. Peace and security are therefore values and ideals to the international legal order that serve to protect and ensure the survival of states through the negation of war, violence and conflict, as well as to prevent external aggression from other states.

Since international peace and security is no longer restricted to the competitive pursuit of military capabilities, progression to prioritise an emphasis on international rules has increasingly bound states to legal obligations in pursuit of common objectives. As Louis Henkin stipulates, 'almost all nations observe almost all principles of international law and almost all their obligations almost all of the time'.[43] On this view, international law imposes responsibilities upon states and it becomes a duty of the state to ensure that these responsibilities are not violated but observed, fulfilled and discharged. The role of international law is therefore essential to the international legal order and indispensable to the achievement of peace and security. States exist in a world of law and order where legal regulation plays a critical role in building and sustaining the international system. The utility of law in the world order is premised on the fact that having a system of law is better than having no system of law at all. An international legal system enables the attainment of common values and legitimises international rules for sovereign states. Particularly in a decentralised international society where interests are diversified and conflicting, an international legal system affords states with the necessary apparatus for implementing international policies aimed at achieving social and economic objectives that reflect the entire international community.

With this in mind, international law functions because states intend for and consent to a form of legitimate governance through abiding by legal rules. The most prominent example of this is through the UN's collective security system and the Security Council in particular, which has the primary

[42] Jan Klabbers, *International Law*, (CUP, 2013) at p. 4.
[43] Louis Henkin, *How Nations Behave*, (Cambridge Polity Press,1979), 47.

responsibility of maintaining international peace and security.[44] The scope of its powers are enacted via the constituent treaty of the Charter of the United Nations, where a broad set of principles relating to matters of international law, such as 'international cooperation', 'friendly relations' and universal peace' are laid out for its members to adhere and observe to.[45] The majority of states are part of the UN, which binds them to principles and rules of law through the UN Charter.[46] In order for the Security Council to carry out its duties, it prescribes, prohibits and permits rules of international law for states through legal mechanisms such as resolutions, decisions and reports. In turn, this process provides a structure that formalises states actions through institutional procedures. This is one example of legal rules prescribed through a legal instrument that binds states to international obligations. Through the UN's collective security system, states demonstrate the will to vest power in institutions, which forms genuine credence to the inference that states see the law as an effective means to securing international peace and security.

Aside from general principles and treaty law, international law is also asserted through rules of customary law. Customary international law is obligatory rules of conduct that are accepted as legal requirements by states. It is widely accepted that the formation of customary law is established from two elements; general and consistent international practice among states and that such practice is in accordance with the law shown in patterns of *opinio juris*.[47] The formation of customary international law involves the crystallisation of emerging custom into new rules. This is the process by which sufficient state practice supplies evidence of *opinio juris* which then codifies an emerging principle of international law into custom. There is, however, uncertainty over what constitutes state practice including how to demonstrate such practice, or how consistent such practice needs to be.[48] As a result, the formation of customary international law has often been described as vague, unclear and a somewhat imprecise source of international law.[49] While this has often been presented as a shortcoming of customary law, the flexible process of such law-making allows it to fill the gaps that

[44] Article 1 (1) of the Charter of the United Nations, 1945; *'The Purposes of the United Nations are to maintain international peace and security…'*
[45] Article 1 (1)-(4) of Charter of the United Nations, 1945.
[46] The United Nations website lists the current members of the UN. Available at http://www.un.org/en/member-states/ accessed 1 October 2017.
[47] See generally: Art. 38(1)(b) of the Statute of the International Court of Justice; North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p.3 at para 77; Ian Brownlie, *Principles of Public International Law* (4th ed.) (Oxford: Clarendon, 1990) 4-11; eds. Robert Jennings and Arthur Watts, Oppenheim's International Law (9th ed.) (Harlow: Longman, 1992) vol. 1. There are alternative views of customary international law, see e.g. Lazare Kopelmanas, 'Customs as a Means of the Creation of International Law, 18 *British Yearbook of International Law* 127 (1937) (customary international law is composed only of state practice); and Bin Cheng, 'United Nations Resolutions on Outer Space: "Instant" International Customary Law', 5 *Indian Journal of International Law* 23 (1965), at 36 (customary international law only has 'one constitutive element', the *opinio juris*).
[48] Anthony D'Amato, *The Concept of Custom in International Law*, (Cornell University Press, 1971) at p. 4.
[49] Karol Wolfke, *Custom in Present International Law* (2nd ed.) (Martinus Nijhoff Publishers, 1993).

treaties and conventions otherwise cannot.[50] Customary law can also aid in the interpretation of international legal rules and shed light on the meaning of treaty provisions where necessary.

Furthermore, customary law is fundamental to international law as the only source of international law that is binding on all states. This is particularly important because it means certain rules of international law impose legal obligations on all states, despite those states not being party to treaties or conventions of the same nature. Thus, customary law is a part of traditional international law-making that allows for the formation of new norms where emerging trends are developing, which are also referred to as 'uncodified fields' of international law.[51] On this view, customary law is capable of evolving to deal with contemporary issues when the need arises. Thus, a great benefit of customary international law is the ability to create law by circumventing the need for extensive treaty drafting and congregations involving a number of states. Custom therefore plays a significant part in international law making and crystallising the development of new legal rules.

In complying with rules established in treaties, UN resolutions and custom, international law ensures states exhibit desirable behaviours enabling them to protect a shared environment which can in turn, guarantee certain values and norms. The performance of such conduct simultaneously demonstrates to other states the effects of adhering to the same international obligations. To some extent, the observance of international legal rules for instance, that 'states will respect each other's sovereign equality and individuality as well as the rights inherent in and encompassed by its sovereignty…', ensures that said states will themselves benefit from the adherence to such rules.[52] International law therefore obliges states to act in certain normatively desirable ways and to encourage the observance of such rules by fostering cooperation within the wider international community for the purposes of achieving shared community objectives.

Nevertheless, the purpose of law is contingent upon states accepting and recognising that these norms form the basis of the international legal order and relies on their compliance with such rules. Since the function of law is to impose a degree of order between the relations of states for the purpose of achieving peace and security, fulfilling these objectives hinges on the performance of states international obligations as it concerns their inter-state conduct. In this sense, states are obedient to international legal rules which allows them to achieve certain conditions. In the context of negative peace then, the achievement of this condition involves the prevention of direct violence between and

[50] United Nations General Assembly, Michael Wood, First Report on Formation and Evidence of Customary International Law, UN Doc. A/CN.4/ 4663 (17 May 2013), at para 35.
[51] Omri Sender and Michael Wood, 'Custom's Bright Future: The Continuing Importance of Customary International Law', pp. 360 -370, at p. 364 in Curtis A. Bradley, *Custom's Future: International Law in a Changing World*, (Cambridge University Press, 2016).
[52] Article I of Conference on Security and Cooperation in Europe Final Act ('Helsinki Final Act'), Helsinki 1975.

against states. Subsequently, the use of military power is prohibited by way of the non-use of force principle.[53] In turn, this offers to some extent, a protection of sovereignty for all states. The abstention from using military force is an example of how international law is implemented to prohibit (and equally, permit) certain actions of states in order to achieve peace and security.

In a similar manner, positive peace is achieved through the compliance of legal rules endorsing the respect for human rights, equality and social justice. Indeed, such values are core to building social justice and in turn, to diminishing structural violence. The notion that achieving international cooperation in solving international problems of an economic, social, cultural or humanitarian nature is a core objective enshrined in the UN Charter.[54] This is further coupled with promoting and encouraging respect for human rights and for fundamental freedoms without discrimination.[55] In this regard, the Charter embraces values that reflect positive peace and implements legal rules that enables the achievement of this condition. States accept the legal rules that compels them either to act or to abstain from acting, enabling them to achieve international peace and security. It can be said then that states observance of 'legal rules, do, in fact, foster compliance with regime norms.'[56] States actively adhere to international legal norms and values because they too desire an international community that embraces these very norms and values. Law is therefore a viable legal framework for which community values can be protected and legitimises the behaviour of states in doing so.

However, dynamic threats to international peace and security are shaped by social, economic and political advances that can impact and change the development of legal rules over time. The threat to security moving from military to non-military sources, specifically international terrorism, is a prime example of this. International law exists to safeguard state relations between each other, and between the state and its citizens. Terrorism threatens this relationship between the state and its citizens by jeopardising their safety with an intent to rebel against the state. In the words of Tal Becker, 'when private actors are able to terrorize communities and perpetrate international violence without international responsibility, individual citizens no longer benefit from the monopoly over the use of force bestowed upon the state'.[57] The prevailing danger of terrorism is that these groups operate without nexus to a state. They threaten international peace and security for all states worldwide, but at the same time, they are able to evade legal responsibility and subsequent principles of international law that would ensure punitive measures if such conduct was attributed to the state.[58] As such, the

[53] This is found in Article 2(4) of the Charter of the United Nations, 1945
[54] Article 1(3) of the Charter of the United Nations, 1945
[55] Ibid.
[56] Harold H. Koh, 'Why Do Nations Obey International Law?', *The Yale Law Journal*, Vol. 106, No. 8, (June 1997) pp. 2599-1659, at p. 2625.
[57] Tal Becker, *Terrorism and the State: Rethinking the Rules of State Responsibility*, (Hart Publishing, 2006), at p. 2.
[58] Ibid, at p. 252.

threat posited by today's terrorist organisations contrast largely with the previous types of non-state activity that were prevalent at one time. Given this, the current legal landscape must be considered in the context in which it was created and in light of the emerging contemporary challenges.[59] Accordingly, the next section situates international terrorism within Galtung's theory of peace and presents it as a threat to international peace and security.

IV. Terrorism as a Threat to International Peace and Security

4.1 The Nature and Evolution of Terrorism

Terrorism has become a central concern for state security in the contemporary world. The concept of terrorism, however, is not by any means new. As early as the 18th century, terrorism was understood as an instrument of state-controlled violence that repressed individuals who were considered enemies of the state.[60] This connotation of terrorism as state directed violence continued into the Second World War, with Nazi Germany's military control across Europe, Germany and Allied Air Forces use of terror bombings and Stalin's ruling of Russia all considered acts of terror.[61] This said, during the 20th century, non-state armed groups remained relatively insignificant and shrouded by the process of state consolidation and the competition among powerful nation states.[62] Post-war terrorism was often linked to self-determinations that saw specific territories being colonised by foreign states in the struggle for power.[63] It was after this period that modern terrorism began to transform into 'new forms of fundamentalist religious terrorism'.[64]

As a result, the last century has witnessed an emergence of terrorism as 'a label for political violence by non-state actors'.[65] International attention became increasingly focused on terrorism in the Middle East as tensions between the US and states in the region intensified and resulted in violence and conflict. For example, Hezbollah – supported by Iran – was responsible for the suicide bombings against the US embassy and the US marine barracks in Lebanon both in 1983.[66] There was also the Lockerbie bombing of Pan Am Flight 103 in 1989 where two Libyans were suspected of being

[59] Ibid, at p. 3.
[60] With its earlier uses of the term deriving from the Reign of Terror (1793-94) in the French Revolution. See Michael Rapport, '*The French Revolution and Early European Revolutionary Terrorism'*, p.72, in ed Randall D. Law, *The Routledge History of Terrorism,* Routledge (2015).
[61] Ben Saul, '*Defining Terrorism in International Law*, (OUP, 2006), p. 2.
[62] See also John Darwin, 'Nationalism and Empire in the 1950s', pp 167 – 221, in *Britain and Decolonisation: The Retreat from Empire in the Post-War World, The Making of the 20th Century,* (Palgrave, 1988).
[63] Ibid.
[64] Saul, supra note 62.
[65] Bourne, supra note 35, at p. 223.
[66] See generally Marius Deeb, *Syrian, Iran, and Hezbollah: The Unholy Alliance and Its War on Lebanon*, (Hoover Institution Press, 2013).

responsible.[67] This led to an increase of contemporary domestic terrorism manifesting in the United States, with Islamic militants eventually bombing the World Trade Centre in 1993. Such calamities provide evidence that terrorism is no longer confined to regional areas core to extremism, but instead the launch of targeted attacks beyond immediate states has led to the globalisation of terrorism as an international phenomenon.

Furthermore, the events of 9/11 illustrated the damage and violence caused by terrorism and has had a profound impact on international security. Since then, there has been an abundance of terrorist attacks. The Bali bombings in Indonesia in 2002, the Madrid bombings on public trains in 2003, and the suicide bombings in London in 2005 are only some examples of increasing large-scale terrorist operations. More recently, the London Bridge attacks and the bomb attacks in Barcelona both in 2017 are notable cases that illustrate the persistence of violent terrorism today.

From the discussion above, it can be said that terrorism is an act of political violence that is not limited by any means nor is it bound to any particular practice. In any case, terrorism been described as a 'special form of violence'.[68] One of the common elements defining terrorism is the need to create fear and terror in the general public, which explains why acts of terrorism are normally carried out within the community and involves some degree of violence. Unlike conventional warfare, terrorism is not facilitated by specific methods such as militancy (though it can certainly take this form). Instead, terrorism adapts itself to various forms of execution in order to achieve its purposes. This is evident in the range of counterterrorism treaties that pertain to specific weaponry use rather than having a general application to the crime of terrorism. For this reason, terrorism has acquired no universal definition to clarify its nature in absolute, at least, not in a formal sense.

4.2 Terrorism as a Threat to Negative and Positive Peace

There is no doubt that terrorism is a contemporary threat to international peace and security. More specifically, terrorism is a threat to both aspects of Galtung's theory of peace. Terrorism causes both direct and structural violence and hinders the achievement of positive and negative peace, thereby justifying the need to prevent international terrorism in all its forms, including OCTAs.

Galtung's theory of peace emphasises the absence of direct violence as the necessary condition to achieving negative peace. In other words, terrorism affects the achievement of peace if it can be shown to cause direct violence to the state. Terrorism ordinarily takes place during peacetime as

[67] See for example Michael Plachta, 'The Lockerbie Case: The Role of the Security Council in Enforcing the Principle Aut Dedere Aut Judicare', *EJIL* Vol. 12 No. 1, 125-140 (2001).
[68] Paul Wilkinson, 'Terrorism', in ed. Dunn Cavelty and Victor Mauer, The Routledge Handbook of Security Studies, Routledge, (2010) at p. 126.

isolated incidents of violence, where violence is committed by those affiliated with a terrorist group acting alone or that do not form part of any wider conflict. Terrorism can also be used as a tactic to support armed conflict which can develop into violence comparable to the likes of guerrilla warfare. Thus, the potential for terrorist conflict to develop into violence in the form of warfare is a very real threat, of which a prime example is the ongoing Syrian Civil War.[69] The escalation of violence and the growing division of factions and emergence of rebel groups has now descended into a 'full-scale civil war'[70] in Iraq and Syria, which is primarily being led by ISIS.[71] The terrorist violence in Syria has contributed towards the invocation of civil war through the use of direct violence that has resulted in a great number of deaths and injuries since its inception in 2011.[72] The achievement of negative peace in the absence of direct violence is threatened by terrorism because of its capacity to produce direct violent conflict and perpetuate civil war. For states like Syria then, efforts to secure negative peace are an essential step in moving towards a stable and peaceful state.

Equally, the failure of institutions can cause the upheaval of political, social or economic conditions and subsequently, lead to chaos and disorder. When state institutions fail to function adequately, violence, conflict and anarchy are the prevailing consequences that pollute the peace. In turn, this creates obstructions to social equality where human society struggles to flourish. As such, acts of terrorism can amount to 'interpersonal violence', finding its roots in institutional and structural violence.[73] Social 'inequality and injustice' can also result from the evolution of conditions resulting from terrorist conflict. In the face of anarchy, the condition of the state directly contrasts with peace and stability and the achievement of positive conditions that enables equality for humanity. Government failures further propel the state into civil unrest and generate violent behaviour, particularly where the use of law enforcement authorities become an instrument of violence used against the people. This is the case in states such as Iraq, Afghanistan, Libya and Somalia, which are similarly affected by civil war and terrorism as a result of political unrest. States suffering from civil unrest struggle to address structural violence like hunger, exploitation, corruption, malnutrition and so forth, because they lack the resources to do so. The presence of positive peace is thus a challenging

[69] Martin Koskenniemi, *The Politics of International Law*, (Hart Publishing, 2011) at p. 83. The author alludes to Agenda for Peace (UN Report 1992) which establishes that *'the greatest proportion of large-scale violence that presents a threat to international peace and security is home-brewed violence – civil war'.*

[70] See e.g. BBC News Article, 'Syria: The Story of the Conflict', (11 March 2016). Available at http://www.bbc.co.uk/news/world-middle-east-26116868 (accessed 28 September 2017).

[71] See e.g., Michael P. Scharf, 'How the War Against ISIS Changed International Law', *Case Western Reserve Journal of Int'l Law 48*, (2016); BBC News, 'Islamic State and the Crisis in Iraq and Syria in Maps' (21 September 2017). Available at http://www.bbc.co.uk/news/world-middle-east-27838034 (accessed 28 September 2017).

[72] BBC News, 'Syria War: New US Sanctions Target Assad Government's Foreign Backers', (17 June 2020). Available at https://www.bbc.co.uk/news/world-middle-east-53076994 (accessed 7 July 2020). The death toll has been reported as *'more than 380, 000'* people since 2011.

[73] Esther Madriz, 'Terrorism and Structural violence', *Social Justice, Vol. 28, No. 3 (85), Law, Order, and Neoliberalism*, (Fall 2001) pp. 45 – 46, at p. 45.

condition to obtain and maintain especially when the state is shrouded with instability.[74] Particularly when the objective of terrorism is the 'intent to cause death' and provoke a state of terror,[75] the creation of peace cannot be free from instability or direct violence as long as terrorism exists in a society.

Terrorism challenges both sides of the peace theory. If peace is the absence of structural violence and structural violence includes terrorism, then terrorism affects the achievement of peace. Acts of terrorism thus explicitly hinder the effective safeguarding of the civil society by threatening the ability for human survival, thereby amounting to structural violence. Accordingly, terrorism must be subject to rules of prevention under international law in order to achieve both positive and negative peace.

V. Cyberterrorism: OCTAs as a Threat to International Peace and Security

Terrorist groups are increasingly exploiting new technologies to commit malicious activities. The advent of cyberspace and cyber technology has become a new and novel platform for which terrorists are able to conduct a range of malicious operations. Specifically, OCTAs as preparatory activities of terrorist groups, facilitate the commission of ultimate terrorist violence that must be subject to both prevention and suppression under international law. As discussed in Chapter 1, OCTAs can be both a part of terrorism and they can fall within the definition of terrorism. The following discussion explores how the theory of peace comes into play when assessing the law, discusses both types of OCTAs and how they affect the achievement of both negative and positive peace. I put forward a theory of peace that can be used to assess the adequacy of international law in dampening and suppressing OCTAs and, ultimately, to gauge whether this legal framework is sufficient to enable the international society to attain its overarching goal of maintaining international peace and security.

There is no doubt that OCTAs are a crucial component of terrorism. Not least are OCTAs enabled by cyberspace, the manifestation of one OCTA is directly the cause and effect of another. In this sense then, the relationship between cyber terrorist recruitment, financing and propaganda can be described as correlative. Without OCTAs, there are no recruits to conduct operations, there are no financial provisions to ensure operations can be carried out and terrorist groups cannot send foreign fighters to conflict zones and equip them with weapons for warfare. The production of terrorist propaganda is contingent upon the provision of resources and funds, the hiring of recruits relies on the dissemination of terrorist ideology through extensive social media campaigns, and the procurement of funds through the exploitation of cyber technology is not possible without skilled

[74] See Lawler, supra note 28, at p. 88.
[75] Security Council Resolution 1566, S/RES/1566, (8 October 2004)

recruits and sophisticated cyber capabilities of both members and computer equipment.[76] Therefore, the more money a terrorist organisation can raise, move and store without detection, the more resources the group can invest in and the greater the potential for operations to become violent and harmful. Each OCTA complements the other to the extent that the proliferation of cyber terrorist activities perpetuates the prospect of a large and violent terrorist operation to manifest, whether in cyberspace or on the ground. As such, direct (and indirect) violence can be caused by an act of terrorism that materialises as a result of OCTAs. This leads to the conclusion that with the continued proliferation and unregimented execution of OCTAs, a fertile ground is nurtured for terrorist groups to accomplish severe and catastrophic acts of terrorist violence in the future.

OCTAs can prohibit the achievement of negative peace by creating the ideal conditions for direct violence to materialise. Particularly, OCTAs that amount to acts of political violence such as incitement to terrorism. This is because OCTAs of this kind lead to the commission of terrorist violence and by doing so, directly obstruct the prevention of physical violence which is the required condition to attaining negative peace. Such OCTAs are so closely related to political violence that, if committed by a state, they would amount to an act of terrorism in and by themselves. OCTAs are the primary catalyst to ultimate terrorist violence and their role towards the commission of direct violence and conflict is a sustained campaign endorsed by terrorist groups such as ISIS. Throughout its social media campaigns and online propaganda, ISIS openly fosters a narrative instigating violence against its Western opposition by encouraging violent terrorism and openly supporting attacks.[77] The use of violence is therefore a principal tactic in ISIS' strategy that is a direct result of employing OCTAs as a means of creating violence against other states. Activities of cyber terrorist recruitment, financing and propaganda then form a crucial part of terrorism that can only be described as the ideal platform to propel and enable terrorist violence. As the starting point of violence and conflict initiated by terrorist groups, OCTAs can be said to hinder the achievement of negative peace. OCTAs sustain terrorism and provide terrorist groups with the means to become effective functioning organisations. Thus, absent of adequate legal address, OCTAs will continue to impede the creation of negative peace and subsequently, hinder the overall achievement of international peace and security.

[76] Maura Conway, 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism,* 40:1, 877-98, (2017), at p.80. The author describes the Internet as '*a single free online platform that can be employed for fund-raising, recruitment, information dissemination, and intra-group communications.'*; Yoram Schweitzer, Gabi Siboni and Einav Yogev, 'Cyberspace and Terrorist Organisations', *Military and Strategic Affairs,* Vol. 3, No. 3, (December 2011) at p. 42. The authors identify the main features that are fundamental to the functioning of terrorist organisations that can be carried out by cyberspace tools, which include propaganda, recruitment and training, fundraising and financing, communications and identifying targets and intelligence.
[77] Lisa Blaker, 'The Islamic State's Use of Online Social Media', *Military Cyber Affairs*, Vol. 1, Iss. 1, Article 4, (2015).

In addition to dealing with direct violence, an important part of creating the necessary conditions for Galtung's theory of peace relies on the absence of structural violence. In the context of international peace and security, positive peace is imperative to achieving the objectives of the international society. Eliminating structural violence is the first step to providing the ideal conditions for peaceful conditions. Threats to positive peace amount to aspects of a culture that can be used to legitimise structural violence and jeopardise the protection of a society against acts of violence. Thus, positive peace facilitates the integration of human society and seeks to promote the ability of individuals to flourish within that society. By tackling its causes and effects, positive peace provides a long-term remedy to achieving peace by offering the best protection against violence through establishing the ideal conditions for peace. OCTAs are the catalysts to violent terrorism and thus, their prevention should be paramount in the fight against terrorism and for the maintenance of international peace and security.

This includes OCTAs that do not amount to an act of terrorism, which can nevertheless pave the way for terrorist violence by providing sustenance to terrorist groups. As the building blocks to terrorism, such OCTAs may involve recruiting individuals from internet chat rooms, sharing ISIS propaganda online or setting up a charity website to acquire donations for terrorism. OCTAs of this sort can cause structural violence by inflicting suffering in marginalised sectors and by precluding the creation of equal opportunities within the society. To demonstrate, the process of recruitment can involve the indoctrination of vulnerable individuals to beliefs or values that are core to a terrorist group. Typically, these individuals may feel isolated and that they do not fit in within their own communities, which leads them to believe that joining a terrorist group provides them with a sense of belonging. Acceptance into a terrorist group in turn, causes the individual to suffer from marginalisation of the community they came from and can subject them to unequal life chances as a result.

As has been noted, structural violence is a result of the unequal distribution of power among actors where that inequality derives from the actions of human agency. Terrorist groups conducting OCTAs can be said to foster a systemic nature of violence by causing economic and social inequalities that are then built within the structure of a society and thus, breed harmful conditions. Cyber terrorist recruitment and propaganda can often be seen to target vulnerable individuals and women, where these members of society can be prone to systematic oppression and repressive state structures.[78] To add to this, structural violence can result from developing country debt and unfair economic relations that result in terrorist groups targeting the wealth or economic resources of specific groups or

[78] Dekker, supra note 20.

institutions through OCTAs in order to reinstate social balance in the dichotomy.[79] Given this, terrorists' exploitation of cyberspace for the purposes of OCTAs has significant and detrimental impacts on the achievement of positive peace.

As Galtung's theory of peace has shown, structural violence can and does lead to the occurrence of direct violence.[80] Structural violence can provoke direct violence, specifically where terrorism seeks to achieve economic, social and political change through violence. Since OCTAs can cause structural violence, they have a serious potential to lead to a direct act of violent terrorism. Put simply, OCTAs depend on and perpetuate the potential for political violence caused by terrorism. Positive peace provides the necessary conditions to create negative peace because war, armed conflict and political violence result from the absence of positive peace. Therefore, direct violence cannot be prevented unless the root causes of structural violence that engenders it are removed. This means that achieving both conditions of peace are contingent upon the deterrence of cyber terrorist recruitment, financing and propaganda to ensure violent terrorism cannot materialise as a result of these OCTAs. If negative peace involves the absence of direct violence and positive peace involves the absence of structural violence, then violence resulting from terrorism is not possible without the prevention and suppression of OCTAs. In accordance with Galtung's theory then, OCTAs sustain terrorist violence and prevent the conditions of peace from being achieved both negatively and positively.

In light of the above, international law must consider OCTAs as a means employed by terrorist groups to achieve violent ends. As acts of political violence, OCTAs are malicious tasks that are vital to the effective functioning of terrorist groups and that continue to perpetuate international terrorism today. Given that the concept of terrorism encapsulates a vast idea 'beyond the mere physical, sectoral acts comprising terrorism',[81] measures to counter terrorism must take heed at the origins of its creation. Countering terrorism must first address the activities and operations that enable terrorist groups to perform violent acts. The perpetuation of OCTAs is a driving force which sustains the survival and success of terrorist groups. With this in mind, the fight against international terrorism must directly tackle OCTAs as the primary and principal catalysts to terrorist violence.

VI. Conclusion

The maintenance of international peace and security is a key objective of the international community and international law is critical to achieving this objective. Through legal rules, principles and norms, states are bound to obligations that enforce these values through restricting or permitting certain

[79] Galtung, supra note 1.
[80] Ibid.
[81] Ben Saul, *Defining Terrorism in International Law*, (OUP, 2006), at p. 27

state behaviour. In order to achieve the conditions to peace then, states must endeavour to ensure the prevention of direct violence and structural violence. Direct violence is no longer the prevailing obstacle to achieving peace. Nevertheless, terrorism pervades the security agenda as a primary threat to both negative and positive peace because it has the potential to cause both direct and structural violence. Given that terrorist groups exploit cyberspace for the means of recruitment, financing and propaganda purposes, there is a need to prevent and suppress OCTAs as a primary means to countering international terrorism.

This chapter has situated OCTAs within the framework of international peace and security. In doing so, this chapter has explored Galtung's theory of peace in both negative and positive concepts, as well as the notion of security and how both conditions can be achieved by international law. Analysis has drawn attention to the significance of international legal rules and states' adherence to such rules for the purpose of achieving community objectives. This chapter has shown the utility of international law in ensuring the protection of norms and values as well as the safeguarding of international legal rights of states through treaty law, UN resolutions and customary law. Discussion has presented an overview of the evolution of modern terrorism and discussed how terrorism constitutes a threat to achieving international peace and security. Lastly, this chapter has explored OCTAs as part of cyberterrorism and how they too endanger international peace and security.

Accordingly, the following chapter addresses the legal responses of both international and regional conventions and treaties in order to assess their adequacy at preventing OCTAs as part of the current measures of counterterrorism under international law.

Chapter Three

OCTAS IN INTERNATIONAL AND REGIONAL TREATY LAW

I. Introduction

As we have seen in previous chapters, OCTAs are central to the core functioning of terrorist groups and they must be seen as primary and principal acts of cyberterrorism that constitute a threat to international peace and security. As such, the international community looks to and expects international law to regulate this type of activity. However, at present, states have failed to develop direct and specific international legal rules regulating terrorist's use of the internet. Accepting this, the following discussion explores available legal regimes in the form of regional treaties addressing cybercrimes and cyber offences to determine if these legal frameworks can be harnessed to regulate and suppress OCTAs under international law.

This chapter examines three regional treaties: the Convention on Cybercrime (Budapest Convention) (2001),[1] the African Union Convention on Cybersecurity and Personal Data Protection (2014),[2] and the Arab Convention on Combating Information Technology Offences (2010).[3] Using the general rules of treaty interpretation deriving from the Vienna Convention on the Law of Treaties 1969,[4] analysis of these conventions will be explored in light of each OCTA; recruitment, financing and propaganda. The following discussion refers to tangible cases of cyberterrorism and uses these reported incidents to evaluate whether the current regulations that are in place for certain regions can be interpreted to apply to OCTAs on an international level. What emerges is a view that these three regional treaties offer some – albeit – limited guidance on the regulation of OCTAs.

II. Regional Treaties and their Interpretation

The three regional treaties that are central to this discussion include the Budapest Convention, the AU Convention and the Arab Convention. This research examines the aforementioned three treaties based on their relevancy and scope in addressing OCTAs. Whilst their regional application may appear to pose some limitations to their practical relevance, these three treaties are nonetheless a stellar demonstration of how prospective cyber terrorism treaties could be drafted and casts a light on the manner and scope in which provisions should be articulated to ensure the prevention of OCTAs. Thus,

[1] Council of Europe, Convention on Cybercrime, ETS No. 185 (November 23, 2001). Hereinafter referred to as the Budapest Convention.
[2] African Union Convention on Cybersecurity and Personal Data Protection (2014). Hereinafter referred to as the AU Convention.
[3] Arab Convention on Combating Information Technology Offences (2010). Hereinafter referred to as the Arab Convention.
[4] Vienna Convention on the Law of Treaties 1969. Hereinafter referred to as 'VCLT'.

the following section discusses the nature of these regional conventions, why they have been selected, and outlines the method according to which they will be interpreted.

2.1. Budapest Convention

The Budapest Convention is imperative to the study because it is the first international treaty of its kind that pertains to offences committed via the use of cyberspace. Whilst all three treaties are region specific, the Budapest Convention applies to states beyond the European region, and which are not party to the Council of Europe. For example, the US, Japan and South Africa are signatories to the Convention despite not being members of the EU.[5] For this reason, the Budapest Convention comes closest to acting as an international treaty for cybercrimes and computer-related offences within international law. It remains the only binding international instrument on this issue and serves as guidance for states developing national legislation against cybercrime. As set out in the preamble, the primary objective of the Budapest Convention is to pursue *'a common criminal policy aimed at the protection of society against cybercrime'*.[6] This means that states must adopt criminal laws that prohibit certain types of conduct committed using cyber technology as laid out in the Convention. Thus, the instrument is an effort to harmonise national laws and to provide a framework for international cooperation as it pertains to cybercrimes.

The Budapest Convention concerns the criminalisation of computer-based acts that involve the misuse of computer data, the computer system, or both. The range of offences prohibited under the Convention includes illegal access, illegal interception, data interference, system interference, the misuse of devices, and computer related forgery and fraud.[7] These offences are listed under Articles 2-8, forming the substantive provisions that concern computer-related offences under the Convention.[8] Alongside its substantive provisions criminalising the misuse of cyberspace, there are several additional texts to support the Budapest Convention and these can be used to aid or otherwise assist our understanding of this agreement.

The Budapest Convention contains an Explanatory Report, which elaborates upon the nature of each offence and extends our understanding on the scope of each provision and how they may be interpreted. The Budapest Convention is also accompanied by several Guidance Notes that relate to

[5] See Council of Europe, 'Charts of Signatures and Ratifications of Treaty 185 (Status as of 28/02/2021), available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=vI0e9aDG
[6] Preamble of the Convention on Cybercrime, 2001.
[7] Articles 2-8 of the Convention on Cybercrime (2001) respectively.
[8] Other substantive provisions range from Articles 9 – 13 which concern offences related to child pornography, offences related to infringements of copyrights and related rights, attempt and aiding or abetting, corporate liability, sanctions and measures. These provisions fall outside the scope of this chapter's analysis, which is reserved predominantly for computer-related offences.

different contexts in which cybercrimes may be committed.[9] In particular, Guidance Note 11 is central to the discussion because it directly refers to cybercrimes committed for the purposes of terrorism. Alongside its significance for the following analysis, it also provides some indication that when drafting the Convention, the Cybercrime Convention Committee anticipated that offences committed via the use of cyberspace could be carried out for terrorist purposes or by terrorist groups.

It is important to note however, that the Explanatory Note and the Guidance Notes are not legal instruments, with the preamble to the Explanatory Report clearly stating that it is not binding. Nonetheless, their addition to the Convention serves as a useful tool when interpreting its substantive provisions.[10] Further analysis of supplementary texts is found within the Additional Protocol to the Convention Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems.[11]

Though the Additional Protocol is a subsidiary agreement which states have no obligation to ratify, it remains a binding legal text for signatory states made by the Council of Europe, which can aid and assist in the interpretation of the Convention.[12] In light of this, reference to the Additional Protocol, alongside both the Explanatory Report and the Guidance Note will be made throughout the following analysis in order to enhance our understanding and determine the applicability of the Budapest Convention to regulate OCTAs under the current legal regime.

2.2. AU Convention

The African Union Convention on Cybersecurity and Personal Data (2011) forms one of the three treaties that are core to the analysis due to its region wide span to states in the African region. The drafting of this treaty relied on the Convention on Cybercrime, which means various provisions are mapped from the former and the AU Convention constructs very similar norms for global cybersecurity and the types of activities that constitute criminal offences.[13] The distinguishing part,

[9] There is a total of 11 Guidance Notes issued alongside the Budapest Convention which all concern different matters. For example, Guidance Note #1 relates to 'Computer System', Guidance Note #2 relates to Botnets and Guidance Note #3 refers to Transborder Access (Article 32) etc. Reference to these Guidance Notes can be found on the Council of Europe website, 'Guidance Notes' available at https://www.coe.int/en/web/cybercrime/guidance-notes

[10] The preamble of the Explanatory Report states that '*the text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions contained therein'.* Convention on Cybercrime, ETS No. 185 (November 23, 2001).

[11] Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189 (Strasbourg, 28.I.2003).

[12] The Additional Protocol has been ratified by 32 states at the time of this writing (May 2019). See Council of Europe, Chart of Signatures and Ratifications of Treaty 189, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=JQOolQVB

[13] Both Conventions construct very similar norms for global cybersecurity and the types of activities that constitute criminal offences. See GLACY+ report, Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime, 20 November 2016 at p. 8.

however, is that the African Union Convention has been ratified by very few states in the region (8 out of 55 AU member states)[14] especially as compared to its predecessor. The object and purpose of the AU Convention is 'to provide the necessary security and legal framework for the emergence of the knowledge economy in Africa'.[15] The AU Convention also states that:

> the goal of this Convention is to address the need for harmonized legislation in the area of cyber security in Member States of the African Union, and to establish in each State party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use.[16]

The AU Convention stipulates the type of cyber offences that state parties must condemn upon the implementation of these provisions into domestic cybercrime legislation. Under Article 29, these offences include attacks on computer systems, computerised data breaches, content-related offences and offences relating to electronic message security measures.[17] The main aim of both Article 29(1) and (2) is to condemn the unauthorised access into a computer system, causing the malfunctioning of a computer system and the alteration of computer data. Under Article 29(3), the AU Convention concerns content related offences that include both child pornography and offences relating to racism or xenophobia, as well as cyber offences concerning genocide and crimes against humanity.

Furthermore, commitment to cybersecurity initiatives is reported as low for African states.[18] The lack of resilience in cybersecurity frameworks is apparent for the African region and urgency to protect cyber infrastructure or personal data seems lacking. The gap in national cyber response mechanisms means there is great potential for harmful cyber offences to materialise and cause serious consequences for African countries. In light of this, the African Union Convention forms a key part of the analysis to determine whether this treaty considers cyberterrorism and, more specifically, OCTAs as a threat to the national security of African states and, if so, how this is dealt with within the treaty.

2.3 Arab Convention

The Arab Convention on Combating Information Technology Offences (2010) is the third and final treaty that forms part of the following analysis in this chapter. This treaty has been selected because it is one of the leading treaties against cyber technology offences within the Arab region and within the domain of regional cybercrime legislation. The Arab Convention contains a range of offences

[14] African Union Convention on Cyber Security and Personal Data Status List. Available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

[15] Preamble of The African Union Convention on Cybersecurity and Personal Data Protection (2014), p. 2.

[16] Ibid.

[17] Article 29(1)-(4) of the AU Convention, 2014.

[18] ITU Publication, Global Cybersecurity Index (GCI) 2018, at p. 18. Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

relating to information technology. The Convention limits its application only to state parties within the Arab region and thus, has limited application. The object and purpose of the Arab Convention is identified under Article 1 as follows:

> The purpose of this Convention is to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individual.[19]

The cyber offences outlined by Articles 6-18 of the Arab Convention include: illicit access, illicit interception, integrity of data, misuse of information technology means, forgery, fraud, pornography, privacy, terrorism, organized crime, copyright, and electronic payment tools. Of particular significance, the Arab Convention dedicates a specific provision relating to terrorism under Article 15 which explicitly condemns the use of information technology for specific terrorist purposes. This starkly contrasts with the Budapest Convention and the AU Convention, in which neither contain any reference in their substantive provisions to criminalise cyber offences concerning terrorism. This makes for particularly interesting analysis when it comes to interpreting whether the language of the provisions can be construed to apply to OCTAs. The inclusion of a terrorism specific provision indicates that the Arab region anticipates the use of cyber technology for terrorist purposes as a conceivable offence that requires legislating against. Therefore, the Arab Convention should form part of the following analysis when it comes to determining if regional provisions can be applied to cyber terrorist activities in the form of OCTAs.

2.4 Nature of Regional Cybercrime Treaty Obligations

In the realm of cybercrime, treaties have predominantly focused on implementing domestic cybercrime laws rather than establishing any cybersecurity standards. The Budapest Convention, the AU Convention and the Arab Convention as well as other regional cybercrime conventions emphasize this view, and arguably act as *opinio juris* to reflect the fact that states are willing to adopt and enforce cybercrime laws within their territories.[20] Cybercrime conventions encourage states to engage in international and regional cooperation, to eliminate both cybercrime and implement measures to prosecute cybercriminals. It is clear that there is a growing international consensus regarding cybercrime and that it is an international obligation for states to develop domestic cybercrime laws

[19] Article 1 of the Arab Convention, 2010.
[20] Other regional cybercrime treaties include The Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information (CIS Agreement) (2001); The Shanghai Cooperation Organisation Agreement (2009); The Organisation of American States (OAS) Comprehensive Inter-American Cybersecurity Strategy (2004).

where possible so as to prevent the misuse of technology and attempt to harmonise national laws across all states.[21]

The Budapest Convention is of pan-regional application and operates as the main cybercrime treaty in existence, whereas the AU Convention and the Arab Convention apply only to their respective regions. Irrespective, substantive provisions that may govern on matters relating to cyberterrorism remain of great use in the subsequent analysis of current cybercrime law. Therefore, the following discussion is an interpretive exercise that alludes to the general application of regional treaties and the pertinence of certain provisions when it comes to determining whether and to what extent OCTAs are addressed under international law.

2.5 General Rule of Interpretation

In order to interpret the provisions of these Conventions, a consistent method of interpretation must be employed throughout the analysis. This can be found under Article 31(1) of the VCLT, which sets out the general rule of interpretation. Forming part of customary international law, the provision holds that:

> A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose.[22]

The general rule encompasses all of the elements that form Article 31(1) and, though the starting point is an examination of the ordinary meaning of the provision first,[23] this must be performed in light of the object and purpose of the treaty as a whole.[24] According to Article 31(2) of the Vienna Convention, interpretation of the legal provision in question can incorporate reference to both preambles and annexes, as well as:

> (a) Any agreement relating to the treaty which was made between all the parties in connexion with the conclusion of the treaty
>
> (b) Any instrument which was made by one of more parties in connexion with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty.[25]

---

[21] See Scott J. Shackelford, Scott Russell and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors', *Chicago Journal of Int'l Law*: Vol 17, No. 1, Article 1 (2016), at p. 5 – 7.

[22] Article 31(1) of the VCLT, 1969.

[23] The general rule arguably begins with the element of 'good faith' that often correlates with the principle of 'effectiveness'. This chapter does not engage in the analytical discussion of good faith on the basis that its formation towards the general rule will not be assumed in the negative, that is, bad faith unless otherwise proven. For a detailed discussion into the meaning of good faith see Richard Gardiner, *Treaty Interpretation*, (2nd Ed, OUP, 2017) at 167-181.

[24] See JG Merrills, 'Two Approaches to Treaty Interpretation', 57 *Australian Yearbook of International Law* (1968) at 57. The author states that: *'The whole tenor of Article 31 makes it clear that the terms of a treaty are to be interpreted in the light of the treaty as a whole and the other factors mentioned in Article 31'.*

[25] Article 31(2) of the VCLT, 1969.

Neither the AU Convention nor the Arab Convention attaches with it any supplementary documents that can further our understanding of their substantive criminal provisions. However, the Additional Protocol attached to the Budapest Convention is an example of Article 31(2)(b), which forms part of the interpretive process to analyse whether the Convention can be applied to OCTAs.

The general rule must also take into account any subsequent agreements or subsequent practice which forms part of the contextual element to interpretation.[26] Altogether, taking into consideration the different components of Article 31 will allow for a deeper understanding of the relevant treaty provisions and their meaning in the following discussion. Since the conventions in this discussion refer to cybercrime rather than cyberterrorism, using Article 31 VCLT will allow for a consistent interpretation of the provisions and to determine whether they can be construed to regulate OCTAs.

2.6 Other Conventions That Were Not Selected

In light of the above discussion, it is worth acknowledging other conventions that were omitted from this study. Specifically, the International Convention for the Suppression of the Financing of Terrorism (1999)[27] and the Convention against Transnational Organised Crime (2000).[28]

The UN's International Convention for the Suppression of the Financing of Terrorism is a significant development in the field of counter-terrorism legislation and arguably, a leading treaty concerning terrorist financing. For this reason, it may be contended that this convention should form part of the following analysis to determine its application to prevent OCTAs. However, there are various limitations of the convention that justifies its exclusion from the core analysis.

First and foremost, the Convention for the Suppression of Financing applies only to acts of terrorist financing that lead to death or injury. The Convention defines the crime of terrorist financing as an offence that is committed by 'any person' who 'by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out' an act 'intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict…'.[29] This definition supposes that the act of terrorist financing in question is intrinsically linked to an impending act of violent terrorism and that its purpose is dedicated to

[26] Article 31(3)(a) and (b) of the VCLT, 1969.
[27] International Convention for the Suppression of the Financing of Terrorism, opened for signature 9 December 1999, 2178 ILM 229. Adopted by the General Assembly of the United Nations in Resolution 54/109 of 9 December 1999.
[28] United Nations Convention against Transnational Organised Crime (2000) adopted by General Assembly resolution 55/25 of 15 November 2000.
[29] Article 2 (1) of The International Convention for the Suppression of the Financing of Terrorism, opened for signature 9 December 1999, 2178 ILM 229.

causing death or serious injury. This, however, may not necessarily be the case. There are various terrorist financing operations that are not intended to cause immediate death or injury, but instead, are intended to support other functions of a terrorist organisation such as recruiting specialised individuals to carry out cyber tasks or funding the training of recruits. Equally, terrorist financing is essential to the lifeline of a terrorist organisation, with the provision of funds allowing it to maintain and carry out daily functions. Thus, it is pertinent to recognise that acquiring funds is not particular to the preparation of a violent terrorist attack but rather quotidian to the survival of the organisation and its functioning. In short, terrorist financing does not always lead to death or injury neither can a nexus be easily established in order to trigger Article 2 of the Convention. As such, regulating acts of terrorist financing should not be limited to instances where such nexus is required. In light of this, the Convention for the Suppression of Terrorist Financing will not be explored in the following analysis because it does not encompass acts that do not lead to death or injury but could still be perceived as terrorist acts.

Secondly, the Convention does not have a sufficiently broad scope of application to capture all activities defined under the term OCTAs. The Convention applies only to terrorist financing and cannot be interpreted to encompass any other OCTAs. Whilst the Convention is a considerable international effort to harmonise the regulation of the financing of terrorism by criminalising acts which can be shown to lead to death or injury, its parameters are confined to this one OCTA alone. Thus, it can be argued that the scope of the Convention is less broad than Resolution 1373 (2001), of which the latter applies exclusively to all acts of terrorism.[30]

For these reasons, the UN's International Convention for the Suppression of the Financing of Terrorism will not form part of the following discussion to determine whether it can be applied to OCTAs.

The UN's Convention against Transnational Organised Crime (2000) is another treaty that some may argue could form part of the analysis in this Chapter.[31] This Convention is ratified almost universally, encompassing 190 states that have agreed to promote cooperation to prevent and combat transnational organised crime more effectively. Most importantly, Articles 5 and 6 cover offences involving the participation in a criminal organisation and the involvement in money laundering.[32] These could be seen as relevant provisions in which to determine the applicability of the

[30] The scope and nature of Resolution 1373 (2001) is discussed in depth in Chapter 4.
[31] Supra note 8.
[32] Article 5(1)(a)(i) makes it a criminal offence to '[agree] with one or more other persons to commit a serious crime for a purpose relating directly or indirectly to the obtaining of a financial or other material benefit and, where required by domestic law, involving an act undertaken by one of the participants in furtherance of the agreement or involving an organised criminal group'. Article 6(1)(a)(i) makes it a criminal offence to '[convert or transfer property], knowing that such

Convention to prevent OCTAs. Whilst this may be the case, a prevailing limitation of the Convention is that it applies to private crimes committed by individuals. This directly contrasts with the objective of this study and the purpose of Chapter which is to determine whether regional treaties can be interpreted to prevent and suppress OCTAs in light of states' obligations. It is also a matter of contention as to what constitutes an organised criminal group and whether the definition proposed by the Convention lacks clarity and impartiality. Under Article 2, the Convention defines an organised criminal group as 'a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes of offense established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit'.[33] There remain controversies over definitional limitations including questions as to what is considered a structured group? How long is a period of time? What constitutes a serious crime? The ambiguity over the definition of organised criminal group therefore poses various issues as to the interpretive process of applying the provisions and the overall characterisations of offences under this Convention. In essence, the Convention poses more questions than it answers. For these reasons, the Convention against Transnational Organised Crime does not form part of the following analysis.

III. Cyber Terrorist Recruitment

Terrorist groups such as ISIS and Al-Qaeda rely heavily on sympathisers and recruits to sustain their existence and enable them to achieve their goals and objectives. In particular, terrorist groups encourage people to join or otherwise support their organisations and activities. In this way, recruitment of members and sympathisers is critical to the function of terrorist groups. To do this, terrorist groups pursue individuals that show an interest in extremist views, target specific individuals for indoctrination as well as disseminate terrorist views and violent actions to the online population.[34] This may include obtaining data in the form of personal information, email addresses or usernames on social media and reaching out to targeted individuals that share mutual interests in support of terrorism.

Given this, it is necessary to see whether any of the aforementioned regional treaties address or can be interpreted to address cyber terrorist recruitment. To see whether the regional treaties can

property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action'.

[33] Article 2(a) of the Convention against Transnational Organised Crime.

[34] The working definition of OCTAs can be found in Chapter 1, constructed using Security Council Resolution 1566: '*Criminal acts, notably recruitment, funding or propaganda, committed using cyber space and / or cyber technology with the intent to provoke a state or terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisations to do or to abstain from doing any act… are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.*

apply, let us examine whether any of their provisions impose obligations on state parties condemning acts that may be related to cyber terrorist recruitment. The Budapest Convention shall be the starting point in this analysis.

3.1 Does the Budapest Convention Apply to Cyber Terrorist Recruitment?

Within the Budapest Convention, there exists no specific provision pertaining to cyber terrorist recruitment. The Convention does not discuss terrorism in its substantive provisions nor is terrorism mentioned in the Explanatory Report. However, it seems the Council of Europe foresees the possibility of cyber terrorist offences to materialise, and this is emphasized in Guidance Note 11.[35] As a supplementary text to the Convention, the Guidance Note depicts the type of terrorist activities that may be criminalised as a cyber offence under the Budapest Convention. In order to evaluate whether the Guidance Note may apply to cyber terrorist recruitment, let us first examine some instances where communication and information gathering are or can be carried out by terrorists.

One of the most prolific online terrorist recruiters is ISIS's Cyber Caliphate leader Junaid Hussain. Part of Hussain's online activity involved the recruitment of fighters and the spreading of propaganda through various of his own Twitter accounts that operated under another pseudonym.[36] Hussain's aim was to encourage people to join ISIS by posting prolifically on social media for recruits to join the Cyber Caliphate.[37] In doing so, his main activity involved a heavy use of social media to gather information and to interact with potential recruits online. Whilst this involved the use of cyber technology in the form of online multimedia outlets on the internet, whether such cyber terrorist recruitment necessitated the misuse of computer systems and computer data is less apparent. It is perhaps more plausible that sourcing recruits online predominantly requires diligent online behaviour to profile individuals that are suitable for the role.[38] Usually, obtaining access to this information is publicly

---

[35] The Council of Europe has produced numerous Guidance Notes attached to the Convention, which is *'aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in light of legal, policy and technological developments.'* See Council of Europe, T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention, (November 15, 2016), in the Introduction at p. 3.

[36] See e.g. Counterextremism Project, Junaid Hussain, which provides an overview of Hussain's profile detailing his alleged tweets in support of terrorist attacks and terrorism generally, available at https://www.counterextremism.com/extremists/junaid-hussain; John P. Carlin, 'Inside the Hunt for the World' Most Dangerous Terrorist: How a British Hacker Joined ISIS's Top Ranks and Launched A Deadly Global Cyber Plot', *Politico Magazine Online*, (21 November 2018) available at https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643; Kimiko de Freytas-Tamura, 'Junaid Hussain, ISIS Recruiter, Reported Killed in Airstrike', *The New York Times*, (August 27, 2015) available at https://www.nytimes.com/2015/08/28/world/middleeast/junaid-hussain-islamic-state-recruiter-killed.html

[37] Mark Hosenball 'British Hacker Linked to Attack On Pentagon Twitter Feed: Sources', *Reuters*, (January 14, 2015), available at https://www.reuters.com/article/us-cybersecurity-pentagon-cybercaliphate/british-hacker-linked-to-attack-on-pentagon-twitter-feed-sources-idUSKBN0KN00X20150114

[38] The main process involves trolling the Internet via chat rooms and forums to recruit members. See Maura Conway. 'Terrorism and the Internet: New Media – New Threat?' *Parliamentary Affairs*, Vol. 59, No. 2, 283-298 (2006) (at p. 290.

available through social media accounts or by virtue of joining online chatrooms or forums and as such, access to personal information can be easily obtained by a user on the relevant platform.

For the sake of analysis, however, let us say that cyber terrorist recruitment involves the deliberate intrusion into a computer system to obtain personal data such as an email address, through which the recruiter can then communicate and maintain contact with a potential recruit. By definition, an activity of this type constitutes a breach of Article 2 of the Convention which prohibits the offence of 'illegal access' by stipulating that:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.[39]

Guidance Note 11 relating to terrorism provides an example of illegal access and states that:

> A computer system may be illegally accessed to obtain personally identifiable information (e.g. information about government employees to target them for attack).[40]

To elaborate on the meaning of 'illegal access', it is necessary to apply the general rule of interpretation as per Article 31(1) VCLT. Article 2 of the Convention, read in conjunction with the Guidance Note, suggests that the offence requires an illegal trespass onto the computer system or part of it. This might be done by breaching security measures in order to gain information or to commit other forms of deceit or fraudulent behaviour using a computer. The Guidance Note uses personal data as an illustration of the type of information that a terrorist offence might involve and which breaches Article 2. Thus, gaining illegal access of a computer system in order to obtain personal data for the purposes of terrorism is the type of cyber offence envisioned by the Budapest Convention.

There are two distinct points to make from applying this provision to cyber terrorist recruitment. Firstly, the practical reality of requiring access to potential recruits as portrayed by the hypothesis above seems far-fetched. As said above, part of the recruitment process involves gathering information that may be taken from a range of public platforms that can be easily accessed by online users and so, accessing this information is done so legitimately and with great ease. For instance, searching social media sites such as Facebook or Instagram allows the browser to access any information which has been willingly published by the account holder in question. Social media sites can contain personal information such as date of birth, location, occupation, interests, extended

[39] Article 2 of the Convention on Cybercrime, (2001).
[40] Council of Europe, T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention, (November 15, 2016), in the Introduction at p. 4.

networks along with other valuable data which may be used as part of the terrorist recruitment process. Since online recruitment largely focuses on virtual communication, exchanges can often take place via social media through instant messaging or encrypted chats such as WhatsApp.[41] Not only does this remove the need for access without consent, but the ease of carrying out online recruitment accurately highlights the dangers posed by terrorists exploiting cyberspace and reiterates the need for international legal address.

Secondly, the Guidance Note hypothesizes computer-related offences carried out for the purposes of terrorism as incidents that involve a certain degree of damage and can arguably be classified as cyber-attacks. For example, Article 2 of the Guidance Note provides an example of illegal access committed for the purposes of terrorism as 'information about government employees to target them for attack'.[42] Article 4 postulates an incident of data interference involving 'a hospital's medical records … altered to be dangerously incorrect'.[43] Similarly, Article 6 provides an example of the misuse of devices whereby computer systems can be accessed to facilitate a terrorist attack, which 'can lead to damage to a country's electrical power grid'.[44] The Guidance Note appears to confine the scope of the Budapest Convention to cyber acts that intrude upon or interrupt a computer system and most notably, to result in some level of damage to its targets. In other words, the hypothetical examples of each offence as set out in the Guidance Note showcases scenarios which cause a consequential loss and has considerable impact to the intended target. This stipulation emphasizes the type of cyber offences that the Budapest Convention envisions, specifically incidents that cause detrimental effects beyond that of a mere or minor inconvenience.

Not only do these examples include targeted attacks against government personnel, but the Guidance Note also uses cyber-attacks against critical national infrastructure to reflect the type of cyber offences which are in contravention of the Budapest Convention. Cyber offences of this type are considered disruptive cyber intrusions that resemble cyber-attacks, such as the incidents between Russia and Georgia in 2008 and the Estonia cyber-attack in 2007.[45] Whilst neither the Convention nor

---

[41] See Javier Argomaniz, 'European Union responses to terrorist use of the Internet', *Cooperation and Conflict,* Vol. 50 (2), 250-268, 2015) at p. 253. Social media is a feature of the Internet which benefits terrorists and civilians alike, *'message forums, media material, and social networking sites such as Facebook or Twitter are also considered powerful tools for mobilisation and recruitment'.*

[42] Guidance Note 11, supra note 30.

[43] Ibid.

[44] Ibid.

[45] Used in conjunction with a kinetic attack, the cyber operation between Russia and Georgia in 2008 disrupted banking activities and limited communications between the Georgian government and its people. See The Telegraph, 'Georgia: Russia 'Conducting Cyber War', (Aug., 11, 2008), available at https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html; In 2007, Estonia experienced a cyber-attack on its government infrastructure, when a historical commemoration of a Russian solider was relocated to the dismay of Estonian Russians. The country then experienced a multitude of cyber-attacks, known as DDoS attacks, shutting down most critical websites, causing widespread social unrest and rioting among the

the Guidance Note elaborate on precisely what a cyber-attack might encompass, the examples used infer that a particular level of damage is necessary to constitute a breach under the Budapest Convention. The parameters of this scope are undefined; however, there is reason to believe that the Convention anticipates cyber offences to produce consequences that run parallel to those of cyber-attacks. At least, the examples presented in the Guidance Note support this view. Guidance Note 11 thus allow Member States to interpret and implement the Convention with a certain type of cyber offence in mind – that is, cyber-attacks. This said, to accede to such a presumption wholly discredits the possibility of the Budapest Convention to regulate OCTAs – or at least, cyber terrorist recruitment.

In light of its scope, Guidance Note 11 can be said to have an overriding normative value that strives towards peace. Since the Guidance Note stipulates against the use of cyberspace and cyber infrastructure for cyber terrorist attacks, the Note and thus the Convention perceives these activities as necessary of prevention for the purposes of protecting society against cybercrime. Whilst the preamble to the Convention on Cybercrime does not explicitly mention peace, its recognition of fostering international cooperation to prohibit cyber offences can speak to the general objective of ensuring national security within member states that ultimately ensures the maintenance of international peace and security. In particular, the prevention of cyber terrorist attacks can be seen to imply the preservation of both negative peace and positive peace. Cyber terrorist attacks can constitute a form of direct violence that impedes the achievement of negative peace. At the same time, hypothetical examples used in Guidance Note 11 can amount to structural violence because the offences include those directed against national systems that are crucial to daily life including public transport, banking systems or hospital infrastructures. It can be concluded from this that, within the sphere of emerging norms relating to the prevention of cyber terrorist offences, the Convention alongside its Guidance Note plays an important role in the achievement of both concepts of peace as stipulated by Galtung.

In any case, further examples from the Guidance Note appear to require some degree of computer proficiency to carry out a cyber offence as stipulated under the Budapest Convention. Whether it is the functioning of a computer system, the alteration of computer data or the damaging of either, the Guidance Note uses examples that require the manipulation of a computer system or computer data. Some advanced knowledge of a computer operating system might be presumed from the Guidance Note when it provides examples such as 'hindering the system that stores stock exchange records'[46]

country. See e.g. BBC News, 'Estonia Hit by 'Moscow Cyber War', (May 17, 2007), available at http://news.bbc.co.uk/1/hi/world/europe/6665145.stm (accessed 22 June 2018).

[46] Guidance Note 11, supra note 30.

or carrying out 'an attack on a country's banking system'.[47] In both these examples and most of the Guidance Note, the computer is posited as a target exploited by terrorists. Notwithstanding Articles 2 and 3 that use government individuals as the target of the cyber offence, Articles 4-8 concern critical national infrastructure as the target. The presumption then seems to be that the Budapest Convention applies exclusively to offences relating to the computer in which it is a target, and such a view seems to be further supported by the Guidance Note.

It is possible for a terrorist group to commit a sophisticated cyber intrusion in order to collect personal data belonging to individuals. For instance, terrorists may hack into a state-controlled data base and trespass without right in order to download sensitive personal data for the purposes of targeting government personnel. Whilst this is a plausible operation, measures of this scale are generally not used by terrorist groups when different ways of engaging recruits are more effective and less costly.[48] Not only are cyber intrusions complex, but the internet is predominantly used by terrorists for small-scale activities that require little cost and little technical knowledge.[49] Therefore, undertaking cyber terrorist recruitment does not require sophisticated use of cyber technology and neither does this seem necessary given that communication is the primary task. Recruitment is a terrorist activity that is enhanced by cyberspace, not to be mistaken as a terrorist operation that relies on technology for its execution. Notwithstanding Guidance Note 11, it might be concluded from this discussion that the Convention has an inherently restrictive capacity to engage with cyber offences that fall below a certain threshold of technical expertise when it comes to carrying out activities of cyber terrorist recruitment.

3.2 Does the African Union Convention Apply to Cyber Terrorist Recruitment?

The provision most relevant to the gathering of information by terrorists for the purposes of recruitment could concern the use of inauthentic data. Under Article 29(2)(b), it is an offence to:

> Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.[50]

[47] Ibid.
[48] Dominika Giantas, and Dimitrios Stergiou, 'From Terrorism to Cyber-Terrorism: The Case of ISIS', *Hellenic Institute of Strategic Studies*, (March 7, 2018). The authors discuss the exploitation of cyberspace by ISIS and highlight numerous practical advantages of using cyberspace as a new battlefield, recognising that terrorist groups may not need to use cyberspace to conduct cyber-attacks though this is still a threatening possibility that may happen in the future.
[49] See e.g. David Benson, 'Why The Internet Is Not Increasing Terrorism', *Security Studies*, 23:2, 293-328, (2014), at p. 301. The author contends that the use of the internet for *'cheap communication allows transnational groups to span greater distances, reach more people and form more diverse social networks for recruitment'*.
[50] Article 29(2) of the African Union Convention on Cyber Security and Personal Data Protection (2014).

For the AU Convention to apply to cyber terrorist recruitment, there must be a link between the computer data and the gathering of information for terrorist purposes. In order to prove a nexus between computer data and information required to carry out terrorist recruitment, the latter must be understood as a definition of the former. The AU Convention affirms this and provides a definition of 'computer data' to constitute 'any representation of facts, information or concepts in a form suitable for processing in a computer system'.[51] According to Article 29(2)(b), the next step is to show whether the information gathered for terrorist purposes has been altered, deleted or suppressed as part of the terrorist recruitment process.[52] In other words, the relevancy of the AU Convention rests on the finding that the information in question – relating to the terrorist recruitment process – has been subject to a computerised data breach. To understand the terms used in the provision in more detail, we must apply the general rule of interpretation under the VCLT.

Starting with the ordinary meaning, the provision stipulates that manipulation must result in 'inauthentic data'. A literal reading of the term infers that the data is not authentic, and that subsequent use of that data must be under the premise that it is believed to be authentic. Article 29(2)(b) thereby requires an intentional manipulation of data insofar that its manipulation is intended to deceive another as to the legality of that information. Taking into consideration the entire context of the provision, the offence stipulates that an intention to defraud or to exhibit dishonest intention can be a requisite upon implementation within domestic legislation. The provision centres around an element of deceit that forms part of the wrongful conduct, and it can be said that Article 29(2)(b) resembles a form of computer-related forgery that is a prohibited cybercrime.[53] The offence requires some level of disruption to a computer system whereby the information is manipulated insofar that it can be considered damage. To elaborate, the preamble of the AU Convention describes damage as:

> any impairment to the integrity or availability of data, a program, a system, or information.[54]

By altering information contained within a database, it is likely that the data would be considered as damage according to the preamble. The integrity of the information would be compromised, and its

[51] Article 1 of the African Union Convention on Cyber Security and Personal Data Protection (2014).
[52] Article 29(2)(b) of the African Union Convention on Cyber Security and Personal Data Protection (2014) states that it is a criminal offence to *'intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes…'*
[53] Article 29(2)(b) resembles Article 7 of the Budapest Convention. The latter concerns computer-related forgery and the provision states that *'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.'*
[54] Preamble of the AU Convention, 2014.

original content no longer preserved through the alteration. In other words, the data would be corrupt as a result of that very damage, thus contravening Article 29(2)(b) of the AU Convention.

There have been no reported incidents of computer-related forgery in relation to terrorism that has come under the scrutiny of international law. However, to find liability under the AU Convention hypothetical examples of OCTAs will be discussed. It is possible that a terrorist recruiter who is engaging with an underage and vulnerable young person may enter into a computer system without consent and change the age of a recruit in a database system to the legal age of 18. This may be for various reasons such as passing travel restrictions or forging identification for access. As part of the terrorist recruitment process, it may also be possible that a similar cyber offence could be committed to fictitiously change an individual's personal details such as their nationality, medical history, qualifications and so forth, where the false information is used as if it were authentic. In such cases, these OCTAs would amount to impairment of data and thus, fall within the scope of Article 29(2)(b) of the AU Convention.

There is reason to believe that this level of technical intrusion to obtain information for the purposes of terrorist recruitment might be unappealing given there are cheaper, more effective means of recruiting individuals. Moreover, there has not yet been a terrorist act that has required the same level of disruption carried out using cyberspace for terrorist recruitment. This said, terrorist recruitment that involves a computerised data breach is certainly possible and if committed, would impede the achievement of peace by virtue of threatening national security. Only if and when acts of terrorist recruitment demand the use of sophisticated cyber skills will their applicability under the AU Convention be satisfied both procedurally and substantively. Until then, the relevancy of computer-centric legislation in the discussion of counterterrorism measures relating to OCTAs may only be hypothesised at best. The more difficult question is whether terrorist groups will begin engaging the use of cyberspace for these exact purposes in the future.

3.3. Does the Arab Convention Apply to Cyber Terrorist Recruitment?

The Arab Convention makes specific reference to cyber offences related to terrorism under Article 15(2), which could be construed to apply to cyber terrorist recruitment. The provision states that the 'financing of and training for terrorist operations and facilitating communication between terrorist organisations' is an offence under the Arab Convention.[55] Different offences are concerned here, namely financing, training and communication of which only the latter may concern cyber terrorist recruitment. There are no provisions, preambular paragraphs or notes in the Arab Convention to

[55] Article 15(2) of the Arab Convention (2010).

define the act of facilitating communication between terrorist organisations. What is known is that such an offence must be committed by means of information technology and thus, through the use of cyberspace.

According to the textual approach mandated from the Vienna Convention, a literal interpretation of this provision is to understand the provision by reference to the text itself.[56] As such, a dictionary definition of the term may be useful to aid our understanding. To facilitate means:

> to make (an action, process etc.) easy or easier; to promote, help forward; to assist in bringing about (a particular end or result*).*[57]

Communication is described as:

> the transmission or exchange of information, knowledge, or ideas, by means of speech, writing, mechanical or electronic media, etc.[58]

A literal meaning of 'facilitating communication' can then be understood to mean making the exchange of information, knowledge, or ideas, or by means of speech, writing, mechanical or electronic media easy or easier or to promote such exchange of information. In other words, allowing contact to be made through different formats for the purposes of sharing information. This understanding is further supported by the United Nations Office on Drugs and Crime (UNODC) that has referred to 'facilitating communication between terrorists' as one function of terrorist organisations and identifying such activity as an offence.[59] Both the Arab Convention and the UNODC use this term to define the exchange of information among terrorists.

However, a point worth discussing is that the UNODC has similarly referred to this activity as '[facilitating] communication within terrorist organisations.' By using 'within', the UNODC infers that the exchange of information occurs among the same terrorist group or as part of it. On the contrary, facilitating communication *between* terrorist organisation implies that different terrorist groups are involved or that there is a point of separation between two objects. As we know, the role of communication within cyber terrorist recruitment refers to the exchange of information from the terrorist to the recruit. Whether that recruit is defined as being part of the same terrorist organisation and thus within that group, or whether the point of separation is defined as the terrorist and the

---

[56] Article 31(1) of the VCLT, 1969 states that *'A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose'.*

[57] Oxford English Dictionary definition of 'Facilitate', Entry I, available at http://www.oed.com/view/Entry/67460?redirectedFrom=facilitate#eid

[58] Oxford English Dictionary definition of 'Communication', Entry II. 5 (b) available at http://www.oed.com/view/Entry/37309?redirectedFrom=communication#eid

[59] See UNODC Website, 'Countering The Use of the Internet For Terrorist Purposes', available at https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html; see also UNODC, The Use of the Internet for Terrorist Purposes, (United Nations, 2012).

recruit and thus between that group, determines whether Article 15(2) could apply to cyber terrorist recruitment.

Let us illustrate the relevancy of the Arab Convention to the act of cyber terrorist recruitment using the case of Erick Jamal Hendrick as a point of reference. In the US, Hendrick was guilty of recruiting and training individuals to commit terrorist attacks in support of ISIS, which led to his arrest and sentencing to 15 years in prison.[60] He was liable for the attempt to 'provide material support to terrorists' after communicating with various individuals over social media.[61] Part of Hendricks' recruitment process involved sharing training materials through Twitter and other encrypted applications.[62] Such sharing of terrorist materials can be understood as an exchange of information through the use of technology as provided for in the above understanding of facilitating communication. The question remains as to whether Hendrick's communication to various individuals he wished to recruit for ISIS can be interpreted as facilitating communication *between* terrorist organisations. There is ground to argue in favour of this view. Firstly, it might be said that by exchanging information for the purposes of terrorism an association with a terrorist organisation can be presumed. Hendrick's dissemination of terrorist training materials reflects his support for ISIS. By supplying information that will provide the tools necessary for others to join the terrorist organisation, his affiliation to ISIS can be proven. Secondly, it could be argued that, irrespective of whether the association is within the group or between the group, any sort of affiliation with a terrorist organisation is sufficient to define the relationship as an offence under the Arab Convention.

The above example equally shows the scope of the Arab Convention in preventing terrorist activities that hinder the achievement of positive peace. Since Article 15(2) can be interpreted to apply to cyber terrorist recruitment, and the case of Erick Jamal Hendrick shows that his offence also involves the use of propaganda, it can be said that the Arab Convention prohibits the use of cyberspace for these OCTAs because they threaten the national security of states party to the Convention. What is particularly interesting is that the Arab Convention explicitly criminalises terrorist activities of this kind, which is significant in the context of preserving positive peace. The condemnation of these OCTAs demonstrates the intention of the Arab Convention to minimise the

[60] The United States Department of Justice, Department of Justice Office of Public Affairs, 'North Carolina Man Convicted of Attempting and Conspiring to Provide Material Support to ISIS', Press Release Number 18-336 (March 20, 2018) available at https://www.justice.gov/opa/pr/north-carolina-man-convicted-attempting-and-conspiring-provide-material-support-isis (accessed 4 June 2018).
[61] The Investigative Project on Terrorism, Sentencing Press Release, 'North Carolina Man Convicted of Attempting and Conspiring to Provide Material Support to ISIS', (February 4, 2019) available at https://www.investigativeproject.org/documents/case_docs/3895.pdf (accessed 4 June 2018).
[62] Eric Heisig, 'Ohio Jury Finds Man Guilty of Trying to Create ISIS-inspired Terrorist Cell in U.S.', Cleveland Online (March 20, 2018) available at https://www.cleveland.com/court-justice/2018/03/ohio_jury_finds_man_guilty_of.html (accessed 4 June 2018).

potential of creating conditions that would otherwise legitimise structural violence. In this sense then, the Arab Convention makes a concerted effort to strive towards achieving positive peace by eliminating possible threats to such conditions within its substantive provisions.

Whilst this interpretation allows for Article 15(2) to be applied to cyber terrorist recruitment, it is worthwhile pointing out that the Arab Convention is restricted only to states party to the agreement within the region. In any case, the Arab Convention identifies cyber terrorist recruitment as an offence which should be addressed within its regional convention and that a sufficiently broad interpretation of Article 15(2) in its ordinary meaning allows states to prohibit this OCTA within their domestic legislations.

The ability to use different social media platforms, to foster and maintain a relationship with targeted individuals and to continue to scout for new recruits is the crux of cyber terrorist recruitment. Whilst these activities cannot be undermined, their dependency on cyber technology is insubstantial. Particularly where recruitment for terrorism is interlinked with both financing and propaganda, subsequent analysis shall determine the cyber dependency of both activities and their interplay with the relevant regional conventions.

IV. Cyber Terrorist Financing

Cyber terrorist financing is the use of cyberspace or cyber technology to acquire funding for the purposes of terrorism. There are various ways in which terrorist groups can raise funds ranging from direct solicitation, e-commerce, the exploitation of online payment tools and through charitable organisations - all of which can be further exploited by criminal activity of terrorist groups.[63] This may involve the acquisition of funds through fraudulent means such as money laundering, identity theft, credit card theft and fraud of other financial assets.[64] Financing not only fuels the prosperity of a terrorist group, but its evolution through the means of cyber technology allows for the illicit acquisition of funds to be achieved in a multi-faceted way. Therefore, it is necessary to determine whether any of the regional conventions can prohibit cyber terrorist financing.

4.1 Does the Budapest Convention Apply to Cyber Terrorist Financing?

As we know, the substantive provisions of the Budapest Convention do not refer to terrorism neither do they refer to any instances of cyber terrorist financing. Whilst Guidance Note 11 relates directly to

[63] UNODC, The Use of the Internet for Terrorist Purposes, (United Nations, 2012), at p. 7.
[64] Ibid, at p. 7 para 15 states that *'online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud'.*

terrorism, its pertinence to the offence depends wholly on whether an association can be attributed between the cyber offence itself and the illicit acquisition of funds for terrorist purposes. Therefore, in order to interpret cyber terrorist financing in a manner consistent with the Budapest Convention, it must be shown that this OCTA is or at least, in part is a cyber-dependent offence.

To determine which provision can be best interpreted to apply to cyber terrorist financing, it is first necessary for the offence in question to concern the procurement of an economic or financial benefit. Article 8 concerning computer-related fraud seems most relevant, with the provision stating that:

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
>
> a) any input, alteration, deletion or suppression of computer data;
>
> b) any interference with the functioning of a computer system,
>
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.[65]

Though it does not make explicit mention of terrorism or terrorist financing, liability under Article 8 can be supposed on the instance that cyber terrorist financing committed through computer-related fraud for the purposes of producing a monetary gain is an offence under the Budapest Convention. The provision specifically mentions fraudulent behaviour as a method of gaining financial profit and the acquisition of which must be through either the misuse of a computer system or the wrongful modification of computer data. In order to define the relationship between computer-related fraud and terrorism, let us refer to Article 8 in Guidance Note 11:

> Computer data may be input, altered, deleted, or suppressed, and/or the function of a computer system may be interfered with, causing other persons to lose property (for example, an attack on a country's banking system can cause loss of property to a number of victims).[66]

Committing computer-related fraud can involve the manipulation of computer data alongside the performance capability of a computer system, which as a result, leads to the loss of property. Whilst Article 8 and the Guidance Note recognise financial loss as an example, it is necessary to interpret the scope of the provision and whether other types of loss can be considered. The Guidance Note stipulates the varying methods in which computer data can be manipulated inclusive of entering,

[65] Article 8 of the Convention on Cybercrime (2001).
[66] Council of Europe, T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention, (November 15, 2016), in the Introduction at p. 5.

amending, erasing or blocking data insofar that the computer system has been hampered. The consequence of this manipulation and interference must then cause the deprivation of property which must result in the acquisition of an advantage that is monetary. The breach of Article 8 is therefore conditional in that there must be a misuse of the computer data and that the computer data must cause a financial gain in order for the provision to be enforceable.

Even though the Guidance Note contextualises computer-related fraud in the nature of terrorism, the example provided emphasizes an offence constituting a cyber terrorist attack. However, it has been well versed that cyber terrorist financing and other OCTAs for that matter, are not cyber offences that produce equally high levels of disruption or destruction comparable to that of a cyber-attack. It can be said then that the Budapest Convention applies distinctly to a certain type of cyber offence and explicitly prohibits such threats to national security that may amount to large scale terrorist operations. Therefore, subsequent analysis explores the case of Younis Tsouli in order to determine whether it is possible and practical to apply Article 8 to acts of cyber terrorist financing.

Younis Tsouli posted several terrorist videos on various free websites online. As his terrorist activity proliferated online, he then *'*turned to sites with better technical capabilities*'*, which required him to pay for such services.[67] In order to do this, Tsouli acquired stolen credit card numbers through the Internet in order to raise funds for better websites.[68] By distributing emails containing viruses to thousands of users on online forums, Tsouli managed to access credit card details of numerous individuals he fraudulently scammed.[69] From these hundreds of transactions, he was then able to launder money which amounted to £1.6 million, all of which appeared to be legitimate.[70] Tsouli sent masses of fraudulent emails with unsolicited attachments (known as phishing) to deceive recipients into providing their personal financial details and to gain access to their money. The phishing emails enabled Tsouli to obtain economic benefits from which he then used to further his terrorist objectives. In using these funds, Tsouli and his co-conspirators were then able to set up websites to disseminate propaganda, circulate beheading videos and distribute bomb-making manuals online.[71]

Notwithstanding the offence of disseminating cyber terrorist propaganda, Tsouli's liability under the Budapest Convention stems from his illicit acquisition of funds through the fraudulent misuse of

[67] Michael Jacobson, 'Terrorist Financing and The Internet', *Studies in Conflict & Terrorism*, 33:4, 353-363 (2010) at 355.
[68] R v Tsouli (2007) EWCA (Crim) 3300. Tsouli was guilty for the *'conspiracy to murder, conspiracy to cause an explosion, conspiracy to obtain money by deception, fundraising and possession of articles for terrorist purposes.*
[69] See The Washington Post Online, Krebs, 'Terrorism's Hook Into Your Inbox', (July 5, 2007) available at http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html??noredirect=on (accessed 13 June 2018).
[70] UNODC, The Use of the Internet for Terrorist Purposes, (United Nations, 2012) at para 15.
[71] The Economist Online, 'Internet Jihad: A World Wide Web of Terror', (July 12, 2007) available at https://www.economist.com/briefing/2007/07/12/a-world-wide-web-of-terror (accessed 9 June 2018).

computer data. He intentionally distributed emails containing malware in order to retrieve sensitive information for economic gain, otherwise recognised as the crime of phishing. Whilst Guidance Note 11 does not refer specifically to this offence, another Guidance Note produced by the Committee of the Convention on Cybercrime pertains directly to identity theft and phishing. To determine whether the scope of Article 8 can be interpreted to include the cyber terrorist financing offence committed by Tsouli, let us explore the Guidance Note of the 8th and 9th Plenary by the Committee.

The Committee addresses the crime of phishing which it describes as a related act to identity theft and requires the perpetrator:

> to obtain password or other access credentials, often through email or fake websites.[72]

Tsouli's intentional distribution of emails that were infected with malware were spread for the purposes of obtaining passwords and this constituted an offence of phishing. According to this Guidance Note, identity theft and phishing are considered two parts of the same offence[73] and there are 3 distinct phases to categorise identity theft and phishing. Phase 1 concerns the 'obtaining of identity information', Phase 2 concerns the 'possession and disposal of identity information' and Phase 3 is described as the 'use of that information to commit fraud and other crimes' to form the offence of phishing and identity theft.[74] What we can see is that the conduct of his crime begins at Phase 1 where he distributes phishing emails for the purposes of obtaining identity information. In doing so, he gains illegal interception of such data which allows him access to sensitive information such as login details and passwords. The use of this protected information may also constitute data interference allowing for the illegal retrieval of credit card information prohibited by Article 4. Phase 2 then determines that the possession of this stolen information, which includes passwords and credit card details, constitutes a misuse of devices and a breach of Article 6. Finally, Phase 3 considers the exploitation of that information to facilitate the commission of fraud and other crimes as the final stage of his offence of terrorist financing constituting a breach of Article 8. Article 8 of Guidance Note of the 8th and 9th Plenary articulates the offence of computer-related fraud offence as:

> The use of a fraudulent identity by inputting, altering, deleting or suppressing computer data, and, or interfering with the function of a computer system will result in the exploitation of bank accounts or credit cards, in taking out loans and credit, or ordering goods and services, and thus causes one person to lose property and causes another person to obtain an economic benefit.[75]

---

[72] Cybercrime Convention Committee (T-CY), 'T-CY Guidance Notes: Adopted by the 8th and 9th Plenaries of the T-CY', (October 8, 2013) 29, at p. 11. Available at https://rm.coe.int/16802e7132

[73] Ibid. Identity theft is described as *'the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name'.*

[74] 8th and 9th Plenaries Guidance Note, supra note 63.

[75] Ibid, at p. 13.

Whilst the Guidance Note of the 8th and 9th Plenary does not refer specifically to terrorism; this document reveals the broad scope of Article 8 and means that this provision is capable of capturing Tsouli's activities. Thus, it seems that the nature of Tsouli's offences involve more than one phase and indeed that his activities may not be confined to one single cyber offence. In fact, the evolution of his criminal activities can potentially render him liable under several provisions of the Budapest Convention, further indicating that cyber terrorist financing can in fact fall foul of various offences under this agreement.

The analysis from both Guidance Notes in their applicability towards Tsouli's offence of cyber terrorist financing is interesting for numerous reasons. First, it shows the seamlessness of committing terrorist activities through cyber means. Tsouli's offence begins with the dissemination of propaganda online and then evolves in a way which requires cyber terrorist financing. There is arguably a narrow interpretation of terrorist offences and the implication of defining these crimes independent of each other might limit their potential for criminal prosecution. By committing two of the three OCTAs core to terrorism, Tsouli's terrorist activities reveal the natural progression of terror offences and how these activities can manifest into more serious and indeed sophisticated use of cyber means. This leads to the second point that recognises how these offences have developed from that of cyber enabled to that of cyber dependent. By progressing from cyber-enabled to that of cyber-dependent, Tsouli's offence of cyber terrorist financing falls within the parameters of the provisions prohibited by the Budapest Convention. Thirdly, it is plausible to assume that not only does Tsouli's offence constitute a breach of Article 8, but that the damage inflicted and the consequence resulting from his financial fraud can constitute a cyber offence as defined by Guidance Note 11. The example provided by Guidance Note 11 contends that loss of property to a number of victims can be considered an attack. Since Tsouli fraudulently acquired finances amassing to over £1.2 million, a substantial loss of economic property defined his offence as that requiring a sophisticated use of cyber means. Accepting this, the applicability of Article 8 and thus the Budapest Convention recognises only those acts that cross beyond this threshold of damage. In this case then, it must be assumed that any instance of cyber terrorist financing that results in such gross consequential losses falls within the parameters of Article 8 as long as it is committed through computer-related fraud.

From this, we could also assume that any large-scale financial crime that resonates a similar degree of economic loss to that of Tsouli's offence, committed through the use of cyber means can fall within the prohibited acts as stipulated by the Budapest Convention. The SWIFT attack on the Bangladesh Central Bank in 2016 is a prime example. A malware targeting attackers led to the modification of a software programme installed on bank servers and resulted in the theft of $81

million from accounts in Bangladesh Bank.[76] The use of malware aims to 'disrupt, damage, or gain unauthorised access to a computer system', which is an offence prohibited by Article 5 concerning System Interference.[77] Guidance Note 11 contextualises this offence in the nature of terrorism and claims that hindering the functioning of critical infrastructure by terrorists is a prohibition as per Article 5.[78] Whilst the SWIFT attack has no reported affiliation with terrorism or a terrorist organisation, the attack is reflective of the type of cyber offences that would fall within the ambit of the Budapest Convention. Undertaking a large-scale cyber operation which causes a significant economic loss of that degree would constitute a cyber-attack prohibited under Article 5. If an attack of such scale was committed by terrorists, it seems that the Budapest Convention alongside its Guidance Notes could be interpreted so as to prohibit such cyber terrorist activities under its substantive provisions. The potential for terrorist groups to carry out operations of this scale remains unprecedented, particularly where other less costly methods are already being exploited.[79] Nevertheless, such a possibility must not be ruled out given the nature and scale of modern terrorist tactics.

It can be concluded that cyber terrorist financing requires the most technical skills of all OCTAs. Whether this is money laundering, scamming credit card users online or exploiting electronic payment systems, cyber terrorist financing can exceed the level of technicality required to commit a cyber offence beyond that of recruitment or propaganda. It is clear that the Budapest Convention supplemented by Guidance Note 11 relating specifically to terrorism, nonetheless, remains central to cyber dependent offences. The Convention does not just prohibit cyber offences, but the above analysis has shown that its substantive provisions apply only if those offences can be shown to result in tangible consequences. At least, the Guidance Notes make implicit references to such a requisite by providing examples that reflect the very presumption that in the event of a cyber-offence, the damage must be a tangible consequence to attribute liability under the Budapest Convention. Therefore, it is unsurprising that only those cyber terrorist offences producing a certain type of consequence can be prohibited under the Budapest Convention. The case of Younis Tsouli and the

[76] Victor Mallet and Avantika Chilkoti, 'How Cyber Criminals Targeted Almost $1bn in Bangladesh Bank Heist', *The Financial Times Online* (March 18, 2016) available at https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8 (accessed 23 May 2018).
[77] Oxford English Dictionary definition accessed February 18, 2019 https://en.oxforddictionaries.com/definition/malware
[78] Guidance Note 11, supra note 30, at p 4. Article 5 'System Interference' provides a hypothetical example to denote how terrorist may be liable under this provision, which involves *'hindering a system that stores stock exchange records [to] make them inaccurate or hindering the functioning of critical infrastructure'*.
[79] For example, UNODC, The Use of the Internet for Terrorist Purposes, (United Nations, 2012), at para 14 to 17 lists the methods via which terrorist financing is acquired. See also FATF Report, Financing of Recruitment for Terrorist Purposes, (January 2018), at para 25 to 36 detailing the source of funds for terrorist recruiters.

SWIFT bank cyber-attack prove this very point: the Budapest Convention applies only to cyber terrorist offences that involve a sophisticated use of cyber means and that inflict a certain level of damage.

4.2 Does the African Union Convention Apply to Cyber Terrorist Financing?

There is no specific provision pertaining to financing for terrorist purposes found within the AU Convention. However, if an offence of cyber terrorist financing involves the use of either a computer system or computer data by virtue of Article 29(1) and (2), then the AU Convention could be interpreted to prohibit such activity. More specifically, Article 29(2)(d) states that it is a criminal offence under the AU Convention to:

> Fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting, suppressing computerized data or any other form of interference with the functioning of a computer system.[80]

There is nothing to infer what type of benefit may be incurred from committing a computer data breach as per the provision, but that any such benefit is sufficient for the provision to apply. From the prior analysis, it can be assumed that such benefit includes financial or monetary gain as prohibited by the Budapest Convention. A dictionary definition of the term benefit is described as *'*an advantage or profit gained from something',[81] with no limitations on what form an advantage or profit can take. Perhaps then, it is prudent to conclude that the general nature of procuring a benefit is not confined to any one sort. Rather, Article 29(2)(d) allows a sufficiently broad scope of its application insofar that financial benefits resulting from a computerised data breach would fall within such a definition so as to allow the finding of criminal liability. This means that an expansive interpretation of the provision could mean that benefits that may not amount to an economic value would also fall within Article 29(2)(d) such as the obtaining of sensitive information, which may then lead to the eventual procurement of financial gain.

Let us use a hypothetical example again for the purposes of analysis. It is possible for an individual who works at a bank and has access to loan applications to fraudulently amend data so as to apply and succeed in a loan renewal in order to unlawfully acquire finances for the purposes of terrorism. The individual is part of a terrorist organisation and also operate as a bank employee and has the intention of committing financial fraud to fund terrorist operations. This instance would meet the conditions of Article 29(2)(d), in that the procurement of a monetary benefit would result from the intrusion into the banking system to commit the fraud for terrorism. Alternatively, another scenario

[80] Article 29(2)(d) of the African Union Convention.
[81] Oxford English Dictionary definition of 'benefit'. Available at https://en.oxforddictionaries.com/definition/benefit (accessed 16 May 2019).

may consist of a more drastic incident such as a group of terrorists hacking into certain computer networks in order to engage in data mining. The terrorist group would then use that information to fraudulently acquire financial benefits and thus use these assets to fund terrorist operations. Both of these examples are plausible incidents that could manifest and form part of the cyber terrorist financing process. So long as it can be shown that an incident of computer-related fraud can be linked to terrorism, it seems that liability can be found under Article 29(2)(d) of the AU Convention.

4.3 Does the Arab Convention Apply to Cyber Terrorist Financing?

Since Article 15 of the Arab Convention dedicates an entire provision to prohibiting the use of cyber technology by terrorists in Article 15, it is clear that state parties see the potential of cyberterrorism as a threat to peace and security and which should attract criminal sanctions. This exemplifies the significance of Galtung's theory of peace and the need to strive towards achieving both concepts of peace, particularly the achievement of positive peace. This is because the Arab Convention's prevention of cyberterrorism can positively add to the overall achievement of peace, rather than merely alleviate the causes of negative peace through the prevention of war and violence.

Article 15(2) of the Arab Convention states that it is an offence to engage in the 'financing of…terrorist operations.'[82] The Arab Convention does not provide a definition to explain the precise nature of financing. However, a literal meaning would suggest that engaging in activities to provide monetary support to terrorist groups or to allow for the illegal acquisition of finances for terrorist purposes for example, are prohibited by the Arab Convention. This assumption is further supported by a dictionary definition of financing, which is to 'provide funding for (a person or enterprise).'[83] Therefore, an individual found to provide any funds or to use money in a way that contributes towards terrorist operations would be liable under Article 15(2) of the Arab Convention.

From this, it can be concluded that the Arab Convention strives towards achieving positive peace by prohibiting terrorist financing by criminalising the offence through legislation. Though there is no explicit mention of peace or the theory of peace within the Convention, the language and the inclusion of provisions such as Article 15 implies that the drafters of the Convention considered the implications of terrorist financing operations and its subsequent effects that can propagate violence within society. The Arab Convention makes a concerted effort to legislate against the financing of terrorist operations, anticipating that such offences can contribute to creating an environment where violence can materialise. Terrorist financing may not immediately cause a terrorist attack.

[82] Article 15(2) of the Arab Convention 2010.
[83] Oxford English Dictionary definition of 'financing', available at https://en.oxforddictionaries.com/definition/finance

This said, allowing the funding of terrorist operations inevitably sustains a terrorist organisation by enabling it to carry out essential functions. Without prevention, such activities will and do gradually foster systemic violence within a social structure by fuelling terrorism and feeding the needs of terrorist organisations ultimately impeding the achievement of peace.

A deeper look into the Arab Convention suggests that the financing of terrorist activities might be prohibited under other provisions on cyber offences. As stipulated by the UNODC in its definition of terrorist financing activities, the use of online payment tools is a principal way for terrorist groups to raise finances. The Arab Convention makes it clear through Article 18 that it condemns the use of electronic payment tools and includes the following offences:

1) Any person who forges, manufactures or sets up any instrument or materials that assist in the forgery or imitation of any electronic payment tool by whatever means.
2) Any person who takes possession of the data of an electronic payment tool and uses it, gives it to a third party or facilitates its acquisition by a third party.
3) Any person who uses the information network or an information technology means to unlawfully access the numbers or data of a payment tool.
4) Any person who knowingly accepts a forged payment tool.[84]

However, the Arab Convention does not suggest that illicit use of such payment tools has to relate to terrorism, or at least it makes no explicit mention of terrorism. Instead, the provision states that 'any person' found to commit such an offence is liable under Article 18, irrespective of the cause. Therefore, it is prudent to conclude that acts of cyber terrorist financing that involve the use of electronic payment tools would be prohibited by virtue of Article 18 of the Arab Convention.

V. Cyber Terrorist Propaganda

A key objective of terrorist groups is to spread their extremist views through propaganda. The use of cyberspace and cyber technology enables terrorists to reach an audience of online users that span across all corners of the world. Propaganda is not restricted to any one format and the development of modern terrorism has allowed for various platforms and outlets via which terrorist propaganda can take place. The UNODC explains that:

> Propaganda generally takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers.[85]

[84] Article 18 of the Arab Convention 2010.
[85] UNODC, The Use of the Internet for Terrorist Purposes, at p. 3.

Not only is this definition reflective of the developing ways in which terrorist propaganda can be produced but there is a sufficiently wide scope for various methods of communicating terrorist propaganda to fall within this definition. It is clear that propaganda is no longer confined to printed leaflets, posters and magazines. Instead, propaganda materials are changing to suit young audiences through the development of video games and targeted adverts aimed at the vulnerable young people. This is particularly worrying in an era where the internet is populated mostly by younger users. Therefore, it is necessary to determine whether any of the provisions of the three regional conventions can apply to acts of cyber terrorist propaganda.

5.1 Does the Budapest Convention Apply to Cyber Terrorist Propaganda?

The Budapest Convention does not contain any substantive provisions that relate directly and specifically to terrorist propaganda. However, the Convention contains an Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[86] Though neither this chapter nor this thesis explores xenophobia and racism in detail, it is necessary to determine whether terrorism has the potential to be xenophobic and racist and therefore discern whether the Additional Protocol can be used to prevent and suppress cyber terrorist propaganda.

The Additional Protocol calls for necessary measures to be adopted at both a national and international level to deter acts of propaganda that contain racist and xenophobic content. Intended as a supplementary instrument to the main Convention, the Additional Protocol serves as a model of law for states to adopt such measures into their national security regimes to safeguard against offensive online content.[87] However, states that are party to the Convention are under no obligations to ratify the Additional Protocol and measures to criminalise the dissemination of racist and xenophobic materials committed online are left to the discretion of states who can choose otherwise.[88]

The term 'racist and xenophobic material' is defined by Article 2(1) of the Additional Protocol as:

[86] Additional Protocol to the Convention, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (ETS No. 189) (2003).
[87] Ibid, Article 1.
[88] As of April 2019, there are 32 state that have ratified the Additional Protocol to the Convention on Cybercrime. See the updated list available at Council of Europe's website https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=EVOZMBnc

> any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion…[89]

There are various factors to consider under Article 2(1) of the Additional Protocol. Firstly, the information can be textual or illustrative and most importantly, the provision allows 'any other representation' to fall within the definition. Instead of prescribing the types of materials that may be discriminatory, the provision leaves a wide scope open for materials that may take new and modern formats that are not abundant at the time it was drafted. The provision places greater concern over the context of said material by prohibiting information that can be characterised as any provocation of prejudice that discriminates, possesses any abhorrence or promotes dangerous behaviour towards one person or a group of people owing to their ethnicity, origin, religion or race. Article 2(1) leaves an indisputably broad scope for possibly offensive and violent materials to be condemned under this Additional Protocol.

The provision places no limitations as to the format of the material, allowing for pictures, articles, publications as well as videos to contain racist or xenophobic content so long as they are made available through a computer system. Under Article 3, the Additional Protocol makes it a criminal offence to:

> distribute or otherwise make available, racist and xenophobic material to the public through a computer system.[90]

The defining feature is the characterisation of the offence by which qualification under the Additional Protocol is satisfied only if the material can be defined as racist and xenophobic. Different definitions of xenophobia include the 'dislike or prejudice against people from other countries'[91] as well as 'behaviour specifically based on the perception that the other is foreign to or originates from outside the community or nation'.[92] The recurring theme from these definitions of xenophobia is that they encompass an objection towards 'an associated group of people' because of the unfamiliarity they

[89] Article 2(1) of the Additional Protocol to the Convention, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (ETS No. 189) (2003).
[90] Article 3(1) of the Additional Protocol to the Convention, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (ETS No. 189) (2003).
[91] The English Oxford Dictionary definition of 'Xenophobia', available at https://en.oxforddictionaries.com/definition/xenophobia
[92] International Labour Office, International Organisation for Migration, and Office of the United Nations High Commissioner for Human Rights Discussion Paper, 'International Migration, Racism, Discrimination and Xenophobia', (2001), at p. 2. Available at https://www2.ohchr.org/english/issues/migration/taskforce/docs/wcar.pdf (accessed 4 June 2018).

possess with the majority in that particular environment or because they are from a different background or different country.[93]

Whilst this is a distinct prejudice against a selected group of individuals, xenophobia is not analogous to terrorism. Rather, xenophobia can occur as a result of terrorism and the two concepts can relate. For example, the increase in terrorist attacks can cause society to feel fear, anger or hatred towards anyone of a particular faith and overt prejudice against those who practice a certain religion.[94] The relationship between terrorism and xenophobia can be described as correlative, with the former causing an increase in the latter. Terrorism and acts of terrorism can cause people to become more xenophobic because they may make a general speculation that those who commit terrorism are individuals of a different *'*race, colour, descent or national or ethnic origin' as stipulated under the Additional Protocol.[95] However, this link can be seen as an over generalisation of those individuals suspected of committing terrorism and in itself a prejudice that is based on speculative presumptions that further the divide between groups of individuals.

In spite of this, there is nothing to dismiss the possibility that a piece of online propaganda could inhibit both racist and xenophobic content in support of terrorism. A prime example is terrorist propaganda encouraging or praising the killing of all Western journalists in support of ISIS such as Tweets of the same manner posted by Junaid Hussain.[96] The targeting of Western journalists is a desire that is motivated by a racist and xenophobic nature. The rationale behind destroying this particular group of individuals is attributed to the fact that these journalists come from a Western culture that is considered an opposition to ISIS and their killing is a cause that is justified by the support for terrorism. This specific terrorist activity could fall under Article 3 only and if the state wishing to criminalise the behaviour has ratified the Additional Protocol and implemented it into its own national laws. Though, with states possibly enforcing other effective remedies to counter such behaviour, the Additional Protocol has rather limited effect.[97]

---

[93] Victoria A. Springer, Camille B. Lalasz and Valeria A. Lykes, 'Social Action in Response to Terrorism: Understanding Xenophobic Violence from a Value-Added Perspective', *The Social Science Journal Vol. 49*, Iss. 2, June 2012 pp. 175 -182.
[94] Ibid at p. 177-179. The authors contend that certain major terrorist events have led to the increase of people that '*appeared to be members of specific ethnic or cultural groups [to be] singled out and subjected to acts of aggression, intimidation, and verbal and physical violence'.*
[95] United Nations Human Rights Office of the Commissioner, 'Counter-Terrorism Measures are Exacerbating Racism and Xenophobia, UN Rights Expert Warns', (31 October 2017) available at https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=22332&LangID=E
[96] Supra note 27.
[97] The measures set out in the Additional Protocol are intentionally separated to avoid alienating the US, which safeguards the Constitutional right to freedom of speech. See Sylvia Mercado Kierkegaard, 'Cracking Down on Cybercrime Global Response: The Cybercrime Convention', *Communications of the IIMA*: Vol. 5, Iss. 1, Article 7 (2005), at p. 63.

It is important to also note that propaganda of this type – exhibiting racist and xenophobic content – creates and perpetuates a culture of violence that can be used to justify or legitimise structural violence. Terrorist propaganda that encourages and promotes violence hinders the achievement of positive peace and if its prohibition falls within the parameters of Article 3 of the Additional Protocol, then such a provision can be argued to have normative value in striving towards peace. Whilst there is no explicit mention of peace within the language of Article 3, there is scope to contend that, through its ordinary meaning and purpose, the provision has an overriding objective to preserve peace by specifically condemning cyber activities that would otherwise subject society to violence of a racist or xenophobic nature. From this, it can be said that Galtung's theory of peace – which embodies the notion of preventing structural violence – permeates through the Budapest Convention and its Additional Protocol by way of deterring activities that could inhibit positive peace in its provisions.

On one hand, the Additional Protocol may be considered appropriate legislation for states that are willing to enforce the prohibition of materials that contain racist and xenophobic content committed through computer systems. On the other hand, the requirement of establishing a causal link with an act of terrorism might prove difficult in certain circumstances, particularly when it comes to regulating cyber terrorist propaganda and OCTAs. Furthermore, the non-compulsory nature of its ratification means that some states will not implement the Additional Protocol and thus the criminalisation of certain offences is not consistently imposed by state parties.

5.2. Does the African Union Convention Apply to Cyber Terrorist Propaganda?

There are no provisions that specifically mention cyber terrorist propaganda within the AU Convention. However, when it comes to content-related offences committed by cyber means, Article 29(3)(e) makes it an offence to:

> create, download, disseminate or make available in any form writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature through a computer system.[98]

Under this provision, liability for an offence is characterised by its racist and xenophobic nature. The type of materials mentioned in the above provision generally correlate with the prior definition of terrorist propaganda depicting the differing multimedia formats in which they may be expressed, such as writings, messages, photographs etc. In addition, Article 29(3)(e) includes a more general description to include 'any other presentation of ideas or theories' as part of the material content that is prohibited by the AU Convention. In doing so, the provision does not specify particular formats of

[98] Article 29(3)(e) of the African Union Convention (2014).

propaganda but leaves a sufficiently wide scope to encapsulate the different possible ways in which materials of a racist or xenophobic nature can take form through a computer system.

To understand the parameters of Article 29(3)(e), the general rules under the VCLT shall be applied. There are various ways in which materials of a racist and xenophobic nature can be presented: they can be made or produced by the author, transferred and re-used, or spread to allow the material to be shared. Rather than restricting the format of the material, the provision begins by making it an offence to use any of the above-mentioned different types of information as long as it is done so through a computer system. This means that there are three conditions that must be satisfied in order for a violation of Article 29(3)(e). One, the format can range from images, illustrations, any representations through text or other forms of communication, two, they are either existing, or generated for the purposes of producing racist or xenophobic content and three, they are conducted through a computer system. Article 29(3)(e) thus leaves a wide scope of materials to be considered within the parameters of this provision.

Echoing the Additional Protocol to the Convention on Cybercrime, to apply Article 29(3)(e) to OCTAs would render only those activities that can be proven to be racist and xenophobic as qualifying offences. Whilst previous discussion has shown that the increase of terrorism may cause xenophobia and racism, these concepts are not synonymous with one another. That is to say, something characterised as xenophobic and racist does not automatically render such content terrorist by nature. For instance, posting an image online in support of ISIS can be xenophobic and racist if it were to say, encourage the overthrow of Western leaders because, for example, they do not conform to the ideals and values of Islamic culture. Xenophobia and racism are certainly a recurring theme in online ISIS magazines such as Dabiq and Rumiyah, which support the opposition and terrorising of the Western culture.[99] On the other hand, posting an image online supporting the abolition of all Western leaders may not necessarily be of a terrorist nature, particularly where the image does not explicitly present terrorist ideologies or values.[100]

This discussion has shown that under Article 29(3)(e), materials of a racist or xenophobic nature can take various forms to constitute propaganda in much of the same way as the UNODC's definition

[99] Both ISIS publications Dabiq and Rumiyah maintain a theme of condemning Western behaviour and culture and sees this as an opposition to the Islamic faith. For example, Dabiq, Issue 15, Shawwal 1437, at p. 20 expresses that *'The deviance carried on until the so-called "Brave New World" of America and Western Europe began legalizing marijuana, bestiality, transgenderism, sodomy, pornography, feminism, and other evils, allowing the Christian pagans of Europe, America, and Australia to break the crime record of every disbelieving nation of precede them in history…'.*

[100] Such an offence may fall under Article 29(3)(1)(f) which states that it is a criminal offence to *'threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of these characteristics.'*

of terrorist propaganda mentioned before. Propaganda that contains xenophobia and racism directly obstructs the achievement of positive peace because it creates fertile ground within a culture or society that can be used to legitimise structural violence, and this is particularly the case if that material is characterised by terrorism. Given this, such materials must be prevented and the AU Convention's recognition of this is significant in the context of legal rules pertaining to cyberterrorism. This said, whilst terrorist propaganda can be both xenophobic and racist, it must be reiterated that this presumption is not absolute. In light of this, Article 29(3)(e) applies to cyber terrorist propaganda activities only if and when they can be shown to possess both a racist and xenophobic nature within its material content.

5.3 Does the Arab Convention Apply to Cyber Terrorist Propaganda?

Within Article 15 of the Arab Convention there are two provisions that may be useful in addressing cyber terrorist propaganda. In the same manner as the other regional conventions discussed in this chapter, the Arab Convention does not use the term propaganda in its legislation. Rather, Article 15(1) makes it an offence to engage in the:

> dissemination and advocacy of the ideas and principles of terrorist groups.[101]

The question is whether ideas and principles can take the form of terrorist propaganda. It is unclear precisely what ideas and principles mean and whether this includes users online sharing information simply out of curiosity or whether more direct association has to be established such as the possession of terrorist materials found within a computer system for example. There is little to indicate the extremity of the provision and the threshold at when this act becomes a criminal offence.

In order to understand the provision better, we are to employ an ordinary meaning of the text as stipulated by the general rule of interpretation held under Article 31(1) of the Vienna Convention.[102] Determining this ordinary meaning can be aided by seeking a dictionary definition of the terms in question.[103] Dissemination is described as the spreading of information, and advocacy denotes the public support for or the recommendation of a particular cause or policy.[104] This support must come in the form of ideas and principles which are considered thoughts or suggestions as to a possible

[101] Article 15(1) of the Arab Convention (2010).
[102] Article 31(1) of the Vienna Convention on the Law on Treaties, 1969.
[103] In order to attribute an ordinary meaning of the terms in question, the function of a dictionary definition allows for 'the basic discovery of ordinary meanings of a term'. See Richard Gardiner, *Treaty Interpretation*, (OUP 2017), at p. 186.
[104] Oxford English Dictionary definition of 'dissemination' is 'the act of spreading something, especially information, widely'. Available at https://en.oxforddictionaries.com/definition/dissemination; Oxford English Dictionary definition of 'advocacy' is 'public support for or recommendation of a particular cause or policy'. Available at https://en.oxforddictionaries.com/definition/advocacy

course of action and rules or beliefs governing one's behaviour.[105] The ordinary meaning of Article 15(1) informs us that it is a cyber offence to spread information that publicly supports or recommends thoughts or suggestions as to a possible course of action and rules or beliefs governing one's behaviour in relation to terrorism. Rather than identifying specific formats of information, the provision maintains a broad interpretation of the types of information relating to terrorism that might fall within Article 15(1). In doing so, it encompasses various forms via which terrorist propaganda can be spread online.

The above interpretation of Article 15(1) implies that the provision prohibits the spread of terrorist propaganda through the use of information technology. Not only can Article 15(1) be construed to apply to cyber terrorist propaganda, but its sufficiently broad application also means there is great potential for various forms of terrorist material, whether new or old, to be condemned under the Arab Convention.

Another provision that may be applicable to cyber terrorist propaganda is Article 15(4) where the final provision of the Arab Convention condemns:

> Spreading religious fanaticism and dissention and attacking religion and beliefs.[106]

The Arab Convention does not elaborate on the terms used in the above provision and whether it can be interpreted to apply to cyber terrorist propaganda. As such, it is again necessary to refer to the general rule of interpretation. In accordance with the Vienna Convention, a literal interpretation requires a reading of the text as it stands. A dictionary definition of fanaticism is explained as 'the quality of being fanatical', which is further described as 'obsessively concerned with something'.[107] This understanding infers that to be obsessively concerned with a particular religion and to act against other religions and beliefs through the use of information technology is an offence prohibited under Article 15(4). The format via which these views are expressed is not specified by the Arab Convention, instead leaving a broad enough interpretation to suppose that any presentation of these views is condemned under Article 15(4).

There is also the possibility that this provision may encompass acts which criticise particular religious beliefs but that do not meet the ideals of terrorist ideologies. For example, the ISIS publication Dabiq often contains content which condemns Christianity amongst other religions:

---

[105] Oxford English Dictionary definition of 'idea' is 'a thought or suggestion as to a possible course of action'. Available at https://en.oxforddictionaries.com/definition/idea; Oxford English Dictionary definition of 'principles' is 'a rule or belief governing one's behaviour'. Available at https://en.oxforddictionaries.com/definition/principle

[106] Article 15(4) of the Arab Convention.

[107] Oxford English Dictionary definition of 'fanaticism'. Available at https://en.oxforddictionaries.com/definition/fanaticism

> Whether they are Catholic, Protestant, or Orthodox Christians, whether they are Orthodox, Conservative, or Progressive Jews, whether they are Buddhists, Hindus, or Sikhs, whether they are capitalists, communists, or fascists – they are ultimately allies of one another against Islam and the Muslims.[108]

A similar ISIS publication known as Rumiyah condones and even encourages violence and hatred against Christians and others:

> If we know that the blood of the Christians is permissible to shed, we know that taking them as slaves is also permissible, and likewise taking them prisoner and ransoming them for our prisoners or for wealth after having inflicted a massacre on them, due to the statement of Allah.[109]

These excerpts show how specific religions and beliefs are targeted and attacked within certain ISIS materials. Given such explicit views, there are compelling reasons to believe that the manifest condemnation of religious beliefs other than the Islamic faith is likely to fall under Article 15(4) as an attack on religions and beliefs as it relates to ISIS publications. Inference of such materials are very much left to the discretion of state parties to make their own postulations on whether the online content constitutes an attack as stipulated by Article 15(4) of the Arab Convention.

There is much to be said about the relevancy of the Arab Convention when it comes to the regulation of cyber terrorist propaganda. An interpretation of Article 15(1) has revealed that terrorist propaganda can be seen as a form of advocacy when it comes to spreading ideas and principles of terrorist groups. On the other hand, Article 15(4) can be understood to prohibit religious views associated with terrorism and to condemn such behaviour under the Arab Convention. Whilst both of these provisions are substantively different and focus on different types of material content, it can be argued that Articles 15(1) and (4) have sufficiently broad scope of application that enables cyber terrorist propaganda to be prohibited under the Arab Convention.

VI. Differing Application of Regional Treaties

The Budapest Convention envisions a certain type of cyber offence in mind: those that meet a certain threshold of harm or damage sufficient to be considered a cyber-attack and thus, threaten international peace and security. This threshold is determined on the basis that the cyber offence in

---

[108] Dabiq, 1437 Safar, 'Terror', Issue 12 at p. 43. Available at http://clarionproject.org/wp-content/uploads/islamic-state-isis-isil-dabiq-magazine-issue-12-just-terror.pdf (accessed 15 February 2017).

[109] See Rumiyah Sha'ban 1438, 'The Ruling on the Belligerent Christians', Issue 9, available at https://qb5cc3pam3y2ad0tm1zxuhho-wpengine.netdna-ssl.com/wp-content/uploads/2017/05/Rumiyah-9.pdf (accessed 15 February 2017). The Clarion Project contains various publications of both Dabiq and Rumiyah which contain various reiterations of condemnation against Western society and Christian Faith. For example, one issue criticises Western females and claims that '*[Christians] encourage the Western woman to be everything opposite of Mary… the solution is laid before the Western woman. It is nothing but Islam'.* Dabiq, 1437 Shawwal, 'Break the Cross', Issue 15 at p. 25 available at http://clarionproject.org/wp-content/uploads/islamic-state-magazine-dabiq-fifteen-breaking-the-cross.pdf (accessed 15 February 2017). See also Rumiyah, Issue 2, Muharram 1438 at p. 3*, 'One should not downplay the importance of targeting and eliminating the imams of kufr [denial or rejection of Islam] in the West, doing so in support of Allahs' religion '*available at http://clarionproject.org/wp-content/uploads/Rumiyh-ISIS-Magazine-2nd-issue.pdf (accessed 16 February 2017).

question produces a consequence that is sufficiently serious. This might be contingent on the scale of the cyber operation such as the SWIFT attack, or the economic loss incurred comparable to that of Younis Tsouli's cyber operation. OCTAs, however, are cyber-enabled activities that absent of the internet are traditionally carried out using physical means. Yet, the Budapest Convention focuses on cyber-dependent offences that can only be committed through the means of cyber technology. Given this, only those OCTAs that rely on cyber technology can be construed under the Budapest Convention as an offence by virtue of its cyber-centric provisions. At present, the analysis has shown that cyber terrorist financing is the only OCTA that may involve such a sophisticated use of cyber technology sufficient to incur liability under the Budapest Convention. Unless the cyber offences in question meet this requisite, provisions of the Budapest Convention fall short of regulating OCTAs despite the supplementary interpretation of its Guidance Notes.

Though the AU Convention may have followed the same model as the Budapest Convention, the scope of its provisions is narrow and thus, less applicable to the regulation of OCTAs. Not only are provisions of the AU Convention central to computer-based attacks, but its content-related offences are restricted only to those acts that can be defined as being either racist or xenophobic. The AU Convention focuses on an exclusive type of cyber offence that mirrors that of the Budapest Convention.[110] The same shortfalls that apply to the latter are not distinct from the former and only those OCTAs that cross the threshold of technical expertise will fall within the scope of provisions under the AU Convention. Unless terrorist recruitment and propaganda require trespass into computer systems or manipulation of computer data, the interpretation of the AU Convention applies only to cyber-dependent offences under its remit.

On the contrary, the Arab Convention has shown great potential to regulate OCTAs. Within its substantive provisions, the provision of Article 15 contains an entire section devoted to terrorism, which neither the Budapest Convention nor the AU Convention does. The provision contains measures that clearly condemn both cyber terrorist propaganda and cyber terrorist financing, making their prohibition explicit. The analysis has also shown that the Arab Convention's provisions have normative value in striving towards peace, specifically to encourage positive peace by preventing activities that can be used to legitimise structural violence. Whilst cyber terrorist recruitment is not expressly identified within Article 15(2), a literal interpretation of 'facilitating communication' infers that communication for the purposes of recruitment can fall within this prohibited activity. Notwithstanding Article 15(2) that begins by condemning financing, Article 18 articulates on ways to

[110] For a comparison between the African Union Convention and the Convention on Cybercrime see Council of Europe GLACY+ Report, 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime', (20 November 2016).

acquire illicit funds through the use of electronic payment tools. Both of these methods to raise funds have been identified by the UNODC as terrorist activities and, while the respective provisions do not mention terrorism, offences characterised in such a manner would indeed fall within the scope of the Arab Convention.

VII. Conclusion

An analysis of the regional conventions has shown that existing legislation criminalises very specific types of cyber offences. The more cyber dependent the offence is, the more relevant the Convention on Cybercrime (2001) becomes to regulating that offence. The same can be said of the African Union Convention (2014), which has similar provisions to the Convention on Cybercrime. Both of these conventions contain respective provisions from which can be inferred a normative value of striving towards peace, and this is particularly more patent in relation to positive peace and signifies the need to prevent OCTAs that can be used to legitimise structural violence. Terrorist financing which may require higher levels of computer proficiency differ from terrorist recruitment and terrorist propaganda which do not surpass the minimum level of technical capability for their employment. However, OCTAs are not limited to purely cyber-dependent crimes such as those offences committed by Younis Tsouli or Junaid Hussain. Instead, what this analysis has shown is that cyberterrorism can often incorporate a range of offences whereby the spread of terrorist propaganda can facilitate terrorist recruitment and so on.

Of the regional treaties assessed, the Arab Convention (2010) is the only one that criminalises the use of technology for terrorist purposes. Not only are there specific provisions relating directly to both cyber terrorist financing and cyber terrorist propaganda, but it is also possible to interpret the Arab Convention to condemn cyber terrorist recruitment. While Article 15 does not mention the terms propaganda or recruitment, interpretation using the Vienna Convention has shown that it is possible for all three OCTAs to fall within the scope of its application. Thus, the Arab Convention shows great potential in its regulation of OCTAs, and Article 15 is a model for counter-terror legislation when it comes to cyberterrorism. The Arab Convention strives to inhibit OCTAs that hinder the achievement of positive peace. This said, its utility remains confined to those states that are party to the Convention in the Arab region. The regulation of OCTAs by this regional treaty is nonetheless a promising example and emphasizes the need for certain states to follow suit and address activities of cyberterrorism.

For both the Budapest Convention and the AU Convention, it seems that regional cybercrime laws relating to terrorism are reserved for acts that cross a certain threshold of harm. In other words, only serious cyber offences that result in tangible consequences are criminalised by these conventions. For example, intrusions to computer systems must result in the damage of critical infrastructure for

relevant provisions to apply.[111] Notwithstanding such cyber-attacks and Article 15 of the Arab Convention, there is a sparse legal landscape that is currently applicable to the regulation of OCTAs within international law and there is not yet a comprehensive regulatory mechanism that can govern cyber activities, less so cyber terrorist activities. According to Mačák, 'states seem reluctant to engage in the development and interpretation of international law applicable to cyber security'.[112] This is in part due to differing cybersecurity abilities of various national states and contrasting priorities of national security regimes, contributing towards the lack of collective action to achieve a standardised international cyber treaty. Whilst states are willing to enter into binding treaties that regulate certain cybercrimes and encourage international cooperation among the region, the likelihood of a comprehensive international treaty on cybersecurity or cyberspace remains a distant optimism for the international community. This is in part due to the progressive advancement of technology which problematizes the crystallisation of cyber treaties because of the unduly length of time it takes for legislation to enter into force. This has the possibility of outdating the provisions before they even have the potential to become enforceable in practice. Yet, the realm of cyberspace and its potential dangers cannot remain void of international regulation. For this reason, the next chapter will explore whether UN resolutions and relevant UN instruments are able to address and regulate OCTAs within international law.

[111] David Fidler, 'Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection', 16 *Georgetown Journal of International Affairs 8* (2015) Special Issue, at p. 11. According to Fidler, terrorist efforts to utilise computer systems for the purpose of accessing, disrupting or damaging critical infrastructure would fall within the ambit of international law on cybercrime.

[112] Kubo Maçak, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers', *Leiden Journal of International Law* (2017), 30, pp. 877-899, at p. 886.

Chapter Four

THE UN'S COLLECTIVE SECURITY SYSTEM AND OCTAS

I. Introduction

The UN collective security system's main organs are the Security Council and the General Assembly. These two organs are pivotal to the prevention of international terrorism by determining how threats to international peace and security are addressed. With the emergence of cyber technology and its exploitation by terrorist groups, it is necessary to evaluate whether and to what extent the UN's collective security system contributes to the prevention and suppression of OCTAs.

This chapter explores whether UN resolutions on terrorism by both the Security Council and the General Assembly apply to OCTAs and indeed, in relation to cyberterrorism. Section II begins by exploring the jurisprudence of the Security Council, identifying its competencies and powers and examining what measures it can take. A distinction is made between two types of resolutions adopted by the Security Council: executive and legislative. This section continues to determine whether Security Council resolutions apply to OCTAs. Section III explores the role of the General Assembly in the field of international peace and security, the nature of its resolutions and its competences and powers in relation to terrorism. This section then investigates whether General Assembly resolutions can be applied to OCTAs. Section IV reveals that, while the organs of the UN collective security system have recognised and sought to prevent and suppress OCTAs, these efforts exhibit limitations. Lastly, Section V offers conclusions.

II. The UN's Collective Security System and the Security Council

2.1 Competences and Powers of the Security Council

Within the UN's collective security system, the Security Council enjoys primary responsibility for the maintenance of international peace and security.[1] Under the Charter of the UN, its functions are outlined in Chapters VI and VII.[2] Article 39 of the Charter states that the Security Council has the competences and powers to make determinations as to whether a threat to the peace, a breach to the peace or an act of aggression has occurred and it must take action according to Articles 41 and 42.[3] According to Wood, the Security Council exercises a range of actions where:

[1] Article 24 of the Charter of the United Nations, 1945.

[2] The Security Council's powers are delineated in Chapters VI and VII of the UN Charter. Chapter VI refers to the recommendatory powers in relation to the peaceful settlement of disputes or situations that might endanger peace. Chapter VII allows the Council to make determinations upon the 'threat to the peace', 'breach of the peace' or 'act of aggression', in the form of military action and a range of non-forcible measures.

[3] The Council has made numerous determinations of 'threats to the peace', and various 'breaches to the peace'. One of the first times the Council exercised its Article 39 powers was in response to the Korean conflict in 1950, demanding a ceasefire

> it may impose obligations… it may reaffirm existing rules, it may apply existing rules, it may depart from or override existing rules in particular cases, but it does not lay down new rules of general application.[4]

This interpretation of the Council's responsibilities is important for two reasons. First, the role of the Council is very clearly defined: the Council is to determine issues and to take executive action over matters that are considered a breach of the peace. Second, by denying the Council the right to lay down new rules of general application, the Charter emphasizes that the powers of this organ are strictly limited to decision making.[5]

When the Council determines a threat to the peace, it may take either forcible or non-forcible measures. Under Articles 39 and 42 of the Charter, the Council may take measures using force such as blockades or land, sea and air operations which may be exercised in response to the threat.[6] Alternatively, the Council may decide to use non-forcible measures to address the threat under Article 41 in the form of financial and economic sanctions.[7] The Council then formalises its decisions through instruments known as Security Council resolutions. Described as having great 'normative value', resolutions can reinstate the underlying norms of international law that emanate from traditional sources of international law.[8] According to Ian Johnstone, Security Council resolutions can serve 'declarative', 'interpretive' and 'enforcement' functions.[9] These categories distinguish the different types of resolutions adopted by the Council in response to particular international crises.[10] What we shall see is that the varying functions of the Security Council are reflective of its increasingly

between North and the South (SC Res. 82 of 25 June 1950). Similarly, the 1990 Iraqi invasion of Kuwait was considered a breach to the peace leading to a ceasefire regime enforced by the Council (SC Res. 687 of 3 April 1991). However, 'acts of aggression' are rarely determined by the Council. See e.g. Christine Gray, 'The Charter Limitations on the Use of Force: Theory and Practice', 86-91 in eds. Lowe et al., *The United Nations Security Council and War: The Evolution of Thought and Practice Since 1945*, (OUP, 2010).

[4] Michael Wood, 'The Interpretation of Security Council Resolutions', *Max Planck Yearbook of United Nations Law*, (Vol. 20, Issue 1, 2017), at p. 78.

[5] For more discussion on the legality of Security Council actions, see for example Eric Rosand, 'The Security Council as "Global Legislator": Ultra Vires or Ultra Innovative?', 28 *Fordham Int'l LJ*. 542 (2004). The author discusses the adoption of both Resolution 1373 and 1540 as necessary to ensure the Council's mandate and thus they should not be considered actions of ultra vires. See also Björn Elberling, 'The Ultra Vires Character of Legislative Action by the Security Council', *International Organisations Law Review* 2: 337-360, (2005). The author explores the increasingly quasi-judicial role of the Council and the illegality of adopting legislative resolutions, which he argues falls outside the remit of the Council's competencies.

[6] The authorisation of force is determined under both Articles 39 and 42 of the Charter, where there is a threat to, or breach of peace, and forcible measures are required for the maintenance or restoration of peace and security.

[7] Sanctions can be taken for numerous reasons ranging from economic, trade, arms embargoes, travel bans, financial restrictions. Smart sanctions are also used, which are targeted restrictions on specified individuals or a group of people rather than imposing conditions upon an entire state. In response to international terrorism, the Council has applied various sanctions and smart sanctions such as those in Resolution 1267 (1999) and Resolution 2253 (2015). Not only are sanctions part of the policymaking capacity bestowed to the Council, they form a key element of the Council's counter-terrorism regime alongside resolutions which together are intended as effective tools for achieving peace and security.

[8] See Marko Divac Öberg, 'The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ', *EJIL V*ol. 16 No. 5, 2006 at p. 884.

[9] Ian Johnstone, 'Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit', 102 *Am. J. Int'l L*. 275 (2008), at p. 283.

[10] Ian Johnstone, *The Power of Deliberation: International Law, Politics and Organisations*, (OUP, 2011), at p. 94.

broadening powers which are considered necessary in response to the evolving threats to international peace and security, and this includes acts of international terrorism.

The Security Council performs a declarative role in matters of international peace and security, making statements concerning the international matters bought before it. Declarations of the Council are said to be 'legal conclusions about areas of law not directly part of the Charter'.[11] The legal and political weight behind declarative statements of the Council carry significant authority in determining state behaviour and thus shape the way in which international rules may form.[12] Whilst declarations themselves do not strictly create new law, certain declarative resolutions that are discussed later on show the Security Council's capacity to establish new rules. On multiple occasions declarations are being made in situations described as an 'emergency' and where the threat is considered 'extreme and imminent'.[13] For example, the Council readily declared 'the proliferation of all weapons of mass destruction as a threat to international peace and security'.[14] Security Council Resolution 2177 (2014) declared the 'unprecedented extent' of the Ebola outbreak in Africa as constituting a threat to international peace and security.[15] And most notably, the adoption of Security Council Resolution 1269 (1999) formally declared terrorism as a threat to the peace.[16] Upon interpreting matters of peace and security, the Security Council makes declarative statements in its resolutions as iterations of legal principles and findings. This sets a standard for Member States on how to approach and address the issue and how the matter is to be considered within the context of peace and security.

When the Council makes determinations as to what constitutes a threat to the peace within the scope of Article 39, it exercises what Johnstone calls an interpretive function. The UN Charter sets 'no limits' on the discretion of the Council to make a determination under Article 39,[17] to which the Council has made various determinations in response to a breadth of issues that it considers international crises. For instance, the Council has on separate occasions, expressly authorised intervention in Somalia[18] and Libya,[19] on both occasions the Security Council declared a threat to the

[11] Steven Ratner, 'The Security Council and International Law', at p. 594. in Eds Malone, *The UN Security Council: From the Cold War to the 21st Century*, (Lynne Rienner Publishers, 2004).
[12] Öberg, supra note 8.
[13] For discussion on the Security Council adopting Chapter VII resolutions under 'emergency' conditions see Jared Schott, 'Chapter VII as Exception: Security Council Action and the Regulative Ideal of Emergency', 6 *Nw. J. Int'l Hum. Rts.* 24 (2008), at 31. See also Devon Whittle, 'The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action', *European Journal of International Law*, Vol. 26, Iss. 3, August 2015, pp. 671 – 691.
[14] United Nations Security Council, Note by the President of the Security Council, S/23500 of 31 January 1992, at 4 (Jan 31, 1992).
[15] S/RES/2177 of 18 September 2014.
[16] S/RES/1269 of 19 October 1999.
[17] Eds. Vaughan Lowe et al., *The United Nations Security Council and War: The Evolution of Thought and Practice Since 1945*, (OUP, 2010), at p. 35.
[18] S/RES/794 of 3 Dec. 1992.
[19] S/RES/1973 of 17 March 2011.

peace on the basis of violations of international humanitarian law and the need for military intervention and a ceasefire to protect civilians. It has since expanded its authority to address rising international crises inclusive of health pandemics, human security and creating ad hoc criminal tribunals in response to war crimes and determining these matters a threat to the peace. Not only has its interpretive function developed in light of emerging issues on the international plane, but the Security Council also recognises a threat to the peace in the form of structural conflicts that develop within the territories of sovereign states. From this, it can be said that peace is a malleable concept that is being constantly redefined and broadened by matters bought before the Security Council and equally, that the Council strives towards peace by using institutional powers within its scope to prevent threats to positive peace (and arguably negative peace) from materialising.

The Security Council also acts as an enforcer of peace. The Council imposes obligations upon how states should or should not act in particular situations and determines how a threat to the peace is addressed by the international community according to Articles 41 and 42 of the Charter. The Security Council can enforce international law only if violations are a threat to international peace and security. For instance, the legal obligations deriving from Resolution 1373 reflects a situation where the Council acts as an enforcer (and creator, as discussed later) of rules of international law in response to an international terrorist attack. Similarly, in response to the humanitarian crises in both Yugoslavia[20] and Rwanda,[21] the establishment of ad hoc criminal tribunals under Article 41 for the prosecution of certain individuals is reflective of the Security Council enforcing international rules to prosecute individuals responsible for committing violations of international law. By determining that the Former Yugoslavia and Rwanda committed violations of international humanitarian law, the Security Council decided to create international tribunals under its Article 41 powers as a necessary measure to restore and maintain peace in those states. In doing so, the Security Council plays a significant role in developing a normative framework to shape the behaviour of states and ensure the protection of societies within these states against structural violence. A primary function of the Security Council thus involves enforcing legal rules and principles on states through obligations as a means of observing international law.

It is clear that there are varying functions performed by the Security Council as a result of its growing competences and powers and it is not always easy or worthwhile to draw bright lines between them. When the Security Council adopts a resolution, it may also follow by establishing new measures to address the threat to peace in unprecedented ways. Despite the Security Council having been

[20] S/RES/827 of 25 May 1993
[21] S/RES/955 of 8 Nov. 1994.

defined as performing a rather distinct executive role, we shall see further on that evolving practice of the Council goes beyond its role as an enforcer of international law to create certain new rules in the contemporary landscape of international terrorism.

2.2 The Security Council's Enforcement of Peace and Security in Relation to Terrorism

During the early 1990s, the rise of state-sponsored acts of terrorism led the Security Council to become a key actor in addressing the threat posed by international terrorism. In 1992, sanctions were launched against Libya in response to the lack of international cooperation from the Libyan government concerning two airline bombings in Lockerbie.[22] Despite the Security Council's requests for cooperation, Libya refused to surrender the suspects for the purposes of international investigation on the matter. In response, the Security Council adopted Resolution 748 (1992) and determined that the refusal of compliance could be considered state-support for terrorism and that Libya's failure to comply with an earlier Resolution 731 (1992) constituted a threat to international peace and security.[23]

In 1996, the Security Council enforced Resolution 1054 (1996) against Sudan for its alleged involvement in the death of Egyptian President Mubarak.[24] In its adoption of an earlier Resolution 1044 (1992), the Security Council requested international cooperation for Sudan to extradite three suspects that were accused of assassinating the President of Egypt.[25] However, Sudan was reluctant to comply and assist with the investigation, which led the Security Council to determine that Sudan was responsible for giving shelter and sanctuaries to suspected terrorists and that this constituted a threat to international peace and security.

The Security Council in both Libya and Sudan issued an initial non-binding resolution to request cooperation from the respective states. What is particularly important and interesting is that in both cases, Chapter VII resolutions were not enforced in relation to the terrorist act in question, but for the states failure to comply with the initial non-binding resolutions requesting for international cooperation. The Security Council considered on both occasions that sanctions were necessary and that an unwillingness to cooperate could be interpreted as state sponsorship of terrorism and therefore amount to a violation of UN obligations. This also affirms the normative value of the Security Council's actions of striving towards peace, in particular to prevent the obstruction to positive peace by reducing opportunities to foster structural violence in both Libya and Sudan.

[22] S/RES/731 of 21 January 1992
[23] S/RES/748 of 31 March 1992.
[24] S/RES/1054 of 26 April 1996.
[25] S/RES/1044 of 31 January 1996.

The emergence of international terrorism was most notably brought about by Al-Qaeda and the Taliban regime, leading the Security Council to adopt Resolution 1267 (1999) to establish a sanctions mandate against suspected terrorists. The Afghan conflict involved destruction, human suffering and displacement of many people and areas controlled by the Taliban were used as terrorist bases for sheltering and the training of recruits.[26] Not least do these terrorist activities threaten state security, they form aspects of a culture that can be used to encourage structural violence and thus, impede development of the full potential of individuals within that society. The Security Council determined that the Taliban government failed to respond to the demands set out in earlier Resolution 1214 (1998) for harbouring the terrorist group Al-Qaeda and adopted Resolution 1267 (1999) under Chapter VII to determine that this presented a threat to international peace and security. Not only was this the first time the Security Council imposed sanctions against Afghanistan, the rationale for enforcing a Chapter VII resolution was again, based on the states failure to comply with the preceding request for cooperation.[27]

The Security Council's implementation of sanctions measures was a significant deterrent for state sponsorship of terrorism, showing states that support for terrorism constituted a threat to the maintenance of international peace and security and directly hinders the achievement of positive peace. Chapter VII resolutions were justified on the basis that the territorial state failed to comply with the requests made by the Security Council to cooperate and prevent the continued threat of international terrorism which includes legitimising structural violence. It appears that the Security Council has given considerably more weight to the failure of complying with resolutions that request cooperation rather than for the act of terrorism itself. While there is much to be said about their effectiveness, sanctions showed the rest of the international community that terrorism and the support for terrorism is condemned by the Security Council. More importantly, the above Chapter VII resolutions seem to show that non-compliance with Security Council resolutions will result in stringent measures of enforcement so much so that determinations made under Article 39 will fall under a wide remit.

The discussion above has shown that resolutions or a series of resolutions are adopted in response to emerging threats. They are secondary sources of international law and rather than acting as hard traditional legislative acts, they are intended as policy-making mechanisms designed to provide

[26] Mónica Lourdes de la serna Galván, 'Interpretation of Article 39 of the UN Charter (Threat to the Peace) by the Security Council. Is the Security Council a Legislator for the Entire International Community?', Anuario Maxicano de Derecho Internacional, vol. XI, 2011, pp. 147 – 185, at p. 173 - 175.
[27] S/RES/1267 of 15 October 1999.

effective regulation in areas where primary sources of international law cannot yet do so.[28] This, however, should not prevent resolutions from being subject to established rules of interpretation, particularly when further elaboration is required to understand the content of the resolution. As such, the general rule of interpretation enshrined under Article 31 of the Vienna Convention will be used to interpret Security Council Resolutions.[29]

However, it must be acknowledged that there are fundamental differences between the nature of treaties with that of resolutions providing scope for the contention that a treaty designed to address treaties cannot then be applied to instruments that are quite frankly, not treaties. This argument is set forth by Papastavridis who argues that Articles 31-33 of the Vienna Convention are not the most appropriate framework to analyse and interpret resolutions.[30] His theory does not envision that the original purpose of the wording can be construed by a simple literal interpretation as is the case for treaty law, but rather that resolutions should be interpreted 'in light of the position it occupies in that enterprise'.[31]

This view is contested for at least two reasons. First, Security Council resolutions and treaties are not entirely dissimilar. Formally, the VCLT concerns the interpretation of treaties. However, since they form part of customary international law on interpretation this means that, because of the similarities between treaties and Security Council resolutions, Security Council resolutions must be interpreted consistently with the rules outlined by the VCLT.[32] Second, given the similarities, the original purpose of the wording in Security Council resolutions can in fact be construed by a simple literal

[28] For more discussion on the effectiveness of Security Council Resolutions see for example Andrea Bianchi, 'Assessing the Effectiveness of the UN Security Council's Anti-Terrorism Measures: The Quest for Legitimacy and Cohesion', *The European Journal of International Law,* Vol. 17, No.5, EJIL 17, 881-919.

[29] The Vienna Convention on the Law of Treaties 1969. Hereinafter referred to as 'VCLT'.

[30] Ethymios Papastavridis, 'Interpretation of Security Resolutions under Chapter VII in the Aftermath of the Iraqi Crisis', *The International and Comparative Law Quarterly,* Vol. 56, No. 1 (Jan., 2007), pp. 83-118, at 95-97. The article develops the 'most coherent analytical framework for the hermeneutics of the Resolutions of Security Council', through the idea of 'interpretive communities' that construe the wording and true meaning of SCRs. According to Papastavradis, the theory of interpretation developed by Stanley Fish is most appropriate and 'best understood as a way of speaking about the power of institutional settings, within which assumptions and beliefs become a matter of common sense'. This theory places great emphasis on the contextual surroundings of the text to interpret its true meaning; 'interpretation is constrained neither by the language of the text nor its context, but by the cultural assumptions within which both texts and contexts take shape for situated agents'. This theory does not envision the original purpose of the wording can be construed by a simple literal interpretation, rather 'in light of the position it occupies in that enterprise'.

[31] Papastavridis, ibid, at 95-97.

[32] See for example, Sovereignty over Pulau Litigan and Pulau Sipadan (Indonesia/Malaysia) (2002) ICJ Rep 625, ICGJ 54 (ICJ 2002), 17th December 2002. 23-24, para 37:'The Court notes that Indonesia is not a party to the Vienna Convention of 23 May 1969 on the Law of Treaties; the Court would nevertheless recall that, in accordance with customary international law, reflected in Articles 31 and 32 of that Convention: a treaty must be interpreted in good faith…Moreover, with respect to Article 31, paragraph 3, the Court has had the occasion to state that this provision also reflects customary law… Indonesia does not dispute that these are the applicable rules'. The ICJ has stated in various cases that the general applicability of the rules forms customary international law. See Arbitral Award of 31 July 1989 (Guinea-Bissau v Senegal) Judgment, [1991] ICJ Reports 53, at 70, para 48: 'These principles are reflected in Articles 31 and 32 of the Vienna Convention on the Law of Treaties, which may in many respects be considered as a codification of existing customary international law on the point'.

interpretation. Employing a literal reading does not diminish the position that a resolution occupies in that enterprise, but instead, reinforces it by way of giving meaning to the resolution in its context and in light of its object and purpose. Thus, the starting point to interpret a resolution is the contextualized ordinary meaning from which the true meaning of the text can be construed.

Based on this, in order to understand whether Security Council resolutions can apply to OCTAs, the following discussion will employ the general rules of interpretation found in the Vienna Convention and determine whether all types of Security Council resolutions should be subject to the Vienna Convention.

2.3 Nature of Security Council's Actions in Relation to Terrorism

At this point, it is useful to distinguish between the two types of resolutions that have been established by the Security Council when acting under Articles 39, 41 and 42 of the UN Charter. By taking measures under Articles 41 and 42, the Council enforces the peace in relation to terrorism and these are reflected in both legislative and executive resolutions. Ergo, the character of these resolutions has become central to the debate on whether they constitute a form of legislation on the part of the Security Council. When the Security Council acts in a law-making capacity and enforces peace through the creation of new rules, it adopts resolutions that are legislative in nature. There are convincing grounds to believe that legislative resolutions have a similar legal status or stature to that of international treaties.[33] These resolutions contrast greatly with executive resolutions, which impose contextually different obligations on Member States, as we shall see next. Executive resolutions impose obligations of a general nature and legislative resolutions enforce obligations relating to a specific situation.

As well as being executive or legislative, Security Council resolutions can be binding, non-binding or contain both binding and non-parting parts. Typical resolutions adopted by the Security Council are described as 'primarily of executive character, namely individuated, expeditious and finite'.[34] Whether a resolution has binding effects is contingent on the language employed. For instance, paragraphs which 'recommend', 'calls upon' or 'urge' states to act are generally not interpreted as binding

[33] For discussion on the role of the Security Council as legislator, see for example Keith Harper, 'Does the United Nations Security Council Have the Competence to Act as Court and Legislature?', *New York University Journal of International Law and Politics*, 27, (1994) pp. 103-157. The article discusses the early evolution of the Council's practice, which embraces roles not only of an executive nature, but arguably exceeds its competencies by carrying out both legislative and judicial functions in response to threats to international peace and security. Note this article was published pre-9/11. See also Stefan Talmon, 'The Security Council as World Legislature', *American Journal of International Law*, Vol. 99:175, (2005).
[34] Nicholas Tsagourias, 'Security Council Legislation, Article 2 (7) of the UN Charter, and the Principle of Subsidiarity', *Leiden Journal of International Law*, 24 (2011), pp.539-559, at p. 540.

language.[35] On the contrary, where the Security Council 'decides' upon a matter it adopts binding paragraphs where a particular choice of language is used imposing a legal obligation for states to comply with this decision as stipulated under Article 24 of the UN Charter.[36] As Higgins succinctly states:

> the binding or non-binding nature of […] resolutions turns not upon whether they are to be regarded as 'Chapter VI' or 'Chapter VII' resolutions … but upon whether the parties intended them to be "decisions" or "recommendations".[37]

It can be said then that any decision of the Security Council is legally binding upon all UN Member States, whether or not the text of the resolution explicitly refers to Chapter VII.[38] The deciding factor to construe whether a resolution is either executive or legislative depends on if it imposes specific obligations for specific purposes. Where the Security Council makes a legally binding decision, the language of the resolution delivers its intentions with clear wording and articulates with great authority the nature of its decision, as we shall see later on.

In addition to executive and legislative resolutions, the Security Council's official documents include meeting notes, presidential statements, state representative statements, and reports of the Secretary-General, all of which feature in the following analysis. Similar documents are produced by the General Assembly (albeit that there are no presidential statements or Secretary-General reports from the GA) and are incorporated in the analysis to determine whether UN outputs can prevent and suppress OCTAs. These documents allow for greater understanding of either the Security Council or the General Assembly's overall position regarding the terrorist activities in question. Meeting notes can reveal a member state's stance on the issue, presidential statements provide a consensus of the Security Council's standpoint on certain questions, and reports of the Secretary-General presents on the issues that feature in resolutions. Also useful for research are press releases, which are declarations to the media made in advance of official documents.[39] Press releases are not official

[35] Though, the author acknowledges that there is contrasting scholarly debate upon the binding terms of UN resolutions. See Gregory H. Fox, Kristen E. Boon and Isaac Jenkins, 'The Contributions of United Nations Security Council Resolutions to the Law of Non-International Armed Conflict: New Evidence of Customary International Law,' *American University Law Review*: Vol. 67: Iss. 3, Article 1, (2018). The authors discuss the contradicting views of binding terms used in UNSC whereby *'some P5 states view only the verb "decides" as signalling a binding obligation, while others declare they are more flexible, noting that a reference to Chapter VII would be sufficient',* at p. 661.

[36] Article 24 (1) of the UN Charter stipulates that the Security Council is conferred upon it the 'primary responsibility for the maintenance of international peace and security'.

[37] Rosalyn Higgins, 'The Advisory Opinion on Namibia: Which UN Resolutions Are Binding Under Article 25 of the Charter?' *The ICLQ,* Vol. 21, No. 2, (April. 1972) pp. 270 – 286, at p. 281 – 282.

[38] Dan Joyner, 'Legal Bindingness of Security Council Resolutions Generally, and Resolution 2334 on the Israeli Settlements in Particular,' *EJIL: Talk!: Blog of the Eur. J. Intl'l L.*, (January 9, 2017) available at https://www.ejiltalk.org/legal-bindingness-of-security-council-resolutions-generally-and-resolution-2334-on-the-israeli-settlements-in-particular/

[39] United Nations website, 'UN Documentation: Overview', last updated May 20, 2021. Available at https://research.un.org/en/docs/pressreleases (accessed 8 July 2021).

documents but nonetheless, provide an overview of the meetings that are held and can be useful information to supplement Resolutions.

Unlike Resolutions, these documents do not have any binding effects and do not impose legal obligations on member states. They are, however, valuable as additional sources of information that can further our understanding of the UN's position on relative issues. As such, the following analysis contains a heterogeneous mix of materials, some of which are binding, some of which are not and some of which may be, and subsequent discussion will expand on how these are interpreted in light of OCTAs. First, the next section explores executive resolutions to determine whether they apply to OCTAs.

2.3.1 Executive Security Council Resolutions Concerning OCTAs

The Security Council has adopted various resolutions that concern terrorist activities committed by ISIS and they form part of this discussion to interpret whether they can be applied to regulate OCTAs. In 2005, the Security Council adopted Resolution 1624 to strengthen international cooperation regarding the security of international borders. Interestingly, the resolution condemned the incitement and glorification of terrorist acts, where the Security Council 'calls upon all states' to:

> (a) Prohibit by law incitement to commit a terrorist act or acts;
>
> (b) Prevent such conduct;
>
> (c) Deny safe haven to any persons with respect to who there is credible and relevant information giving serious reasons for considering that they have been guilty of such conduct.[40]

The Security Council's efforts to prohibit incitement to some extent reflects its position on certain OCTAs. Resolution 1624 is a notable effort by the Security Council to address the more severe category of OCTAs as it concerns those acts that can amount to international wrongful acts in and by themselves. The Security Council considers the proximity of incitement to terrorist violence as sufficiently close that it requires international legal attention and international cooperation for its prevention. By explicitly addressing incitement, the Security Council emphasizes the threatening nature of certain OCTAs by drawing attention to this OCTA as a matter of international peace and security. This further affirms the Security Council's endeavour to address terrorist activities that could otherwise encourage violent behaviour and legitimise structural violence by recognising and condemning the incitement to terrorism.

An important point to note, however, is the non-binding language used by the Security Council in Resolution 1624. As discussed in the previous section, by 'calling upon' states the Security Council

[40] S/RES/1624 of 14 September 2005.

does not make it obligatory for states to behave in such a way that would ensure the prohibition of incitement as it concerns terrorist acts. Instead, it appears that Resolution 1624 is an attempt by the Security Council to emphasize the danger of such terrorist acts and to inform states of the need to prevent such conduct. The resolution, however, stops short of ensuring the prohibition to the incitement of terrorism by its reluctance to impose a binding obligation where a breach of such would be a clear violation of international law.

The Security Council's efforts to address terrorism and terrorist use of the internet started to increase in 2013, when ISIS began its online terrorist campaign through the use of social media platforms. In response, resolutions started to recognise the dangers of using technology and presented the internet as a serious enabler to terrorism. Resolution 2129 (2013)[41] is a prime example, and recognises:

> the evolving nexus between terrorism and information and communication technologies, in particular the Internet, and the use of such technologies to commit terrorist acts, and to facilitate such acts through their use to incite, recruit, fund or plan terrorist acts…[42]

Whilst the Security Council acts in an executive manner in its adoption of Resolution 2129, its decision-making capacity seems to be exercised in language of a non-binding nature. The Security Council 'notes' a growing association between the use of the internet and terrorism. Rather than imposing an obligation upon states to act, the use of the term 'notes' acknowledges the relation by recognising a nexus between the exploitation of the internet and terrorist groups. The language employed in Resolution 2129 lacks the requirement of state action. Nevertheless, the Security Council has made significant headway in bringing attention to Member States as it concerns terrorist exploitation of the internet and this almost certainly coincides with the growing online presence of ISIS and its cyber caliphate infiltrating the internet domain.[43]

The nexus between the use of the internet and OCTAs is further highlighted in Resolution 2133 (2014). This resolution specifies that the financing of terrorism provides indispensable support to terrorist recruitment efforts and adds terrorist financing to the increasing list of counter-terror measures that Member States should address.[44] Resolution 2133 does not directly address terrorist

[41] S/RES/2129 of 17 December 2013.
[42] Ibid, at para 14.
[43] S/RES/1624 of 14 September 2005. The preambular paragraphs refer directly to the increasing use of the internet to commit terrorist acts: *'All States must cooperate fully in the fight against terrorism, in accordance with their obligations under international law, in order to find, deny safe haven and bring to justice, on the basis of the principle of extradite or prosecute, any person who supports, facilitates, participates or attempts to participate in the financing, planning, preparation or commission of terrorist acts or provides safe havens'.*
[44] S/RES/2133 of 27 January 2014 at para 7. The Security Council notes that: '*ransom payments to terrorist groups are one of the sources of income which supports their recruitment efforts, strengthens their operational capacity to organise and carry out terrorist attacks…'*

use of the internet and its language is non-binding. However, it is an executive resolution that recognises the interdependency of OCTAs and emphasises that such activities are necessary to the functioning of terrorist organisations.

As the presence of ISIS remains prominent, OCTAs continue to be recognised by the Security Council. Resolution 2249 (2015) unequivocally condemns the terrorist attacks carried out by ISIS and declares that the group constitutes an 'unprecedented' threat to international peace and security.[45] The Security Council:

> calls upon Member States that have the capacity to do so to take all necessary measures, in compliance with international law, in particular with the United Nations Charter, as well as international human rights, refugee and humanitarian law, on the territory under the control of ISIL also known as Da'esh, in Syria and Iraq, to redouble and coordinate their efforts to prevent and suppress terrorist acts committed specifically by ISIL…[46]

The Security Council's use of semantics is particularly interesting when it comes to determining actionable measures that can be taken by Member States in response to ISIS and international terrorism generally. Amongst other counter-terror resolutions, Resolution 2249 'calls upon' states to take 'all necessary measures' to suppress terrorist acts, a phrase that appears in Resolution 1373 (2001) and imposes legally binding obligations. Whilst the Security Council is essentially asking Member States to make serious efforts to prevent ISIS' continued terrorist acts, there has been some scholarly debate surrounding Resolution 2249 and whether it imposes legally binding obligations upon states.[47]

Resolution 2499 recommends that states redouble and coordinate their counter-terror efforts specifically in the territories of both Syria and Iraq.[48] Not only does this resolution limit measures to ISIS' conflict zones, but it intentionally does not deal with what measures can be imposed beyond the states of Syria and Iraq, such as Afghanistan or Somalia, and which have comparably strong ISIS presence in their territories. Resolution 2499 appears executive in nature. Yet, Resolution 2499 does not actually authorise any actions against ISIS nor does it explicitly allow for the use of force against ISIS. It can therefore be said that Resolution 2499 remains 'traditional in its vagueness' and leaves

[45] S/RES/2499 of 20 November 2015.
[46] Ibid, at para 5.
[47] See e.g. Dapo Akande and Marko Milanovic, 'The Constructive Ambiguity of the Security Council's ISIS Resolution', *EJIL: Talk!: Blog of the Eur. J. Intl'l L.*, (November 21, 2015) available at https://www.ejiltalk.org/the-constructive-ambiguity-of-the-security-councils-isis-resolution/. The authors discuss Resolution 2499's ambiguous nature and debate whether the language used can be construed as legally binding. See also Elena Cirkovic, 'Incomplete World Order: United Nations Security Council Resolution 2249 (2015) and the Use of Force in International Law', *Comparative Law Review*, Vol. 8, (2017).
[48] Article 25 of the UN Charter provides that UN Member States 'agree to accept and carry out the decisions of the Security Council'.

open a wide discretion for states to interpret what measures could be taken when it comes to preventing ISIS' continued terrorist acts in specified territories.[49]

The Security's Council commitment to preventing terrorism appears consistently throughout its work including various reports, meetings and statements solidifying its agenda on countering all forms of terrorism. The analysis of such efforts can expand our understanding as to the status of OCTAs in accordance with Article 32 VCLT. This is particularly prudent in a Presidential Statement where the Security Council condemns all OCTAs. In this statement, the President:

> [expresses] concern at the increased use, in a globalized society, by terrorists of new information and communication technologies, and the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities and underlines the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts…[50]

The Security Council has affirmed in various resolutions of its desire to prevent terrorists from exploiting the internet and using such tools to commit political violence. Resolutions reiterate concern over the use of OCTAs and highlight the expectation of Member States to aid in alleviating such threats. The Council recognises the threat that OCTAs pose and the plausibility of these activities creating and perpetuating violent behaviour that can then be used to legitimise structural violence. Whilst asserting the new age threats of cyberterrorism, counter-terror resolutions place significant onus on the responsibility of states to engage in all measures that are necessary to curb the continued presence of ISIS online. By underlining the need for states to act collectively to suppress cyberterrorism, the Security Council identifies the link between OCTAs and the catalysing effect it may have on prospective terrorist acts further emphasizing the potential for OCTAs to threaten negative peace as well as positive peace. It also recognises that achieving this mandate requires a committed effort from all Member States and a unified approach across the international community.

In 2015, ISIS were responsible for a series of terrorist attacks in Paris,[51] Ankara,[52] Beirut[53] and California.[54] Having been condemned by the Security Council, this has led to a growing number of resolutions adopted in response to such threats to the peace. Notably, Resolution 2253 (2015) concerns the freezing of assets of ISIS, Al-Qaeda and associated terrorist groups. In light of these ISIS terrorist attacks, the Security Council 'decides that' the Al-Qaida Sanctions list extends to include ISIS

[49] Peter Hilpold, 'The Fight Against Terrorism and SC Resolution 2249 (2015): Towards a More Hobbesian or a More Kantian International Society?' *Indian Journal of International Law* (2015) 55 (4): 535 – 555, at p. 539.
[50] S/PRST/2013/1 Statement by the President of the Security Council of 15 January 2013.
[51] SC/12121, Security Council Press Release of 13 November 2015.
[52] SC/12132, Security Council Press Release of 20 November 2015.
[53] SC/12120, Security Council Press Release of 13 November 2015.
[54] Mr. Osbourne of the United Kingdom speaking in S/PV.7587 United Nations Security Council 7587th Meeting (17 December 2015) at 11, identifies the most recent tragic terrorist attacks that resulted in various loss of lives.

and makes it a legal obligation that all states are to freeze assets of those associated to ISIS and Al-Qaeda and this includes:

> (a) participating in the financing, planning, facilitating, preparing or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of;
>
> (b) supplying, selling or transferring arms and related materiel to
>
> (c) recruiting for; or otherwise supporting acts or activities of Al-Qaida, ISIL, or any cell, affiliate, splinter group or derivative thereof.[55]

The Security Council imposes a legal obligation upon states to ensure that certain activities carried out by ISIS for the purposes of terrorism are forbidden under a dedicated sanctions list, implementing measures directly applicable to proscribed circumstances. From this, it can be said that the Security Council's approach to preventing terrorism is entrenched in a general desire to eliminate threats to both concepts of the peace theory. The condemnation of these activities plays a significant role in the Security Council's counterterrorism agenda and reiterates the need to impede OCTAs that could encourage structural violence and potentially develop to threaten negative peace. Whilst Resolution 2253 contains both binding and non-binding parts, the Security Council adopts a predominantly executive resolution by stipulating that specific offences committed by ISIS are prohibited and must be addressed by states.

In enforcing measures to prevent terrorism, Resolution 2253 also identifies propaganda (alongside incitement) through the use of the internet and social media.[56] The Council requires that states are to 'act cooperatively to prevent' these activities by 'developing effective counter narratives' within their domestic laws.[57] However, the Resolution does not provide a definition of propaganda or recruitment within its substantive provisions so we must explore other relevant sources to determine what might be included in the definition of propaganda and recruitment.

In the Sixth Report of the Secretary-General, the threat of online propaganda presented in the form of online magazines, as well as 'propaganda videos, articles and imagery.[58] Further to this, the

---

[55] S/RES/2253 of 17 December 2015 at para 3 (a) – (c).

[56] The Security Council has recognised activities of recruitment and propaganda and also incitement to commit terrorist acts through the use of the internet, otherwise known as cyberterrorism in this research. See UNSC Resolutions S/RES/2129 of 17 December 2013 at para 13 and 14; S/RES/2133 of 27 January 2014 at para 1 and 7; S/RES/2170 of 15 August 2014 at paras 2, 7, 9, 11 and 18; S/RES/2178 of 24 September 2014 at para 7; S/RES/2253 of 17 December 2015 at para 22; S/RES/2322 of 12 December 2016 at para 14; S/RES/2368 of 20 July 2017 at para 23.

[57] S/RES/2253 (2015) at para 22. The remaining resolution stipulates that the activities aforementioned are to be prevented *'by developing effective counter narratives, while respecting human rights and fundamental freedoms and in compliance with obligations under international law and stresses the importance of cooperation with civil society and the private sector in this endeavour'.*

[58] S/2018/80 of 31 January 2018, Sixth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) To International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat, at para 8 and para 15.

Counter-Terrorism Committee Executive Directorate (CTED) has identified different types of ISIS propaganda as:

> videos inspired by popular contemporary culture, such as movies and videogames. The portrayal of violence and force (e.g., recordings of beheadings or images of innocent victims allegedly killed by enemies of ISIL) is designed to resonate powerfully with aggrieved or marginalized individuals. In propaganda aimed at other market segments, images of food, kittens and babies seek to cast ISIL in a favourable light and portray the "normality" of life in ISIL-controlled territories. Some online recruitment campaigns now aim at skilled professionals, such as hackers, web designers, and developers of mobile telephone applications and dedicated social media platforms, both open and encrypted. Other campaigns are targeted at doctors, engineers and other professionals.[59]

The report recognises the novel ways in which terrorist groups can disseminate their propaganda, targeting specific groups that may be useful in contributing to its operations or whom may be more susceptible to joining a terrorist group. It is clear that terrorist propaganda is not confined to a particular mode or method, rather that technology allows terrorists to exploit the internet insofar that their propaganda can be disseminated beyond the once restrictive and traditional methods that were offline. The CTED report also tells us that recruitment and propaganda are interconnected activities often carried out by terrorist groups. The launch of cyber terrorist recruitment campaigns is a form of propaganda by way of encouraging or promoting terrorist ideologies through engaging with supporters or individuals. On the ease of online recruitment, the report posits that:

> social media [is] effective for recruitment because of their capacity to launch decentralized campaigns through volunteers who re-post content…[and] certainly makes it easier for radicalized individuals to connect with a terrorist recruiter.[60]

To add to this, the advent of technology facilitates terrorist activities to which:

> recruitment through encrypted messages poses difficult challenges for law enforcement and eventually for prosecution. Online messages by terrorist organizations have urged individuals to conduct terrorist acts or to join ISIL.[61]

The CTED report does not explicitly provide definitions of either recruitment or propaganda. Rather, it elaborates in detail what activities are considered under these terms as it relates to ISIS, something which Resolution 2253 does not provide. Looking at surrounding documents issued by the Security Council allows deeper interrogation as to the meaning of the terms employed by resolutions, whilst also informing us on the most recent developments surrounding these terrorist activities. For instance, Security Council meeting 7587th which discusses Resolution 2253 reveals that:

> the terrorists take advantage of weaknesses in financial and regulatory regimes to raise funds. They circumvent formal channels to avoid detection and exploit new technologies and tools to transfer resources. They have forged destructive and very profitable links with drug and criminal

[59] S/2016/49 of 20 January 2016, CTED, Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States, at para 43.
[60] Ibid, at para 42.
[61] Ibid, at para 403.

> syndicates, among others, and they abuse charitable causes to trick individuals to contribute. They are agile and have been far too successful in attaining resources for their heinous acts.[62]

In its meeting, the Security Council emphasises the impact of financing in facilitating terrorism and highlights the need to prevent such activity from manifesting. It appears that the Security Council holds a majority view in its condemnation of terrorist financing, propaganda and recruitment among other terrorist activities that exploit the internet. To some extent then, it can be said that the Security Council acknowledges that the use of the internet and cyber technologies catalyses the potential for political violence. The continued proliferation of these activities can and does foster an environment where such violent behaviour can become normalised within certain cultures, breeding a fertile ground for terrorists to legitimise structural violence.

Formal recognition of new age terrorism and its exploitation of the internet is again clearly expressed by the Security Council through Resolution 2322 (2016). The violent bombings in Brussels and Paris in 2015 and 2016 respectively, found online bomb making guides were available for public access and that home-made explosives were used to carry out the attacks.[63] In response, the Security Council made a declaratory statement to:

> [encourage] Member States to act cooperatively to prevent terrorists from recruiting, to counter their violent extremist propaganda and incitement on violence on the internet and social media, including by developing effective counter narratives…[64]

The Security Council reiterates the indispensable need for international cooperation to reduce and prevent cyber terrorist activities. The surge of online terrorist activity in addition to the occurrence of violent terrorist attacks leads the Security Council to plead for states to 'strengthen legal cooperation in the fight against terrorists in order to weave a legal and judicial dragnet across all regions of the world'.[65] The plight of enhancing international cooperation is further voiced by various states acknowledging that harmonising efforts is a key objective to address acts of cyberterrorism.[66] This includes the sharing of intelligence information, effective cooperation in mutual legal assistance and

---

[62] S/PV.7587, UNSC 7587th Meeting (17 December 2015) at p. 2. The President of the Security Council Meeting, Mr. Lew of the United States of America.

[63] EUROPOL, 'Changes in Modus Operandi of Islamic State (IS) Revisited', The Hague, (November 2016), available at https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited. The report identifies that 'instructions on how to produce TAPT [a home-made explosive] can be found on the internet on Jihadi websites and e-magazines (e.g. INSPIRE, DABIQ)'.

[64] S/RES/2322 of 12 December 2016. Resolution 2322 (2016) emphasises five major issues related to counter terrorist activities including mutual legal assistance and extradition, foreign terrorist fighters and returnees, the financing of terrorism, the proliferation of information technology and the role of multilateral agencies in preventing terrorism.

[65] Mr. Wu Haitao of China speaking at Security Council Meeting 7831st S/PV.7831 of 12 December 2016, at 19.

[66] Ibid. See e.g. Mr. Barro of Senegal submits that 'judicial cooperation remains the weakest link in the international fight against terrorism' at p. 20. Ms. Odour similarly echoes that 'the weak capacity of any one country to address effectively some of those new threats and challenges translates itself into an overall weakness in the entire international regime of criminal justice cooperation' at p. 4.

extradition as well as strengthening coordination between Member States.[67] The Security Council thus recognises the need for states to address OCTAs when exercising efforts to counter terrorism.

Whilst the resolution sets out recommendations that expressly tackle terrorist activities involving recruitment, propaganda and incitement using the internet and social media, it does not specifically refer to ISIS. Neither can Resolution 2322 be considered as binding since it does not impose any obligations upon states to condemn these terrorist activities completely. By using the term 'encourage', the Security Council persuades Members States to act together to prohibit these terrorist activities. The choice of language does not compel Member States to cooperate but just strongly recommends that they do so.

There are certain cyber terrorist activities identified by the Security Council as a matter necessary for international address. In the preamble of Resolution 2322, the Security Council:

> [expresses] concern at the continuing use, in a globalized society, by terrorists and their supporters, of information and communications technologies, in particular the Internet, to facilitate terrorist acts, and condemning their use to incite, recruit, fund, or plan terrorist acts.[68]

Not only does this preamble acknowledge terrorist exploitation of cyberspace, but it recognises specific terrorist activities that must be prevented, citing recruitment and financing and propaganda in its substantive paragraphs. By condemning these activities, there is normative value in the Security Council's language which strives towards peace by recognising OCTAs as impediments to achieving international peace and security. Resolution 2322 therefore addresses OCTAs and presents these terrorist activities as matters of international concern that states must actively try and discourage. This again, reaffirms the notion that the Security Council does in fact perceive OCTAs as threats to peace, hindering the achievement of the peace in both its negative and positive concepts.

Both Resolutions 2253 and 2322 reflect the threat of international terrorism, specifically recruitment, propaganda and incitement, and the Security Council's concern over the need to address these terrorist activities. This is further reaffirmed in Security Council meeting 7831st, in which Mr. Zagaynov of the Russian Federation acknowledges that:

---

[67] S/PV.7831, supra note 64. The Security Council meeting discusses various measures which must be enhanced in order to prevent and suppress OCTAs and cyber terrorism. Ms. Odour expresses a '… need to institutionalize and expand cooperation, the sharing of intelligence and data, training and technology and organization that can be shared without compromising national capabilities' at p. 4-5; Mr. Delattre of France on the adoption of Resolution 2322 (2016) opines that 'it highlights the need to use all available legal tools for cooperation in mutual legal assistance and extradition' at p. 25; Mr. Vitrenko of Ukraine is of the view that 'there is a growing need to provide the basis for timely sharing of imperative intelligence information when investigating terrorist activities and securing criminal evidence, apprehending suspects and preventing terrorist acts from being carried out' at p. 15.

[68] Ibid, at the preamble.

> one priority is to address the increase in radicalism, which is fuelled by unprecedented terrorist propaganda aimed primarily at youth. That propaganda has adapted to modern technological advances such as the Internet and social networks.[69]

Resolution 2396 (2017), which is adopted under Chapter VII, continues in the same vein by recognising the threat of OCTAs.[70] In its preambular paragraph Resolution 2396 reiterates the significance of using the internet and the role it plays in advancing terrorism. Terrorist groups create 'distorted narratives, which are utilized to polarize communities, recruit supporters and foreign terrorist fighters, mobilize resources and garner support from sympathisers…',[71] through exploiting the internet and social media. The operative paragraphs of Resolution 2396 contain both binding and non-binding parts in relation to terrorist financing and recruitment. The Security Council specifically addresses foreign terrorist fighters and restates that:

> foreign terrorist fighters and those who finance or otherwise facilitate their travel and subsequent activities may be eligible for inclusion on the ISIL (Da'esh) and Al-Qaida Sanctions List… where they participate in the financing, planning, facilitating, preparing or perpetrating of acts or activities… or recruiting for… acts or activities of Al-Qaida, ISIL, or any cell, affiliate, splinter group or derivative thereof…[72]

The Security Council adopts an executive tone when identifying specifically ISIS and Al-Qaeda related terrorism. However, Resolution 2396 falls short of imposing legal obligations upon the state to take action and address OCTAs in relation to foreign terrorist fighters. Rather, the binding obligations it imposes on states are in relation to gathering information on travel, passenger data, and suspected terrorists and to create systems to collect biometric data.[73] Thus, while Resolution 2396 acknowledges OCTAs, it does so through the use of non-binding language that does not coerce states to take action.

There is no doubt that the Security Council recognises the danger of OCTAs and their role in proliferating terrorism. In Resolution 2396's corresponding meeting 8148th, Mr. Lie Cheng of China expresses that:

> the coordinating role of the United Nations should be given full play and efforts must be made to curtail the terrorist organisations' use of the Internet for propaganda, recruitment and other terrorist activities.[74]

The Council consistently and continually addresses the threat of cyberterrorism through its associating delegates, with Secretary-General Reports emphasising the dangers of cyberterrorism and the

[69] S/PV.7831, supra note 64, at p. 24.
[70] S/RES/2396 of 21 Dec. 2017.
[71] Ibid, in preamble.
[72] Ibid, at para 42.
[73] Ibid, at para 11 – 13, para 15.
[74] Mr. Lie Cheng of China speaking at Security Council Meeting 8148th, S/PV.8148 of 21 December 2017, at p. 6.

continued proliferation of ISIS' online presence.[75] However, the Security the Council is yet to adopt a binding executive resolution that specifically and directly addresses OCTAs as a threat to the peace. For instance, Resolution 2368 (2017) echoes its preceding resolutions to address ISIS terrorist recruitment and financing using the internet in its operative paragraphs.[76] However, the beginning of the resolution prioritises the freezing of assets, arms embargo and travel bans as its primary concern.[77] Similarly, Resolution 2178 (2014) concerns foreign terrorist fighters and preventing their recruitment.[78] The Security Council places great concern on violent extremism that is sectarian violence and the commission of terrorist acts by foreign terrorist fighters, rather than the act of terrorist recruitment itself.[79] Again, Resolution 2170 addresses individuals connected with ISIS and Al-Qaeda groups, condemning recruitment and discouraging foreign terrorist fighters to travel to conflict zones of Syria and Iraq.[80]

Whilst these activities still appear throughout the main body of counter-terror resolutions and it is clear that they threaten international peace and security, its locus within the framework of the resolution reflects the position within which the Security Council attributes attention towards OCTAs. There is compelling ground to argue that imposing binding obligations to address OCTAs will accentuate their importance within the counterterrorism discourse and call on states to prohibit such activities as a primary means of combatting international terrorism. Until then, the pressure upon states to tackle OCTAs is subsidiary and OCTAs may be seen as a peripheral threat rather than one that poses imminent danger to the security of states. To add to this, the non-binding nature of executive resolutions means that states have a wide discretion to choose whether or not to implement measures within their own national jurisdictions. Priority to do so is largely attributed to the demand for such measures to be put in place in light of every states own national security agenda.[81] Resolution

[75] S/2016/830 of 30 September 2016, Third Report of The Secretary-General on The Threat Posed by ISIL (Da'esh) To International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat. The Secretary-General reiterates the continuing dangers of terrorist groups online; 'ISIL continues to assert itself in cyberspace. Potential recruits are increasingly instructed by ISIL recruiters to use closed forums and encrypted messaging systems…This ongoing recruitment activity is helping to build an ever-increasing transnational network of ISIL sympathizers and fighters, thereby obviating the need for physical proximity between leaders and operational figures. Moreover, ISIL continues to be a prolific publisher of online propaganda, the continued military pressure notwithstanding.' See also Presidential Statements reiterating the dangers of ISIS; S/PRST/2016/6 of 11 May 2016 and Fourth Report of the Secretary-General on The Threat Posed By ISIL (Da'esh) To International Peace And Security And The Range Of United Nations Efforts In Support Of Member States In Countering The Threat, S/2017/97 of 2 February 2017.
[76] S/RES/2368 of 20 July 2017, at para 23.
[77] Ibid.
[78] S/RES/2178 of 24 September 2014, at para 4.
[79] Ibid, at para 1.
[80] S/RES/2170 of 15 August 2014, at paras 7 and 9.
[81] See e.g. S/2016/50 of 28 January 2016. Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counterterrorism addressed to the President of the Security Council, at para 48-52. The Security Council recognises the different national strategies adopted to counter incitement through engagement with local communities and civil society. For example, the UK introduced the Prevent programme with the Home Office working with local authorities and in Australia, the Living Safe Together initiative was announced to counter violent extremism.

2178 (2014) saw only 10 of 21 states having implemented measures concerning the financing of foreign terrorist fighters and many of these 21 states having not yet fully criminalised acts of the perpetration, planning, or preparation of, or participation in, terrorist acts.[82]

More recently, in the Security Council's 8460th meeting of Feb. 11, 2019, France considered the prevention of the use of the internet as their third national priority.[83] In the same meeting, however, China makes specific reference on the need to 'focus on enhancing international cooperation in combating cyberterrorism, terrorist financing and the spread of extremist ideologies'.[84] Similarly, the Russian Federation highlights the 'expanding ideological, propaganda and recruitment activities, which make intelligent use of information and communications technologies' and must be diminished.[85] Despite the Security Council making various suggestions as to the dangers of cyberterrorism, enforcing adequate measures to prevent terrorist groups from exploiting the internet is a responsibility that rests on the individual will of Member States. Even so, such a responsibility is subject to the discretion of states when it comes to adhering to obligations set out in executive resolutions that are adopted in the face of counterterrorism.

The Security Council continues to mandate the prevention and suppression of financing and recruitment via the adoption of Resolution 2462 (2019) under Chapter VII of the UN Charter.[86] Affirming Resolution 1373 (2001), the Security Council adopts the first comprehensive UN resolution on countering the financing of terrorism. The preamble highlights the importance of the FATF standards to tackling money laundering and counterterrorism financing and encourages states to adhere to the FATF framework. Within the resolution, there are broad prohibitions on terrorist financing and support including calling upon Member States 'to reinforce the access to information and terrorist financing analytical capacity of their financial intelligence units' and to cooperate with the private sector.[87] Interestingly, the Resolution 'demands' that states take all measures to counter terrorism and the financing of terrorism, which infers a strong requirement to adhere to this provision. Such a demand, however, is not one that appears to compel a result. If the Resolution demanded for states to implement all measures to counter terrorism and the financing of terrorism, the use of language would impose an obligation for states to achieve a result. Instead, the Security Council makes a demand for certain behaviour of states as it relates to countering terrorism where that demand can be satisfied by states taking all measures to counter terrorism and terrorist financing, irrespective of

[82] S/2015/338 of 14 May 2015. Letter dated 13 May 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counterterrorism addressed to the President of the Security Council.
[83] S/PV.8460 of Feb. 11, 2019, at p. 13.
[84] Ibid, at p. 11.
[85] Ibid, at p. 9.
[86] S/RES/2462 of 28 March 2019.
[87] Ibid, at para 16.

whether all measures are actually taken by states or not. In this sense then, the language used in Resolution 2462 again emphasizes the discretion for states to choose whether or not to comply with the operative paragraphs of this executive resolution. Moreover, subsequent language of the resolution calls upon, urges and encourages states to take action, which again, falls short of imposing decisive obligations on states that could otherwise compel specific behaviour.

Resolution 2482 (2019) follows in a similar manner, by reiterating the dangers caused by terrorism and organised crime as well as stressing the need for states to counter corruption, money-laundering and terrorist financing.[88] The language adopted by the Security Council remains non-binding and limits any obligatory action by 'calling upon' states to engage in measures to prevent terrorism and organised crime. To add to this, the Resolution does not provide a definition of organised crime, despite it having a distinct legal regime from terrorism. Though Resolution 2482 is not a Chapter VII resolution and does not activate obligations for states, the lack of legal clarity is problematic particularly where legal and political challenges pervade the field of terrorism.[89]

From the above analysis, it can be said that the Security Council has adopted executive resolutions encompassing both binding and non-binding parts that specifically address OCTAs committed by ISIS. OCTAs consistently appear within counter-terror resolutions and this can be said to reflect the Security Council's mandate to curtail this issue. It is clear that the Security Council perceives OCTAs are impediments to achieving peace by legitimising structural violence with the potential to escalate into the possibility of conflict. In particular, Resolution 1624 (2005) specifically pertains to the prohibition of incitement to commit terrorist acts, which is distinguished as an OCTA that has the potential to violate international law. Even with the loss of territorial control, it is clear that ISIS remains a continuing terror threat and speculations of an ongoing growth into a global covert network has led the Security Council to emphasize that there can be no 'complacency' afforded when it comes to the suppression of ISIS and its terrorist activities.[90]

Yet, despite the Security Council recognising the role of OCTAs within terrorism, the resolutions adopted in relation to terrorist use of the internet and technologies makes no explicit condemnation of these terrorist activities as unlawful acts that violate international law. Rather, the Security Council appears to address OCTAs as subsidiary acts which, albeit perpetuate terrorism, do not warrant the need for prevention under an independent legal obligation. It seems that the Security Council imposes

[88] S/RES/2482 of 19 July 2019.
[89] Fionnuala Ní Aoláin, 'A Post-Morten on UN Security Council Resolution 2482 on Organized Crime and Counter-Terrorism', *Just Security* (August 12, 2019). Available at https://www.justsecurity.org/65777/a-post-mortem-on-un-security-council-resolution-2482-on-organized-crime-and-counter-terrorism/ (accessed 4 April 2020).
[90] Security Council Meeting Coverage, Voronkov. V., 'ISIL/Da'esh Continues Evolution into Covert Global Network Enjoying Access to Millions of Dollars, Top Anti-Terrorism Official Tells Security Council', SC/13697 of Feb. 11, 2019.

a general duty for states to prevent terrorism and considers OCTAs to fall within this general duty. The reluctance in addressing OCTAs as international delicts means that their suppression under international law is contingent upon states own volition and will, rather than regarding its prevention as a legal duty under which distinct obligations might flow. In doing so, the Security Council tacitly renders the prevention of terrorism to include that of OCTAs, when in reality, the course of the former cannot be achieved without clear and precise direction to prohibit the latter. Given this, one can conclude that there are gaps afforded in the protection of states against OCTAs under the Security Council's executive resolutions.

2.3.2 Legislative Security Council Resolutions Concerning OCTAs

In the last century the rise of terrorism has pushed the once predominantly executive body of the Security Council to what some now consider as a 'world legislator'.[91] After the events of September 11, 2001, matters of terrorism have fallen squarely into the hands of the Security Council. Resolution 1368 (2001) was adopted with immediate effect and unequivocally condemned the 9/11 terrorist attacks, concluding that the Security Council is prepared to take all necessary steps to respond to the attacks and combat all forms of terrorism in accordance with the UN Charter.[92] Most importantly, this resolution concludes by reaffirming the right to self-defence as stipulated under Article 51 of the UN Charter which permits states to exercise this right to fight off armed attacks by terrorist groups.[93]

Shortly after, the Security Council adopted Resolution 1373 (2001), which 'broke new ground' by exercising what can be seen as primarily legislative powers for the very first time, taking an unprecedented step in order to achieve its mandate.[94] Resolution 1373 (2001) has been monumental in the UN's counterterrorism efforts and it has been described as a 'departure' for the Security Council which has ordinarily maintained an executive function.[95] Resolution 1373 makes a formal declaration in its preambular paragraph that sets the agenda for countering terrorism on an international level, by famously declaring that:

> …any act of international terrorism, constitute[s] a threat to international peace and security.[96]

---

[91] Talmon, supra note 33.
[92] S/RES/1368 of Sept. 12, 2001, at para 3. The Security Council emphasizes the importance of international cooperation and calls on states 'to work together urgently to bring to justice the perpetrators, organizers and sponsors of these terrorist attacks'.
[93] Ibid, at para 5. The Security Council 'expresses its readiness to take all necessary steps to respond to the terrorist attacks of 11 September 2001, and to combat all forms of terrorism, in accordance with its responsibilities under the Charter of the United Nations'.
[94] See Jane E. Stromseth, 'An Imperial Security Council? Implementing Security Council Resolutions 1373 and 1390', *Proceedings of the Annual Meeting (ASIL),* Vol. 97, (April 2-5, 2003), pp. 41-45.
[95] Eric Rosand 'Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight Against Terrorism', *The American Journal of International Law*, Vol/ 97, No.2 (Apr. 2003), pp. 333-34, at p. 333.
[96] S/RES/1373 of 28 September 2001.

Whilst the adoption of Resolution 1373 could be seen as a 'natural extension of the Security Council's traditional crisis management role',[97] the fundamental question remains as to firstly, whether this resolution contributes towards countering cyberterrorism generally, and secondly, whether the wording of this resolution can be interpreted to address OCTAs specifically.

First, let us refer to the general rule of interpretation as per Article 31(1) of the VCLT, 1969. We must begin by taking a literal and ordinary meaning of the text which is to take the provision as it stands. The Security Council, by condemning 'any act' of international terrorism as a threat to peace and security, does not specify the form or method in which terrorism may be executed. The events of 9/11 were launched from physically violent and destructive attacks. However, there is nothing to suggest that Resolution 1373 considers all forms of terrorism to manifest in this way. Rather, the provision is intentionally broad and described as having an 'untemporal and abstract' nature when it comes to imposing binding obligations.[98] The Security Council does not seek to condemn one particular type of terrorism, but instead leaves a purposefully wide scope to capture any prospective terrorist acts that may be executed in unimaginable and unpredictable ways.[99] Resolution 1373 enforces obligations without reference to a specific time and place, denoting for the first time a critical moment where the Security Council has effectively laid down new rules of international law.[100]

Leading into more detailed prohibitions of terrorist acts, the resolution's operative paragraphs begin by imposing a binding obligation upon Member States to, inter alia, 'prevent and suppress the financing of terrorist acts', 'refrain from providing any support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups' and 'to take necessary steps to prevent the commission of terrorist acts'. [101] By identifying certain activities that require prevention, the Security Council recognises that such activities are fundamental to the operation of terrorist groups. It seems that measures to combat terrorism apply broadly with no specific reference to a particular conflict and that such obligations pertain more generally to the pervading threat to peace and security caused by global terrorism. In doing so, the Security Council condemns all forms of terrorism insofar that it regards any one method of terrorist activity irrespective

[97] Johnstone, supra note 9, at 284.
[98] Galván supra note 26, at p. 176.
[99] Rather, the Security Council reaffirms the earlier resolution S/RES/1368 (12 September 2001) para 1 which:
'Unequivocally condemns in the strongest terms the horrifying terrorist attacks which took place on 11 September 2001 in New York, Washington, D.C. and Pennsylvania and regards such acts, like any act of international terrorism, as a threat to international peace and security'.
[100] Talmon, supra note 33, p. 176. The author states that 'the hallmark of any international legislation is the general and abstract character of the obligations imposed'.
[101] S/RES/1373 (2001), para 1 (a) 'prevent and suppress the financing of terrorist acts'; para 2(a) 'refrain from providing any support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists'; para 2(b) 'take the necessary steps to prevent the commission of terrorist acts'.

of its character, to be expressly prohibited under international law. This is a direct result of the catastrophic events of the 9/11 attacks which grossly obstructed the achievement of negative peace by causing serious and direct violence to the civilian society.

In addition to this, there is no agreed definition of terrorism within the resolution or from the UN, which allows Member States to define themselves against whom these provisions shall apply. States have the discretion to apply these provisions of the resolution as they see fit. In other words, it is not for the Security Council to determine who, in fact, is a terrorist group and whether certain acts constitute terrorism. This interpretation is subject to each individual Member State. For instance, 'to take necessary steps' is overly vague. How does one define what is necessary? What is necessary for one state, may not be necessary for another. For one state this might mean ensuring there is a counterterrorism unit deployed and they endeavour to prevent the commission of terrorist groups by prohibiting all acts of terrorism including OCTAs. For another state, this might be a very basic step. States thus only need to do what is required under the circumstances to prevent the commission of terrorist acts. Thus, there remains creative ambiguity over the scope of Resolution 1373. With little semantic clarity to deny or approve specific acts of terrorism, its application is exceptionally broad.

The reluctance of Resolution 1373 to define the parameters for its application has far-reaching effects for the obligations it imposes upon Member States, further illustrating its constitutional capacity to act as legislator. The Council, in adopting Resolution 1373, has made a unilateral act of imposing legal obligations of a general and abstract nature insofar that all acts of terrorism, irrespective of scale, form or time of execution constitute a threat to international peace and security. Accepting that such obligations are binding upon Member States and using the interpretive framework of the Vienna Convention to interpret the resolution to include acts of terrorism executed via communication technologies, one can tentatively conclude that Resolution 1373 can be construed to assume that 'any act of international terrorism' must then by nature, include acts of cyber terrorism. In spite of its overly broad nature, the question remains as to whether OCTAs, which include recruitment, financing and propaganda of terrorism committed through cyberspace, can find themselves subject to the obligations set forth in Resolution 1373 as a means of preventing terrorism under international law.

During the time of the 9/11 attacks, terrorist activities such as recruitment were carried out in conventional ways, taking place in a physical space such as in mosques or camps in conflict zones and

terrorist material was often printed and distributed within these environments.[102] Though the use of technology was far less developed and access to the internet was not as prolific as it is today, a remarkable assertion made by the Security Council identified the 'use of communications technologies by terrorist groups' as a novel concern for the international community.[103] Whilst there is no elaboration on what communications technologies might encompass, the inclusion of such a provision reflects the matter as forming part of the counterterrorism discourse that is intrinsically linked to the attacks of 9/11. This terrorist activity is further elaborated during Security Council's 4413rd meeting which held that the 'exploitation of modern information technology [is] to spread the culture of extremism, violence and provocation'.[104] Alongside the internet, it is believed that communications consisted of telecommunications, wireless networks and cell phones, all of which became critical technology for Al-Qaeda to greatly facilitate its 'capacity-building and planning activities'[105] in the lead up to the 9/11 attacks.[106] Not only were these communications enabling Al-Qaeda to materialise their terrorist attacks, their proliferated use contributed significantly to the abhorrent violence by obstructing the maintenance of negative peace.

As a mechanism to ensure implementation of the resolution, the Counter-Terrorism Committee (the CTC) was established by Resolution 1373.[107] The Resolution called on states to report to the CTC measures taken to implement the Resolution within their domestic laws, which included adhering to the international conventions and assisting in strengthening national capacities for less able states.[108] This includes 'upgrading the capacity of each nation's legislation and executive machinery to fight terrorism'.[109] The creation of a Counter-Terrorism Committee Executive Directorate (CTED) further strengthened the institutional capacity of the CTC to assist states in building counterterrorism capabilities and coordinate the process of monitoring the implementation of the resolution.[110] Though

[102] See e.g. Martin Rudner, '"Electronic Jihad": The internet As Al-Qaeda's Catalyst for Global Terror', *Studies in Conflict & Terrorism*, 40:1, 10-23. The article discusses the use of the internet by Al-Qaeda and the various platforms used to further terrorism which has evolved from a time when recruitment required physical proximity.
[103] S/RES/1373 of 28 September 2001, at para 3 (a).
[104] S/PV.4413 of 12 November 2001, at 13.
[105] See Bruce Don et al., 'Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations,' Santa Monica, CA: RAND Corporation, 2007. Available at https://www.rand.org/pubs/technical_reports/TR454.html. The report highlights various ways in which terrorists use network technology for the purposes of committing terrorism, ranging from attack-focused activities to those of capacity-building and planning. The latter of which are concerned with recruitment and training of terrorists, forming low intensity operations resembling those of OCTAs.
[106] See Rudner, supra note 101. The article discusses the growing use of the Internet by terrorist groups, beginning from merely online references to jihadi literature to now an operational role consisting of recruitment, incitement, financing and catalysing terrorist attacks.
[107] S/RES/1373, at para 6.
[108] SC's 4618th Meeting Press Release, 'Security Council Considers Terrorists Threats to International Peace, Security', SC/7522 of Oct. 4, 2002.
[109] Eric Rosand, 'Security Council Resolution 1373, The Counter-Terrorism Committee, and the Fight Against Terrorism', *The American Journal of International Law*, Vol. 97, No. 2, (April, 2003), pp. 333 – 341, at p. 334. The author further discusses the efforts of the Counter-Terrorism Committee in achieving its objective to combat global terrorism.
[110] S/RES/1535 of March 26, 2004.

the CTC does not possess any enforcement mechanisms, reports affirming the implementation of Resolution 1373 was received from almost all states. In turn, this solidified the commitment to tackling terrorism worldwide and showcased some of the successful efforts of the CTC in relation to counterterrorism.[111]

As a result, trepidations over the use of the internet are of growing concern within the Security Council and an implementation guide produced by the CTED explains that the 'vast reach of the Internet [provide] terrorist organisations and sympathizers with a global pool of potential recruits'.[112] Member States echo the concern of terrorists taking advantage of developing technology providing them with 'a more global reach, with greater destructive and lethal capacities' having the potential of endangering the security of states in unprecedented ways.[113] It is clear that the Security Council considers the internet as a tool that terrorists can use to advance their ideological and violent campaigns, and this was recognised in as early as 2001. It seems then that the assertions regarding terrorists' exploitation of cyberspace have continued to surface and have now become more central to the counterterrorism regime of today.

This being said, Resolution 1373, similar to the Security Council's subsequent resolutions adopted following the 9/11 attacks in its counterterrorism agenda, does not prohibit OCTAs as specific terrorist activities. Whilst Resolution 1373 imposes a binding obligation upon states for the prevention and suppression of financing of terrorist acts and recruitment, states have the discretion to determine the nature of these terrorist activities in accordance with their national interests. On the one hand, Resolution 1373 is broad and general enough for all types of terrorist activities to fall within its scope, including OCTAs. On the other hand, its overly broad and general nature cannot precisely prohibit OCTAs because there is no specific obligation for states to do so. Though the wording of Resolution 1373 might be interpreted to apply to OCTAs as 'any act of international terrorism', the expectation that states will readily assume an obligation to prevent such activities leaves a doubtful gap in the law that cannot adequately be filled by a resolution that lacks distinct duties.

The second and only legislative resolution adopted under Chapter VII of the UN Charter is Resolution 1540 (2004). Concerning the proliferation of nuclear, chemical and biological weapons, the Resolution is enacted to prevent the use of weapons of mass destruction by terrorist groups.[114] Similar to Resolution 1373, Resolution 1540 created a committee to oversee the implementation of the

[111] SC/7522, supra note 107.
[112] UNSC CTED, 'Technical Guide to the Implementation of Security Council Resolution 1373 (2001) and other Relevant Resolutions' (2017), available at https://www.un.org/sc/ctc/wp-content/uploads/2017/08/CTED-Technical-Guide-2017.pdf
[113] Mr. Haraguchi of Japan, Security Council Meeting 4710th Meeting of 20 February 2003, S/PV.4710 at p. 3.
[114] S/RES/1540 of 28 April 2004.

resolution and to monitor the commitment of Member States in fulfilling the obligations as set out in the resolution.[115] In the same way that Resolution 1373 relates to no specific situation, Resolution 1540 does not correspond to a particular event nor a specific instance of threats to peace and security.[116] Rather, both Resolutions 1373 and 1540 are considered to 'relate to the form of behaviour rather than to particular manifestations of that form of behaviour' and thus significantly widens the scope of powers for the Security Council to act within its remits.[117] Resolution 1540 lays down binding rules on their proliferation and determines such weapons of mass destruction as a threat to international peace and security. Whilst the adoption of Resolution 1540 has further tested the legislative capacity of the Council, its applicability to OCTAs is limited. The resolution applies specifically to the use of particular weapons by terrorist groups, and prohibits any non-state actor to 'manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons'.[118] The resolution does not refer to terrorist use of technologies or the internet for the commission of terrorist acts or activities. The lack of relevance to terrorist activities generally indicates that Resolution 1540 cannot be interpreted to apply to OCTAs.

On the nature of Resolutions 1373 and 1540, there is little dispute that 'rather than issuing commands to deal with a discrete conflict, they create obligations of a sort usually found only in treaties'.[119] Both these resolutions indicate the willingness of the Security Council, most certainly in response to threats of international terrorism, to widen the scope of Article 39 insofar as it exceeds its constitutional competencies enshrined within the UN Charter.[120] At the same time, both these resolutions have an exceedingly broad and general nature of application, which makes interpreting their application to OCTAs an ambiguous and indefinite task. This said, the Security Council's consistent recognition of OCTAs forming part and parcel of terrorism and its acknowledgment of the implications of such activities is expressive and significant in driving the counterterrorism initiative. Nevertheless, it remains imperative that in the current counterterrorism agenda and to achieve the

---

[115] Ibid at para 4. The Security Council hereby 'decides to establish… for a period of no longer than two years, a Committee of the Security Council, consisting of all members of the Council, which will, calling as appropriate on other expertise, report to the Security Council for its examination, on the implementation of this resolution, and to this end calls upon States to present a first report no later than six months from the adoption of this resolution to the Committee on steps they have taken or intend to take to implement this resolution'.

[116] Elberling, supra note 5, at 339. The introduction of legislative resolutions has received widespread controversy with the growing discretion of the Security Council's capacity to act questioning the legitimacy of its actions and it has been said that 'while Resolution 1373, already referring to terrorist acts in the abstract, had still also been a reaction to a particular attack, Resolution 1540 dealt with the problem of proliferation only in the abstract'.

[117]Gabriel H. Oosthuizen and Elizabeth Wilmshurst, 'Terrorism and Weapons of Mass Destruction: United Nations Security Council Resolution 1540', *Chatham House International Law Programme Briefing Paper* (Sept. 2004) at p. 3, available at https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/ILP0904bp.pdf

[118] Ibis, at para 2.

[119] Johnstone, supra note 9, at 283

[120] See e.g. Justin Morris and Nicholas J. Wheeler, 'The Security Council's Crisis of Legitimacy and the Use of Force', *International Politics,* Vol. 44, Iss. 2-3, pp. 214 – 231 (March 2007); see also Elberling, 'The Ultra Vires Character of Legislative Action by the Security Council', *International Organisations Law Review* 2: 337-360, (2005).

fight against global terrorism, there must be an explicit and specific prohibition of OCTAs in order for their adequate prevention and suppression under international law.

III. The UN's Collective Security System and the General Assembly

3.1 Competences and Powers of the General Assembly

The General Assembly is responsible for addressing broader issues of international concern that do not pertain to a single specific matter. Rather, the role of the General Assembly is to contribute towards the development of international law by prescribing measures that enhance legislation in a broad and general sense, mostly producing resolutions in a declarative manner. Described as 'foremost a political body expressing political opinions,' the General Assembly is the main global forum where matters of international concern are discussed.[121] Its composition incorporates all members of the UN, allowing all such members to vote on matters bought before the Assembly.[122] The view is that the General Assembly has a clear delineation of powers that operate in a recommendatory nature. As Higgins rightly states:

> Generally speaking, it is widely agreed that the General Assembly possesses recommendatory rather than mandatory powers, except in such matters as the admission of new Members, the approval of the budget and the apportionment of expenses.[123]

The competencies of the General Assembly are defined in Articles 10-14 of the UN Charter. Article 10 empowers the Assembly with a general competence over issues within the scope of the Charter and Article 14 re-emphasizes this power by delineating its wide discretion with specific reference to international security.[124] In the language of the Charter, the General Assembly may make recommendations to the Security Council and Member States on 'any questions or any matter' that fall within the scope of the Charter.[125] In the event of any conflict between the two organs, Article 12(1) provides that 'the General Assembly shall not make any recommendations with regard to that dispute or situation' should the Council be exercising any powers in respect of that very situation or dispute.[126] It is clear then that matters of international peace and security are a shared responsibility with the General Assembly performing a subordinate role in support of the Security Council. Such a distinction clearly reinstates the nature of roles expected of the collective security system and the

[121] Ben Saul, *Defining Terrorism in International Law*, (OUP, 2003), at 192.
[122] Article 9 of the Charter of the UN, 1945.
[123] Higgins, supra note 37, at p. 272 – 273.
[124] Article 14 of the Charter of the UN, 1945. This provision states that: 'Subject to the provisions of Article 12, the General Assembly may recommend measure for the peaceful adjustment of any situation, regardless of origin, which it deems likely to impair the general welfare or friendly relation among nations, including situations resulting from a violation of the provisions of the present Charter setting forth the Purposes and Principles of the United Nations'.
[125] Article 10 of the UN Charter, 1945.
[126] Article 12 of the UN Charter, 1945.

affirmation of the Council enjoying a primary role in determining matters of international peace and security.

Whilst this holds true, the Charter does not – explicitly or otherwise – confer a legislative function on any of its constituent organs, despite the Security Council having shown otherwise. It is argued that 'while there is no true legislative organ within this system, the organ that comes closest to such a function is the General Assembly'.[127] Under Article 13(1)(a) UN Charter, the General Assembly is responsible for 'encouraging the progressive development of international law and its codification'.[128] This suggests that the Assembly, when dealing with matters of international peace and security, should endeavour to contribute towards the formation of rules where possible. Therefore, any legislative role that could be inferred from the language of the Charter would reside with the Assembly over that of the Council. For this reason, it can be said that the institutional roles between the two organs have a clear distinction. It is argued that 'the Assembly can appropriately deal with long-term 'root cause' aspects of peace and security, while the Security Council undertakes operative actions.'[129] Saul attributes this to the structural contrast between the General Assembly and the Security Council, with the former appearing as the 'soft UN' and the latter acting as the 'hard UN'.[130]

Despite its institutional differences, the General Assembly nonetheless makes general determinations of law for a wide range of issues typically in a declaratory manner. That is to say, declarative resolutions do not refer to specific facts or legal situations. Rather, they are general declarations of international law. This is because the General Assembly is better equipped to address the sources of causation affecting peace and security because of the procedures by which decisions can be taken. For example, there is no veto power in the General Assembly like there is in the Security Council. Given this, the Assembly determines policies that may then lead the Council to adopt binding decisions, and therefore enable general determinations of law to become obligations of international law.[131] The case of Namibia affirms this, where the Council took action because the General Assembly acted under Article 11(2) to draw attention to the case before the Council. The ICJ in Namibia stated that:

[127] Elberling, supra note 5, at 343.
[128] Article 13 (1)(a) of the UN Charter, 1945.
[129] Alexander Orakhelashvili, Collective Security, (OUP, 2011), at p. 46.
[130] Saul, supra note 120, at p. 213.
[131] Orakhelashvili, supra note 128, at p. 47. The author holds that 'the Council could adopt binding decisions or resort to enforcement measures on the basis of a policy determined by the General Assembly'.

> it would not be correct to assume that, because the General Assembly is in principle vested with recommendatory powers, it is debarred from adopting, in specific cases within the framework of its competence, resolutions which make determinations or have operative design.[132]

Whilst the General Assembly may not produce legally binding resolutions that oblige Member States to act upon them, it nonetheless embraces views of the international community that reflect the moral underpinnings of different states in a collective manner. Despite this, it is apparent that powers of the General Assembly at least in matters of international peace and security are residual. It remains a secondary enforcer of international rules only and when the Security Council is unable to do so.

3.2 Nature of General Assembly Resolutions

The General Assembly has the power to adopt resolutions as per Articles 10-14 of the UN Charter, and its decisions can be declaratory or recommendatory.[133] As such, the General Assembly tends to issue non-binding recommendations when it comes to matters of international peace and security. According to Saul, declarative resolutions have direct legal effect as authoritative interpretations of the UN Charter.[134] They represent the common attitude of the international community, and arguably create customary international norms owing to their institutional make up. On the one hand, declarative resolutions reinforce existing customary law. On the other hand, declarations may give rise to state practice and opinio juris and create new customary norms that might be considered evidence of emerging custom.[135]

Since the nature of General Assembly practice embraces a largely political agenda by acting as a global forum for all Member States, the most common type of resolution made by the General Assembly is recommendatory. The UN Charter is explicit in the conferral of powers stipulating that the General Assembly 'may make recommendations' on matters within the scope of the Charter.[136] Resolutions may begin with the word 'recommend' by way of presenting international legal matters bought before it and carry a soft approach of advising Member States. This, however, does not mean General Assembly resolutions use of the word 'recommend' is purely recommendatory. Despite the choice of word, General Assembly resolutions are not of limited binding authority as the term might

[132] Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, ICJ Reports 1971, *p. 16* at 50.
[133] Saul, supra note 120, at p. 192.
[134] Ibid, at p. 193.
[135] North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3; Military and Paramilitary Activities in and against Nicaragua (hereinafter referred to as 'Nicaragua v. United States of America'), Merits, Judgments, I.C.J. 14, Reports 1986.
[136] Article 10 of the UN Charter, 1945.

suggest.[137] There are some resolutions that 'recommend' measures in a binding manner by enforcing obligations upon Member States to act upon these measures.

3.3 The General Assembly's Interpretation of Peace and Security in Relation to Terrorism

For the early part of the UN, matters of terrorism were dealt with by the General Assembly. During the 1970s, the adoption of various counterterrorism treaties to address the increasing acts of violence directed against particular targets frequented the security agenda. This led to the condemnation of the use of civil aviation,[138] hostage taking,[139] nuclear materials,[140] maritime navigation,[141] plastic explosives,[142] and protected persons[143] by terrorists. What became apparent was the struggle to conclude a definition of international terrorism with the agreement of all states, leaving the General Assembly the task of criminalising different ways of executing terrorism instead of addressing terrorism itself.

Nonetheless, the General Assembly continued to progress with counterterrorism efforts and in 1994, a Declaration on Measures to Eliminate International Terrorism was adopted under Resolution 49/60.[144] In response to terrorism, the Declaration makes an important determination and states that:

> Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.[145]

The General Assembly identifies the principal features of acts of terrorism, which gives this provision a broad scope of application. It does not provide a definition of terrorism and it makes no concrete attempt to define an act of terrorism. However, what it does do is suggest that acts of violence like those mentioned within the paragraph 'may pose a threat to international peace and security',

---

[137] F. Blaine Sloan, 'The Binding Force of a Recommendation of the General Assembly of the United Nations', *25 Brit. Y.B. Int'l L.1* (1948), at p. 13-14.
[138] Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo Convention), Sept. 14, 1963; Convention for the Suppression of Unlawful Seizure of Aircraft (Hague Convention), Dec. 16, 1970; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage Convention or Montreal Convention), Sept. 23, 1971.
[139] International Convention against the Taking of Hostages (Hostages Convention), Dec. 18, 1979.
[140] Convention on the Physical Protection of Nuclear Material (Nuclear Materials Convention), Oct. 26, 1979.
[141] Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention), March 10, 1988.
[142] Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention), March 1, 1991.
[143] Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons (Diplomatic Agents Convention), Sept. 28, 1973.
[144] Measures to Eliminate International Terrorism A/RES/49/60 of Dec. 9, 1994.
[145] Ibid, at para 3.

expressly affirming its stance against terrorism.[146] In doing so, the General Assembly identifies the obligations deriving from the Charter and international law.

In 1996, this Declaration was further reaffirmed when the adoption of Resolution 51/210 came with developments to include the financing, planning and incitement of terrorist acts.[147] The incorporation of these activities indicates the growing concern of the General Assembly to suppress the means used to facilitate international terrorism in an attempt to prevent hindrances to achieving peace. This resolution then led to the establishment of an Ad Hoc Committee on Terrorism, of which created an international convention for the suppression of terrorist bombings and the suppression of nuclear terrorism.[148] The resolution also attached with it an annex as a means of developing a comprehensive legal framework to deal with international terrorism.[149]

International efforts to strengthen the global counterterrorism regime came into force in 2006 when the General Assembly adopted Resolution 60/288 to establish the Global Counter-Terrorism Strategy.[150] Consisting of a wide range of measures to strengthen international cooperation, the framework reflects a common strategic approach by agreement of all Member States to pursue the countering of terrorism in unity. A key provision of the strategy aims:

> to refrain from organising, instigating, facilitating, participating in, financing, encouraging or tolerating terrorist activities and to take appropriate practical measures to ensure that our respective territories are not used for terrorist instillations or training camps, or for the preparation or organisation of terrorist acts intended to be committed against other states or their citizens.[151]

The provision makes a number of remarks. Firstly, the General Assembly identifies various ways in which terrorist groups can commit attacks by listing different methods to conduct terrorist operations and accounts for the distinction of these acts to form part of the terrorist process. In the same way, the provision acknowledges the correlation of such activities as imperative to engage in terrorism. That is to say, the financing of terrorism might allow for the purchase of computers, which could then be used for the organisation of attacks, the recruitment of individuals, and the dissemination of propaganda or otherwise. Thus, it is clear that terrorism is not limited to any one particular act but instead can take a range of unprecedented forms that together can dovetail to intensify global

[146] Ibid, at para 2.
[147] Measures to Eliminate International Terrorism A/RES/51/210 of Dec. 17, 1996. The resolution at para 3 (f) calls upon states: 'to take steps to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organisations…'
[148] Ibid, at para 9.
[149] United Nations General Assembly, "Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism", annexed to UNGA, "Measures to Eliminate International Terrorism", 17 December 1996, UN doc. A/RES/51/210. Available at https://www.legal-tools.org/doc/c8397d/
[150] A/RES/60/288 The United Nations Global Counter-Terrorism Strategy of 8 September 2006.
[151] Ibid, subject to para 1, Pillar II.

terrorism. By recognising terrorism's interconnected nature, the General Assembly makes a concerted effort to strive towards peace by diminishing the potential for terrorists to act in ways that can otherwise legitimise structural violence and perpetuate violent terrorism.

Secondly, the General Assembly emphasizes that terrorism is an international matter that transcends territorial boundaries. This stipulation reiterates the sheer importance of states to coincide national efforts in a unified manner to eliminate any prospect of terrorism emanating from their own national territories that may violate the security of another and potentially hinder the achievement of negative peace. Respect for sovereign equality therefore requires states to harmonise cooperation as a means to prevent international terrorism and to eliminate the possibility of conflict. This is an implicit affirmation of the principle of sovereignty through which the right of the state to govern its own territory is exclusive.[152] Acts of global terrorism, however, impede state sovereignty by way of challenging states abilities to protect its own territory through acts of violence and measures recommended by the General Assembly to encourage collective action reflect this.

Last, but by no means least important, the General Assembly does not confine measures of counterterrorism to those listed in the provision. Instead, it suggests that 'appropriate practical measures' are to be taken by states in light of the different challenges each state may face when it comes to terrorism. Thus, it allows states to adopt and implement national security measures that suits the threats of terrorism faced before them. Not only is the suppression of these activities imperative to tackle terrorism, but the Resolution reinstates the aim of the strategy, which is to unite the efforts of all states through collective action in order to maintain international peace and security.

Developments of the General Assembly's counterterrorism initiative are adopted by consensus of all Member States, by which universal agreement then allows measures to address the long-term implications of terrorism. The mechanisms that are in place have a considerably longitudinal effect with the inclusion of consistent biennial reviews to evaluate the progress of the Global Counter-Terrorism Strategy.[153] By nature of its composition, the General Assembly establishes a holistic and inclusive approach bound by unanimity and congruency of its Member States which is sufficiently broad to achieve a global consensus in tackling terrorism.

[152] The principle of sovereignty is a fundamental principle of international law. See e.g. Hans Kelsen, 'The Principle of Sovereign Equality of States as a Basis for International Organisation', *The Yale Law Journal*, (Vol. 53, No.2, March 1944) pp. 207-220.
[153] A/RES/60/288, supra note 149.

3.4 General Assembly Resolutions and OCTAs

One of the first instances where the General Assembly addresses terrorists use of the internet in a resolution is found in Resolution 60/288 where states are suggested to:

> coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet.[154]

Continuing its commitment to further counter terrorism, the General Assembly begins to adopt resolutions that pertain more specifically to the type of terrorist activities taking place online, identifying the precise use of the internet by terrorist groups:

> [Expressing] its concern at the increasing use, in a globalized society, by terrorists and their supporters, of information and communications technologies, in particular the Internet and other media, and the use of such technologies to commit, incite, recruit, or plan terrorist acts…[155]

Throughout discussions vis-à-vis terrorism, the General Assembly's concern over terrorist use of the internet for recruitment, financing, and planning of terrorist acts continue to be reiterated and dangers over the commission of OCTAs are highlighted time and time again. The need for the international community to counter terrorist activities through the use of the internet is a core theme of measures suggested by the General Assembly and encouraged throughout its resolutions within discussions of the Global Counter-Terrorism Strategy review.[156] Since Resolution 68/276 (2014), subsequent resolutions of the General Assembly insist the need for states to address these OCTAs in response to the increasing terrorist activity taking place online and maintain the importance of doing so to prevent the growth of terrorism.

Whilst the Internet is perceived as a platform vulnerable to malicious use, at the same time it is praised as a useful tool to engage with counterterrorism initiatives.[157] In suggesting measures to prevent terrorism through the Internet, the General Assembly considers ways to promote awareness of online terrorism to protect civil society from being vulnerable to radicalisation. Thus, through the suggestion of practical measures, the General Assembly attempts to circumvent the continuation of online terrorism by focusing on prevention techniques that intend to produce long-term results, much in line with its responsibilities within the UN that have been discussed before. This coincides with the

---

[154] Ibid, at para 12 (a).

[155] A/RES/68/276 The United Nations Global Counter-Terrorism Strategy of 24 June 2014.

[156] A/RES/70/291 of 19 July 2016 at paras 42 and 54; A/RES/72/194 of 23 January 2018 at para 12; A/RES/72/284 of 2 July 2018 at paras 21 and 22.

[157] A/60/285 at para 85. The General Assembly recognises the utility of the internet as a:
'powerful and unparalleled tool for countering the spread of the ideologies of terrorism, focusing on the plight of victims, linking communities and educational establishments in different countries, and gathering and sharing information on terrorist suspects'. See also Walker and Conway, 'Online Terrorism and Online Laws', *Dynamics of Asymmetric Conflict*, 8:2, 156-175, (2015) which discusses the functionality of the internet, considering both the benefits and the setbacks in relation to counter-terrorism.

General Assembly's efforts having normative value of striving towards peace in its positive concept. Measures to prevent terrorism online is the General Assembly's attempt to address an aspect of culture that can be used to legitimise structural violence. By identifying pragmatic techniques to counter terrorism, the non-binding nature of General Assembly resolutions and reports offers a realistic initiative to tackle the issues of cyberterrorism and to inform states of the contemporary threats posed by international terrorism.

The General Assembly's commitment to countering terrorism places great emphasis on the need for international cooperation. The Global-Counter Terrorism Strategy Review in 2018 sees the General Assembly calling on a 'unified solution to tackle threats' particularly in relation to threats posed by ISIS.[158] The Assembly further recognises:

> the significance of a sustained and comprehensive approach to address conditions conducive to the spread of terrorism, adding that it could not be defeated by military force, law enforcement and intelligence operations alone.[159]

The General Assembly makes a significant point that tackling those conditions, which allow for the continued proliferation of terrorism, fall to the efforts of all Member States collectively to protect societies against terrorist violence. Although the waning presence of ISIS on the ground is a huge loss to the terror group's physical presence, 'even when terrorist groups are territorially defeated, their ideological roots can remain pervasive'.[160] Thus, physical occupation is no longer the primary concern to countering terrorism.[161] Instead, the subsequent challenge should focus on tackling the exploitation of modern technologies that pervade the counter-terrorism agenda.

Not least does the General Assembly stress the need for Member States to grow an awareness for emergent terrorism and the threat of violent attacks, but there is consistent reiteration for states to understand that this prospect is intrinsically correlated with the propagation of violent extremism, the radicalisation and recruitment of individuals and the financing of terrorist operations, all of which are OCTAs.[162] Above all, a number of Member States distinguish the use of modern technologies exploited by terrorist groups as a serious concern, acknowledging that these activities facilitate terrorism and

---

[158] General Assembly President Miroslav Lajcak (Slovakia), UNGA GA/12035, 'General Assembly Unanimously Adopts Resolution Calling for Strong Coordinated Action by Member States to Tackle Terrorism, Violent Extremism Worldwide', (June 26, 2018).
[159] Ibid.
[160] Singaporean Delegate, ibid.
[161] BBC News, 'IS 'Caliphate' Defeated but Jihadist Group Remains a Threat', (March 23, 2019), available at https://www.bbc.co.uk/news/world-middle-east-45547595 (accessed 2 June 2018).
[162] Various Member States such as UAE Iraq, Korea, India and Sri Lanka identify the use of new technologies as contributing to the continuing threat of international terrorism. UNGA GA/12035, 'General Assembly Unanimously Adopts Resolution Calling for Strong Coordinated Action by Member States to Tackle Terrorism, Violent Extremism Worldwide', (June 26, 2018).

subsequent initiatives must pay attention to such developments. Perhaps the biggest takeaway of the General Assembly's Review is the recurring theme that stresses:

> [t]he international community should consider developing an accurate understanding of how terrorists motivated others to commit terrorist acts or how they recruited them.[163]

This view is further affirmed by the General Assembly's Secretary-General Report of April 2018, which explains that threats of terrorism are entering a new phase with:[164]

> ISIL is likely to try to retain global influence after its territorial collapse by using the Internet and social media platforms to inspire, mobilize and direct its supporters to carry out attacks in their home countries.[165]

It is clear that through the use of technology, the General Assembly confirms that ISIS continues to be a threat with its terrorist tactics developing in far more nuanced ways than envisioned before. The report suggests that ISIS' terrorist tactics will be expected to move online, emphasizing a link between OCTAs and the commission of physically violent terrorist attacks as a result of exploiting the internet. In other words, the General Assembly actually deduces a direct causation between the commission of cyber terrorist activities developing into terrorist attacks of which is catalysed by the use of the internet.

This perception is important for two main reasons. Firstly, the acceptance that OCTAs can develop into physical attacks reaffirms the danger of these activities that are being carried out by violent terrorist groups. Not only do OCTAs threaten the security of states, but they also shake the very foundations of international law. This can be seen as a threat to positive peace developing into a threat to negative peace, hampering the achievement of peace in its totality. This is because of the lack of accountability for harmful acts committed by non-state actors and because of the lack of adequate legal address surrounding OCTAs, which makes them particularly hard to regulate.[166] Secondly, identifying OCTAs as the precursors to terrorist attacks indicates that international law must find a way to prohibit these activities as a primary method to engage with the counterterrorism initiative of today. Absent of this, violent terrorist attacks will continue to dominate the global security agenda until their cessation can be achieved to some degree. Subsequent General Assembly reports reflect the current context of circumstances that are bought before it. The General Assembly thereby has the

[163] Ibid.
[164] A/72/840 Activities of the United Nations System in Implementing the United Nations Global Counter-Terrorism Strategy: Report of the Secretary-General of 20 April 2018.
[165] Ibid, at para 9.
[166] See Nicholas Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', *Journal of Conflict and Security Law*, Vol 21 Iss. 3, 1 Dec 2016 p. 455-474.

responsibility of informing states of the existing counterterrorism initiatives in order to encourage and promote state action in the fight against terrorism.

The most recent General Assembly Resolution 72/284 (2018) stresses the need to suppress terrorist exploitation of the internet in all its manners and forms, with a particular focus on OCTAs as the main culprit to its misuse:[167]

> [T]errorists may craft distorted narratives that are based on the misinterpretation and misrepresentation of religion to justify violence, which are utilized to recruit supporters and foreign terrorist fighters, mobilize resources and garner support from sympathizers, in particular by exploiting information and communications technologies, including through the Internet and social media, and also notes in this regard the urgent need for the international community to globally counter such activities.[168]

Despite the General Assembly's continued efforts to encourage international cooperation to counter terrorism, the decision remains with states who are free to decide whether or not they wish to take these measures with no obligation to do so. For all matters, the General Assembly does not have the capacity to bind states to any of its recommendatory measures and though it narrates on various issues concerning peace and security it does so in a discursive manner. That is not to say the General Assembly's recommendations over matters of terrorism are without significance, but its ability to instigate actionable responses from the international community has limited scope when it comes to OCTAs and such limitations are attributable to the nature of its composition. Indeed, there is little ambiguity over the fact the General Assembly is reliant on Member States to take initiative and implement pragmatic responses to action its recommendations and adopt counter-terrorist measures to tackle global terrorism.

From the above analysis, it can be said that resolutions of the General Assembly make concerted efforts to address the challenges posed by OCTAs. General Assembly resolutions recognise the vast ways in which terrorists can exploit cyberspace through recruitment, financing and propaganda among other terrorist activities and emphasises practical measures which can be taken in response to such threats. Yet, states remain 'legally free to accept and implement or oppose and disregard' suggestions made by the General Assembly meaning there is little authoritative effect of its resolutions to compel states to act.[169] Whilst the Assembly may have at one point, adjudicated at a time when the Council could not, the role of each institution is far more distinguished today. Since the General Assembly does not have the competency to legislate or impose obligations of any kind, the resolutions it adopts can be seen more as an acknowledgement between states upon the matter in

[167] A/RES/72/284 The United Nations Global Counter-Terrorism Strategy Review of 2 July 2018.
[168] Ibid, at para 22.
[169] Stephen M. Schwebel, 'The Effect of Resolutions of the UN General Assembly on Customary International Law', *Proceedings of the Annual Meeting, ASIL,* Vol. 73 April 26-28, 1979 (pp. 301-309), at 302.

question. Thus, General Assembly Resolutions, though pragmatic and valuable, do not have the scope or capacity to regulate OCTAs in the same manner that legislation or even customary international law is able to do so. The question is, can General Assembly resolutions constitute customary law? The next section examines this issue.

VI. Analysis of Customary International Law

The preceding analysis of UN resolutions may suggest the emergence of a customary norm concerning the prevention of OCTAs. Certain resolutions can pass into customary international law where they evidence general state practice accepted as law of certain rules. Whether a UN resolution establishes the formation of customary law is contingent upon, first, the uniformity and consistency of state practice, and second, states accepting the rule in question as law. For an emergence of customary law concerning the prevention of OCTAs, UN resolutions must regularly address and condemn cyber terrorist recruitment, financing and propaganda. Importantly, states must also engage in measures to prevent these OCTAs in order to maintain international peace and security. Together, these two requisites would indicate the emergence of a customary rule applicable to the prevention of OCTAs.

As seen from the above analysis of UN resolutions pertaining to terrorism, both Security Council and General Assembly resolutions consistently broach the subject of OCTAs by recognising their impact and influence in wider terrorist goals and agendas. Resolutions frequently present terrorist financing, recruitment and dissemination of propaganda as operations that further violent terrorism and thus, are a matter of international concern.[170] Identifying OCTAs as supporting acts to international terrorism could constitute the existence of an emerging rule in such resolutions adopted by the Security Council and the General Assembly that are all valuable in seeking to determine actual state practice as it regards the prevention of OCTAs. The behaviour of states can be observed through what they say and what they do, and resolutions in the General Assembly are particularly significant in denoting state practice as well as *opinio juris*.[171] There is symbolic impact of GA resolutions because they can crystallise the opinion of the international community (unlike SC resolutions which require unanimity among its permanent members) which can influence the behaviour of states.

General Assembly Resolutions including 68/276 (2014),[172] Resolution 70/291 (2016),[173] Resolution 72/194 (2018)[174] and Resolution 72/284 (2018) condemn terrorism in all its forms.[175] On one hand,

[170] See e.g., S/RES/1624, S/RES/2129, S/RES/2133, S/RES/2499, S/RES/2253, S/RES/2322, S/RES/2178, S/RES/2170, S/RES/2462, S/RES/2482, A/RES/51/210, A/RES/60/288, A/RES/68/276, A/RES/70/291, A/RES/72/194, A/RES/72/284.
[171] Shaw, *International Law*, 6th Ed., (Cambridge University Press, 6th Ed., 2008), pg. 81-88.
[172] A/RES/68/276 of 13 June 2014.
[173] A/RES/70/291 of 1 July 2016.
[174] A/RES/72/194 of 19 December 2017.
[175] A/RES/72/284 of 26 June 2018.

repetition of these determinations might be considered evidence of state practice and *opinio juris* because it represents the behaviour of states accepting that all acts of terrorism must be prevented. There is political significance in stigmatizing terrorism and repeated declarations can serve as evidence of an emerging legal norm. On the other hand, a series of counterterrorism resolutions adopted by the GA does not automatically mandate certain behaviour of states and constitute a legal conviction. It can be argued that they fall short of sufficiently normative language used in those resolutions to constitute the requisite *opinio juris* for a specific customary rule prohibiting terrorism in the form of OCTAs. Repetition indicates the *opinio juris* as it currently stands by affirming the international condemnation of terrorism and signifies the possibility of *opinio juris* evolving. However, repetition does not inform of whether *opinio juris* exists due to the lack of normativity to legally commit states to ensuring that terrorism is truly condemned in all its forms and manifestations.

To establish *opinio juri*s in a General Assembly resolution, the Nuclear Weapons opinion clarified that 'it is necessary to see whether an *opinio juris* exists as to [the resolution's] normative character'.[176] In other words, this analysis relies on whether states believed that the normative content of the resolution was of a legal nature or whether any normative content of the resolution can be understood in legally binding terms.[177] If the resolution lacks sufficient normativity to materialise the content, whether the resolution remains a reality of the *opinio juris* relies on if states find the resolution to be a formulation of law. The difficulties in establishing the reality are further complicated by the General Assembly's inherently political institutional structure. The rationale for voting certain resolutions can be may be influenced by moral, political, social or economic reasons. States may vote for a resolution but may not legally commit to its content knowing that General Assembly resolutions are recommendatory and thus, do not impose obligations to coerce action. Thus, the reality of the *opinio juris* cannot easily be assumed given the nature of the General Assembly as a political organ and one that is not tasked with creating or establishing legal rules or norms.

The heterogeneous mix of GA materials and the lack of sufficient normativity of language used in those resolutions could be said to deprive them of the requisite state practice and *opinio juris.* Accepting this, it cannot be said that they would amount to general acceptance sufficient to evident customary law-making as it relates to the prevention of OCTAs in international law.

[176] Supra note 173 at 255, para 70.
[177] Öberg, 'The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ', *EJIL* Vol. 16 No. 5, 2006, at p. 901-902.

V. Conclusion

This chapter has explored the role of the UN's collective security system in suppressing OCTAs, with a particular focus upon the contributions of the Security Council and the General Assembly. This chapter has shown that the powers and practice of the Security Council have evolved in unprecedented ways when it comes to tackling international terrorism. In light of increasing acts of international terrorism and the rise of terrorist group ISIS, the Security Council has been at the forefront of countering modern terrorism. In its adoption of various executive resolutions that are both binding and non-binding, the Security Council has shown clear acknowledgement that OCTAs contribute towards the functioning of terrorist groups and threaten both negative and positive peace. To add to this, the Security Council has notably adopted certain legislative resolutions that tackle international terrorism, which has demonstrated its capacity to act as both enforcer and creator of new rules.

Although the Security Council has unlimited powers and it has sought to deal with terrorism and OCTAs, this chapter has found that efforts of the Security Council have not gone far enough. As such, there remains a pressing need for the Security Council to adopt binding counterterrorism resolutions that pertain specifically to OCTAs and to determine this as a threat to international peace and security. And whilst the General Assembly has made invaluable contributions towards the countering terrorism, its resolutions are recommendatory. Therefore, this chapter has found that the adoption of counterterrorism measures without imposing compelling norms that demand collective action of states, has limited value. States are therefore indispensable to steer the fight against cyberterrorism and their will to prohibit OCTAs is fundamental to achieving international peace and security, particularly in light of ISIS's waning physical occupation in both Syria and Iraq. Accepting this, the next two chapters explore the obligation to prevent transboundary harm to determine whether this principle of international law can be used to prevent and suppress OCTAs and to maintain international peace and security.

Chapter Five

THE OBLIGATION TO PREVENT TRANSBOUNDARY HARM IN CYBERSPACE

I. Introduction

Customary international law imposes an obligation upon states to ensure that their territory is not used as a platform to cause harm to the rights of other states.[1] Importantly, state practice demonstrates that the obligation to prevent transboundary harm exists in cyberspace and can be applied to activities therein.

This chapter explores whether this customary obligation can be used to prevent terrorists' exploitation of cyberspace to conduct OCTAs in the form of cyber terrorist recruitment, financing and propaganda. In pursuit of this objective, this chapter adheres to the following structure. Section II demonstrates the customary international status of the obligation to prevent transboundary harm and discusses the applicability of the obligation to prevent transboundary harm in cyberspace. Section III sets out the content and scope of the obligation to prevent transboundary harm by exploring the quantity of harm and quality of harm needed to trigger the application of this rule. Section IV examines the nature of this obligation and reveals that its application is conditioned by the standard of due diligence. Section V examines the specific duties of prevention attached to the obligation to prevent transboundary harm. Section VI offers conclusions.

II. The Obligation to Prevent Transboundary Harm in International Law

2.1 The Legal Status of the Obligation to Prevent Transboundary Harm

The obligation to prevent transboundary harm is a well-established rule of customary international law. It derives from the principle of sovereignty, a foundational norm of international relations which confers upon states the right to determine their internal affairs free from external intervention.[2] The customary status of this rule has been confirmed by multiple decisions of national and international tribunals.

One of the most prominent and early international disputes concerning the prevention of transboundary harm is found in the Alabama Arbitration of 1872.[3] Great Britain, by failing to prevent

[1] Corfu Channel (UK v. Albania), 1949, Judgment of April 9th, 1949 I.C.J. Reports 1949.
[2] Article 2(1) of The Charter of the United Nations, 1945.
[3] *Alabama Arbitration Case (United States of America v United Kingdom)* (14 September 1872), Papers relating to Foreign Relations of the United States 1872 (United States Government Printing Office Washington 1873) part 2 Vol IV. Different standards of due diligence obligations emanated from the Alabama case, discussing the broad and narrow readings of the concept relating to the security of foreign states. The US argued for a strict interpretation of due diligence which would

a warship from being equipped and armed on its territory to be used against the US was found liable for breaching its obligations to the US under international law.[4] The Arbitration established that 'states are not to use or allow their territories to be used in ways that are capable of causing injuries to properties or persons in other states'.[5] In awarding its judgment, the Arbitration confirmed that states are under a legal duty to ensure that their territory is not used in a manner injurious to the legal rights of other states.

Over time, the obligation to prevent transboundary harm broadened when it was extended to cover the protection of aliens in state territory. In the 1920s, a series of claims made before the US/Mexico General Claims Commission concerned the failure of the Mexican authorities to apprehend and punish those responsible for the murder of American nationals in Mexico. In all such claims, the US repeatedly asserted the liability of Mexico for failing in its duties, actively engaging in practice to demonstrate that the state is in fact under a legal obligation to apprehend and punish persons where there was inadequate protection of foreign nationals which lead to mortalities. The Commission found that Mexico had breached its obligations and failed to take adequate measures to punish those implicated in crimes against foreign nationals.[6]

The rule was further expanded by the tribunal in the Trail Smelter Arbitral case (1941), in a matter relating to the protection of the environment.[7] A dispute arose before the Tribunal concerning the pollution of territories across the US border between Canada and the US.[8] As a result, the Tribunal

give rise to a breach of an international standard. The UK however, favoured a broader understanding of the principle articulating that the lack of due diligence should be attributed to the domestic state's failure to provide care as ordinarily expected of it.

[4] Ibid, at 714 – 716. The Tribunal held that '[u]nder the principles of international law, as well as of the law of the United States, no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence'. The Alabama Tribunal ruled that Britain owed the US a duty of 'active due diligence' to prevent private parties from supplying the southern rebels, she had failed to observe her international obligations as a neutral state.

[5] Ibid.

[6] *Janes (U.S. v Mex.)*, 4 R.I.A.A. 82 (1926), at p. 87. The application of due diligence extends to instances of post-hoc denial of justice, where 'the culprit is liable for having killed or murdered an American national; the Government is liable for not having measured up to its duty of diligently prosecuting and properly punishing the offender'; *Youmans (U.S. v. Mex.),* 4 R.I.A.A. 110 (1926). The Youmans claim involved a Mexican mob against three American nationals, Mexican authorities shot at a foreign national and killed him. A mob of a thousand people converged amongst a property where the 3 foreign nationals were trapped. Mexico demonstrated a breach of the state's due diligence obligation for its inability to hold anyone accountable for the killings. At p. 114, the General Claims Commission was to deal with 'the failure of the Mexican Government to exercise due diligence to protect […Youmans] from the fury of the mob at whose hands he was killed, and the failure to take proper steps looking to the apprehension and punishment of the persons implicated in the crime'; *Massey (U.S. v. Mex.), 4 R.I.A.A. 155 (1927*). The Massey Claim concerns a U.S. national who was killed by a Mexican national. The criminal was captured and confined in prison but managed to escape with the help of a prison guard. The General Claims Commission held that Mexico was liable for allowing the criminal to escape and for failing to take adequate measures to punish him. The state must bear responsibility for its own nationals and take proper measures to apprehend and punish when they commit wrongs against foreign nationals, otherwise known as 'aliens'.

[7] *Trail Smelter (US v. Canada),* 3 R. International Arbitration Awards 138 (1941).

[8] Ibid.

notably ruled that 'states owes at all times a duty to protect other states injurious acts by individuals within its jurisdiction'.[9] This decision was fundamental to the recognition of injurious consequences arising out of activities that are otherwise lawful within the territory of a state but whose harmful effects occur in a neighbouring state and thus must be prohibited by international law.[10] What this indicates is that states are expected to bear responsibility for the external consequences of internal regulations in respect to the rights of other states. The Tribunal emphasized the significance of this rule by stipulating that when it comes to the interests of other states, the state is responsible for the conduct of private actors, specifically where that conduct breaches international law and where the state has exclusive control over that territory to engage in preventive measures. The case of Trail Smelter recognises that transboundary harm challenges the demarcated boundaries of state authority and the traditional concept of state sovereignty by ruling that environmental pollution is capable of defying borders where states have limited authority.[11] In spite of this, states must accept the consequences of injurious acts originating from its own territories by complying with the responsibility to prevent transboundary harm as a means of protecting not only its own sovereignty but to respect the sovereignty of other states when it comes to transboundary activities of private actors. The Tribunal, in clarifying the existing obligation to prevent transboundary harm whilst simultaneously broadening its scope to encompass harmful transboundary non-state activities to fall within its scope, slowly codifies the existence of this rule as customary international law.

The ICJ articulated this general rule for the first time in Corfu Channel (1949), by recognising that it is 'every state's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states'.[12] The UK, in bringing its proceedings against Albania for the explosion of mines in the Corfu Channel, submitted that Albania had committed a breach of its obligation to prevent its territory from being used to cause harm to the legal interests of other states.[13] The ICJ held that, at a minimum, states have a duty to notify other states of known or foreseeable harms and this rule applies where those harms arise from within the warning state's territory.

[9] Ibid, Trail Smelter, at 714-716. The Tribunal further concluded that '[u]nder the principles of international law, as well as of the law of the United States, no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence'.

[10] Sompong Sucharitkul, 'State Responsibility and International Liability Under International Law', *18 Loyola of Los Angeles Int'l & Comp. L. J.* 821 (1996), at p. 836.

[11] See Rebecca M. Bratpsies and Russell A. Miller, 'Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration', Rebecca M. Bratpsies & Russell A. Miller, eds., (Cambridge University Press, 2006); *Washington & Lee Legal Studies Paper* No. 2011-30 (23 January 2012).

[12] Corfu Channel, supra note 1.

[13] Ibid, at p. 9 – 11.

2.2 The Obligation to Prevent Transboundary Harm in Cyberspace

Cyberspace is a borderless realm that is characterised by its virtual landscape. This said, sovereignty does not cease to exist in cyberspace simply because it is not constrained by territorial borders. Rather, states maintain sovereignty over the cyber infrastructure located on its territory where the likes of computer systems and internet networks form the physical element that bridges the gap between cyberspace to a particular state territory.[14] For this reason, the principle of sovereignty and its corresponding rules of international law apply in cyberspace and to the activities therein. The state is de facto subject to the same legal obligations in cyberspace as it is in the kinetic world. Accordingly, a number of states have argued that the rule of sovereignty has application in cyberspace including France,[15] Australia,[16] the Netherlands,[17] Estonia,[18] Finland[19] and New Zealand.[20]

In its Cyberdefense Strategic Review in 2018, France referred to the emergence of a 'digital sovereignty' in cyberspace.[21] In September 2019, the French Ministry of Defence then released a document titled 'International Law Applicable to Operations in Cyberspace', articulating France's position that international law applies to state activities in cyberspace.[22] France's position over its sovereignty within cyberspace has continued to develop and significantly, it is of the view that 'state sovereignty and international norms and principles that flow from sovereignty apply to the conduct by states of ICT-related activities'.[23] By asserting this claim, France assumes the obligations that flow

[14] Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention', *Chatham House Research Paper*, December 2019, at para 42.
[15] See Republique Française Ministère Des Armées, Droit International appliqué aux operations dans le cyberspace, 9 September 2019. Available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf (accessed 18 November, 2019).
[16] Australia International Cyber Engagement Strategy, Annex A: Application of International Law in Cyberspace (2017) available at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html (accessed 19 November, 2019).
[17] Government of the Netherlands, 'Appendix: International law in cyberspace', 26 September 2019. Available at https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (accessed 7 January, 2020).
[18] President of Estonia, 'President of the Republic at the Opening of CyCon 2019', 29 May 2019. Available at https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/ (accessed 7 January 2020).
[19] Finnish Government Ministry for Foreign Affairs, 'Finland published its positions on public international law in cyberspace', 15 October 2020. Available at https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace (accessed 21 January 2021).
[20] New Zealand Department of the Prime Minister and Cabinet, 'The Application of International Law to State Activity in Cyberspace', 1 December 2020. Available at https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf (accessed 21 January 2021).
[21] François Delerue, Aude Géry, "France's Cyberdefense Strategic Review and International Law, Lawfare", 23 March 2018, available at https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law (accessed 18 November, 2019).
[22] Republique Française Ministère Des Armées, supra note 15.
[23] Ibid.

from sovereignty, of which a corollary principle is the obligation to prevent transboundary harm.[24] The French document appears to accept the stance that there is an existing responsibility to prevent transboundary harm in cyberspace and with that, 'a reasonable level of control over the various actors in its cyber infrastructure' including that of non-state actors.[25] In essence then, France supports the view that the principle of sovereignty and thus the obligation to prevent transboundary harm operates in cyberspace, supporting the applicability of existing rules in an emerging area of international law.

Australia shares a uniform approach to the applicability of international law to cyberspace and considers that for cyber activities taking place outside of armed conflict that includes malicious use of ICT infrastructure, general principles of international law and the law of state responsibility apply.[26] The right to exercise sovereignty over cyber infrastructure within its territory means that Australia sees itself shouldering corresponding duties to ensure its territories are not used for acts injurious to the rights of other states. States, in exercising sovereignty over their cyberspace, owe obligations to ensure their cyber infrastructure is not used for acts that are injurious to the rights of other states. Reiterating both the Tallinn Manual and France's position, Australia's view merely adds to the emerging state support for the application of sovereignty and its relative obligations in cyberspace. Likewise, the Dutch support for sovereignty in cyberspace contemplates practical difficulties between sovereignty in cyberspace and the traditional concept of sovereignty, recognising that 'the precise boundaries of what is and is not permissible have yet to fully crystallise'.[27] The general view is that cyber operations causing physical harm or injury clearly violate sovereignty and reflect the failure of the state to prevent transboundary harm.[28] Finland further confirms this and 'sees sovereignty as a primary rule of international law, a breach of which amounts to an international wrongful act and triggers state responsibility.'[29] For cyber acts that do not produce direct physical or tangible impacts, its qualification as a violation of sovereignty remains a contentious matter that only the development of state practice and *opinio juris* can resolve.

The general obligation to prevent transboundary harm has been applied to diverging areas of international law, and there are compelling reasons to assert its adequacy to govern the conduct of

[24] Przemyslaw Roguski, 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I', *Opinio Juris*, 24 September 2019, available at https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed 18 November, 2019).
[25] Ann Väljataga, 'Tracing Opinio Juris in National Cyber Security Strategy Documents', *NATO CCDCOE*, Tallinn 2018, p. 8.
[26] Australia International Cyber Engagement Strategy, supra note 16.
[27] The Government of the Netherlands, supra note 17.
[28] New Zealand also confirms its position this matter and considers that 'territorial sovereignty prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state'. See supra note 20, at para 14.
[29] Finnish Government, 'International law and cyberspace: Finland's national positions', 15 October 2020. Available at https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 (accessed 21 January 2021).

states in cyberspace. With the increasing *opinio juris* surrounding the matter, there is evidence that a number of states concur the application of international legal rules in cyberspace. States have been explicit in their view that sovereignty and international norms that flow from this principle, including the obligation to prevent transboundary harm, have the same application in cyberspace as they do in other areas of international law. Therefore, the state is under a duty to prevent its territory from being used in a manner injurious to the rights of other states, and this responsibility extends to cyber infrastructure and harmful cyber activities that fall within the state's exclusive jurisdiction. Arguably, the greater dispute lies in the challenge that the Netherlands, France, and other supporting states face, which is to determine what types of cyber operations qualify as a violation of state sovereignty and whether such violations include hostile cyber operations in the form of OCTAs.[30]

III. Nature and Content of the Obligation to Prevent Transboundary Harm

The obligation to prevent transboundary harm applies only in relation to certain activities, namely, i) conduct which – if it had been committed by a state – would be internationally wrongful, and ii) conduct giving rise to sufficiently serious consequences for the legal rights of the victim state. These two issues will be examined in turn.

3.1 Quality of Harm: Internationally Wrongful Act

As a general matter, the ICJ has dealt with different types of transboundary harm in the form of nuclear accidents, hazardous waste and toxic chemicals as well as cross-border air and water pollution matters concerning environmental harm that it considers internationally wrongful acts. The obligation to prevent has since expanded into other areas of international law such as human rights protections, law of the sea and now, cyberspace.[31] Despite the differing interpretations of harm, the ICJ has refrained from explicitly defining transboundary harm in its international decisions. Instead, the ICJ recognises 'personal and material injury'[32] and 'damage and loss of human life' as derivations of transboundary harm.[33] In Corfu Channel, the ICJ considered the explosion of mines in Albanian waters as constituting harm.[34] In Trail Smelter, the Arbitration contended that pollution to the environment

[30] Michael Schmitt, 'France's Major Statement on International Law and Cyber Assessment: Use of Force, Sovereignty and More', *Just Security* (16 September 2019). Available at https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/ (accessed 18 November, 2019).
[31] See for example Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnian and Herzegovina v. Serbia and Montenegro) Judgment, I.C.J. Reports 2007, p. 43; The Mox Plant Case (Ireland v. United Kingdom) ITLOS (3 December, 2001); Michael Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (2nd Ed., Cambridge University Press, 2017).
[32] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgments, I.C.J. Reports 1986, at para 80.
[33] Corfu Channel, supra note 1, at p. 11.
[34] Ibid.

from Canada to Washington, USA amounted to harm[35] and in Pulp Mills, the polluting of the Uruguay river was enough to qualify as transboundary harm.[36] It seems then that the ICJ understands death or injury to persons to constitute harm, as well as the infliction of physical harm that impairs the value, the normal functioning or the use of something, at least, when it concerns the environment.

Harmful conduct in cyberspace, however, is yet to be addressed by the ICJ. The Tallinn Manual 2.0, a soft-law document concerning the application of international law to cyberspace, clarifies that the obligation to prevent transboundary harm only applies to conduct in cyberspace, which if attributable to the territorial state would violate an obligation of international law owed to the victim state.[37] The Tallinn Manual supports the view that the state must prevent harmful acts in cyberspace that would otherwise be unlawful if committed by the state itself. This poses the question as to whether acts of cyberterrorism, if committed by a state, are harmful acts that are internationally wrongful.

Under Article 2 of the ILC's Articles for the Responsibility of States for Internationally Wrongful Acts (2001),[38] an internationally wrongful act is defined as conduct consisting of an act or an omission that is attributable to the state and constitutes a breach of an international obligation of the state.[39] This means that if the state violates the obligation to prevent transboundary harm, or any other primary rule of international law, whether in cyberspace or in the physical world, it violates the principle of sovereignty and thus, commits an internationally wrongful act. Since sovereignty imposes legal obligations on states, namely the obligation to prevent transboundary harm for the cessation of injurious cyber activities emanating from the state's territory, the state is under a duty to engage in preventive measures in the face of harmful cyber conduct as a means of preserving peace.[40] The right to territorial sovereignty comes with the responsibility to prevent transboundary harm. States enjoy the independence to regulate its internal affairs with non-intervention, though the entitlement to this right has always been at the expense of obligation. In this sense then, the exclusive jurisdiction of states over their territories is concomitant with the general duty of states not to allow their territory to be used for acts contrary to the rights of other states of which flows the obligation to prevent transboundary harm.[41] The obligation to prevent transboundary harm can thus be seen as a 'legal

[35] Trail Smelter, supra note 7.
[36] Pulp Mills on the River Uruguay (Argentina v. Uruguay) (hereinafter referred to as Pulp Mills), Judgment, I.C.J. Reports 2010, p. 14.
[37] Schmitt, Tallinn Manual 2.0, supra note 31, Rule 14.
[38] ILC's Articles on Responsibility of States for Internationally Wrongful Acts (2001), ILC Yearbook 2001/ II (2) (ARSIWA). Hereinafter referred to as ARSIWA (2001).
[39] Ibid, Article 2 ARSIWA (2001).
[40] Schmitt, Tallinn Manual 2.0, supra note 31, Rule 2, para 12.
[41] Pulp Mills, supra note 36.

mechanism' to protect state sovereignty against harmful cyber operations which may hinder the achievement of peace.[42]

In short, the obligation to prevent transboundary harm is triggered by cyber terrorist activities that violate a primary rule of international law. It is an obligation that depends on cyber terrorist activities violating another obligation such as sovereignty, or non-intervention. Thus, cyber terrorist acts that amount to a considerable encroachment on the sovereign rights of another state to determine their internal affairs free from external intervention are significantly harmful and would amount to a violation of the obligation to prevent transboundary harm. Harm, in this sense, can be normative referring to the principle of sovereignty and the rights attached to this principle.[43] There is, however, no requirement for the harm to materialise in order for the state to breach its obligations under customary international law. The territorial state can violate the obligation to prevent transboundary harm if it did not act diligently to prevent the cyber terrorist act once it acquired knowledge of the harm occurring on or from its territories.[44] By allowing its territory to be used for acts injurious to the rights of the other states, the territorial state would be violating the territorial integrity and therefore, the sovereignty of the target state if the cyber terrorist act had been conducted by the territorial state itself. Depending on the harmful act, it is equally possible that the territorial state would be subjecting the target state (and potentially the international community) to direct or structural violence if it did allow its territory to be used in such injurious ways.

Whether there is a violation of the obligation to prevent transboundary harm is contingent upon whether the cyber terrorist act constitutes a violation of another state's rights, in addition to the diligent behaviour of the territorial state from where that harmful act originates. As we shall see, the due diligence standard regarding transboundary harm is assessed on the standard of what is reasonable and proportional to the harm in question under those particular circumstances. If the state acts diligently in regard to the transboundary cyber act and does all that it reasonably can under the circumstances, it will not violate the obligation to prevent transboundary harm even if the harm materialises. This is because the obligation is one of conduct and not result. The violation of sovereignty depends on whether the cyber terrorist act is unlawful. This means that, as a matter of international law, a cyber terrorist act launched from one state's territory against another could constitute an internationally wrongful act, if it were committed by a state and the act was unlawful.

[42] Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevention Transboundary Harm', *Journal of Conflict and Security Law*, Vol. 21, No. 3, 429 – 453 (2016), at p. 429.
[43] Nicholas Tsagourias, 'Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace', *ESIL Reflections* Vol. 9, Issue 4 (December 17, 2020).
[44] Corfu Channel, supra note 1.

This is governed by the customary rule, that in order to violate the obligation to prevent transboundary harm, a breach of the victim state's international legal rights must occur.

According to the Tallinn Manual, this applies irrespective of the type of actor operating the computer systems or networks.[45] When harmful cyber terrorist acts are committed by a non-state actor from a computer system located under the exclusive and complete control of a state, it breaches the sovereignty of the victim state. The territorial state's failure to take measures of prevention, including to terminate ongoing cyber terrorist operations conducted by either states or non-state actors, violates the sovereignty of another and constitutes an internationally wrongful act. Since sovereignty applies to both government and private cyber infrastructure, damage to either amounts to a violation of state sovereignty.[46] The principle of sovereignty thus affords protection to the state's public and private cyber infrastructure against harmful activity committed by states or non-state actors. However, the Tallinn Manual 2.0 experts put forward the view that cyber operations only violate state sovereignty when they produce serious consequences. This includes physical or material damage, death or injury to people, or the loss of functionality of the cyber infrastructure such as the reparation of computer systems or harm that is akin to physical damage or injury.[47] There is little contention over the fact that physical violations of territory are an encroachment upon the state's sovereignty. The more difficult question is whether violations of sovereignty are defined by physical violations alone as quantifications of harm, or whether non-physical harm is sufficient to violate the principle of sovereignty.

Cyber operations produce harmful effects; however, they are not always physical in nature. In fact, it is more common that harmful cyber acts do not produce physical damage. On this view, there have been several notable cyber operations that have caused categorically harmful effects that are non-physical, such as the SWIFT bank attack that resulted in the theft of millions of dollars and Younis Tsouli's online terrorist campaign that targeted hundreds of online users and illegally accessed their personal finances.[48] To limit transboundary harm to physical damage alone infers that only cyber-attacks producing physical consequences for the victim state are sufficiently grave to trigger obligations of the territorial state when this is not the case. Furthermore, transboundary cyber operations that are injurious to the rights of other states can constitute a breach of sovereignty regardless of whether they produce harmful effects resulting in physical damage. The violation occurs as a result of the harmful conduct encroaching upon a state's sovereignty, rather than being

[45] Tallinn Manual 2.0, supra note 31, Rule 2, para 3.
[46] Ibid, Rule 4 para 5.
[47] Ibid, Rule 4, para 10-14.
[48] See Chapter 3 for discussion on SWIFT bank attack in Bangladesh and Younis Tsouli's online terrorist campaign. Both caused substantive levels of harm without having physical effects.

determined on the quality of harm that manifests. Although damage can render harmful cyber conduct to constitute a breach of sovereignty, it is not the sole qualifying factor. This is because consequences of harmful cyber conduct do not necessarily lead to destructive outcomes or result in physical impairments but may nonetheless violate the state's territorial sovereignty. They may cause harmful effects to the victim state where the protection of such rights is otherwise afforded by the principle of sovereignty. This also includes the prohibition of interference with the state's governmental functions, regardless of territorial breach. Sovereignty protects the state's ability to perform functions of the government that are essential to its autonomy.[49] A cyber operation that trespasses into another state's sovereign cyber infrastructure therefore constitutes an internationally wrongful act, even in the absence of physical damage.

To summarise, the state is under a duty to prevent its territory from being used in a manner that is injurious to the rights of other states and that includes acts of cyberterrorism, that if committed by a state, would be internationally wrongful. Physical damage, however, is not a necessary requisite to determine whether an internationally wrongful act has occurred. Rather, the inviolability of a primary rule of international law triggers the state's obligation to prevent transboundary harm. As such, the state is under an obligation to prevent harmful cyber conduct from cyber infrastructure located on its territory within which it exercises sovereignty, and this obligation becomes ever more important when such harmful conduct can affect the maintenance of peace in both concepts. The question that remains is what threshold of harm is necessary to trigger obligations of prevention belonging to the state.

3.2 Quantity of Harm: De Minimis Threshold

Significant attention has been given to the question of whether the violation of rules of international law require a certain intensity of harmful effects in order to activate the obligation to prevent transboundary harm. Generally, states do not condemn violations of territorial sovereignty that are minimal as breaches of international law. Rather, harmful activities must produce harmful effects that reach a certain level of intensity to meet the threshold of harm and amount to a violation of international law. The de minimis threshold requires the harmful effects of a terrorist act to reach a certain level for it to constitute harm to the state, referring distinctly to the quantity of harm. However, the harmful effects do not have to produce physical consequences to violate rules of international law. In the words of Noam Lubell, 'the dividing line [to the threshold of harm] is neither

[49] Tallinn Manual 2.0, supra note 31, Rule 3, para 16 – 32.

the format of the attack nor the physical violence involved, but rather the level of harm caused'.[50] By exploring the extent of harmful effects, the de minimis threshold concerns the level of harm that is caused by the terrorist violence and which could threaten the peace. To determine whether an act of terrorism crosses the de minimis threshold then, is to assess the scale and nature of the harmful conduct, which involves assessing factors such as the number of citizens affected, the geographical reach of the attack, and the duration of the attack, all of which are factors that can define the scope of harm and determine whether it obstructs the achievement of peace.

The obligation to prevent transboundary harm is activated when the conduct in question produces harm or damage that is 'significant' or 'serious.' In Certain Activities, the ICJ held that there was no breach of international legal obligations because Nicaragua failed to prove that 'significant transboundary harm' was caused.[51] In Tehran Hostages, the ICJ considered the extent of damage based on its seriousness.[52] The ICJ more recently considered the 'harmful effects' of the act as a measure for its severity, where the court similarly held that 'significant damage' was the benchmark used to assess whether international legal obligations were triggered and determined liability on this basis.[53] On the contrary, the ILC in its Articles on the Prevention of Transboundary Harm from Hazardous Activities, explains that 'significant damage' means 'something more than detectable but need not be at the level of "serious" or "substantial"'.[54] Interpretations by both the ICJ and the ILC infer that harm is understood as conduct that must cross a threshold of harm that is significant, in order to constitute harm to the state and trigger obligations.

From this, it could be said that the obligation to prevent transboundary harm imposes duties on the state to take action when that harmful act is sufficiently serious to threaten the peace. In doing so, it sets a benchmark for states to act when not doing so would cause serious harm to the peace and security of the victim state. Enforcing a minimum standard of harm implies that the customary obligation subjects states to legal duties only if and when such harm crosses a certain level at which it would then be considered a serious threat to the peace and subsequently, impede the maintenance of either positive peace or even negative peace. In doing so, the obligation to prevent transboundary harm can be seen to have some normative value in striving towards peace by virtue of compelling states to mitigate certain harmful situations before they continue to perpetuate violence. In this sense

[50] Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' *89 Int'l L. Stud. 252* (2013), at p. 265.
[51] Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 655, at para 226.
[52] United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment of 24 May 1980, ICJ Reports 1980, p. 3.
[53] Pulp Mills case, supra note 36, at para 80.
[54] ILC's Draft Articles on Prevention of Transboundary Harm from hazardous Activities, with commentaries (2001), Commentary to Article 2, 152, at para (4).

then, the customary obligation endeavours to protect the international community against harmful acts of terrorism that could threaten the territorial sovereignty and peace of the victim state.

Similarly, the Tallinn Manual endorses the need for a de minimis threshold of harm. The Tallinn Manual requires that first, a legal rule is violated, and second, that the effects of the harmful act are sufficiently serious to trigger responsibilities of the state.[55] The Manual stipulates that there must be some degree of harm above that of a mere inconvenience or minor disruption. In other words, there is a minimum standard of harm that does not extend to include instances that are trivial or trifling. The Tallinn Manual applies exclusively to harmful conduct that surpasses a particular threshold and the assessment of such harm is reserved for acts that clearly cause or are likely to cause some degree of harm. More specifically, the Experts agreed that 'a peril is grave when the threat is especially severe'.[56] Not only does the Manual apply exclusively to acts that are more than de minimis, but it also distinctly recognises harm of a particularly grave and serious nature. As such, cyber operations, including those conducted by non-state actors, can violate the sovereignty of another state as long as its harmful effects are significant and severe enough to cross the threshold of harm to trigger state responsibility.

Rules of the Tallinn Manual distinguish between different types of cyber operations that affect the state, with particular emphasis that the state must not conduct cyber operations that violate the sovereignty of other states.[57] The Manual concludes that physical damage or injury can constitute a violation of sovereignty. Likewise, the remote causation of the loss of functionality of cyber infrastructure located in another state can constitute a violation of sovereignty. Of particular interest, however, is that the Tallinn Manual does not reach a consensus on whether it considers a cyber operation that results in neither physical damage nor falls below the threshold of loss of functionality of cyber infrastructure to constitute an infringement of territorial sovereignty.[58] An example used by the Manual is when a cyber operation causes cyber infrastructure to operate differently by altering or deleting data stored in cyber infrastructure without causing physical or functional consequences.[59] It is unclear whether such an incident would violate sovereignty. It can be argued then, that the Manual does not definitively reject the notion that a cyber operation can, in fact, violate state sovereignty even if it does not result in physical damage nor the loss of functionality. Accepting this, there is scope to contend that the Tallinn Manual can be interpreted to consider cyber conduct that is more than a

[55] Tallinn Manual 2.0, supra note 31, Rule 6, para 15 – 17.
[56] Ibid. Rule 26, para 4. The Manual states that to invoke the plea of necessity in response to harmful acts, the harm posed to the interest 'need not risk physical damage or injury' though 'mere inconvenience, irritation or minor disruption never suffice'.
[57] Ibid. Rule 4.
[58] Ibid. Rule 4, para 14.
[59] Ibid.

mere or minor convenience, that does not result in physical damage and that does not result in the loss of functionality of cyber infrastructure as a possible violation of state sovereignty.

To add to this, in determining what constitutes a violation of sovereignty in cyberspace, the Experts refer to the use of propaganda. The Manual emphasises that while propaganda can be transmitted into other states, generally it is not considered a violation of state sovereignty.[60] The Experts recognise that propaganda transmitted into other states for other purposes, however, may constitute violations of other rules of international law. Though the Experts do not explicitly discuss whether terrorist propaganda violates sovereignty, the Manual leaves open the potential that propaganda transmitted into other states for the purposes of terrorism may amount to a breach of international law. This understanding is premised on the idea that acts of terrorism, including acts of cyberterrorism, are universally condemned and constitute a threat to international peace and security. If terrorist propaganda violates international law, then it has the potential to violate the obligation to prevent transboundary harm rule. This said, not all forms of terrorist propaganda constitute a violation of international law. The dividing line is reserved for propaganda that poses a serious level of harm. For instance, propaganda that instigates or incites acts of terrorist violence constitutes a violation of international law that is sufficient to cross the de minimis threshold. Only then would terrorist propaganda trigger a state's responsibilities and duties under the obligation to prevent transboundary harm.

In sum, the obligation to prevent transboundary harm applies to cyber operations including those for the purposes of terrorism, that if committed by the state, are internationally wrongful and that impose a level of harm more than a mere or minor inconvenience and that could hamper the achievement of negative and/or positive peace. Both the ICJ and the Tallinn Manual endorse the de minimis threshold that otherwise applies exclusively to acts that cross a threshold of harm that is serious or significant enough to perpetuate violence. Differentiating between levels of severity that harm imposes allows states to avoid carrying an unduly heavy burden to prevent all instances of harm originating from their territories, but only to prevent the most severe and serious and this applies to transboundary cyber conduct of a terrorist nature. What has emerged is that cyber conduct, terrorist or otherwise, that does not result in physical damage nor the loss of functionality of cyber infrastructure can nonetheless constitute harmful conduct that violates sovereignty to trigger responsibilities of the state under the obligation to prevent transboundary harm.

[60] Ibid. Rule 4, para 29.

IV. The Obligation to Prevent Transboundary Harm Conditioned by the Standard of Due Diligence

As a standard conditioning the performance of the customary obligation to prevent transboundary harm, due diligence is an important criterion for assessing state efforts to meet their obligations under international law.[61] The first part explores the legal standard of due diligence including the requisite of knowledge, the state's best efforts, its technical capacity and the dereliction of duty. The second part explores different factors that have the potential to affect the state's execution of its obligations in the context of cyberspace, including effectiveness of state control, likelihood of harm and importance of legal rights and interests requiring protection.

4.1 Legal Standard of Due Diligence

4.1.1 Knowledge: Actual or Constructive

The requirement to exercise due diligence in preventing transboundary harm is triggered when the state has knowledge of the harmful act in question. It is generally understood that obligations of due diligence are triggered only when the state knows or should have reasonably known about the injurious act.[62] This is otherwise known respectively as actual knowledge and constructive knowledge. If the state knew or it was 'fully aware' of the harm, it is obligated to comply with its duties of due diligence in light of its technical capacity to do so. States are expected to have adequate 'methods of proof' to adduce knowledge of potentially harmful activities before they can materialise into threats against international peace and security.[63] This involves having appropriate mechanisms in place to monitor potentially harmful activities and being able to employ the use of such means effectively. The ICJ in Tehran Hostages concluded that Iran failed in its due diligence obligations on the basis that 'the Iranian authorities (b) were fully aware… of the urgent need for action on their part; (c) had the means at their disposal to perform their obligations; (d) completely failed to comply with these obligations'.[64] It is widely accepted that the onus is on the state to act on its duties of due diligence where it has actual knowledge of harmful activities happening on its territories.

States, however, are not expected to have absolute knowledge of all activities happening on its territories. Moreover, it cannot be deduced from the mere fact of control exercised by the state over

[61] Neil McDonald, 'The Role of Due Diligence in International Law', *International and Comparative Law Quarterly* 68 (4): 1041 – 1054, October 2019.
[62] The ICJ confirmed the requirement that states are subject to an obligation to prevent and identified the point at when this duty is triggered in Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide, at para 222. The ICJ recognises that '…a State's obligation to prevent, and the corresponding duty to act, arise at the instant that the State learns of, or should normally have learned of, the existence of a serious risk...'.
[63] Corfu Channel, supra note 1, at p. 18.
[64] Tehran Hostages, supra note 52, para 68.

its territory that the state knew or should have known about the harmful act or the authors of the act.[65] Not least is this impossible, but it creates an evidentiary burden on states to satisfy the standard of proof when it comes to demonstrating the existence of knowledge. Alternatively, knowledge can be imputed through evidence or the inference of facts, which is otherwise known as constructive knowledge. When a specific situation occurs, one that causes harm or carries a risk of causing harm, the state is expected to have known about that situation. For instance, the state may be subject to specific obligations to obtain knowledge of activities happening in its territories or under its exclusive jurisdiction as measures to prevent transboundary harm, such as the obligation to monitor specific activities. This is because the state, as sovereign, ought to have the means to acquire knowledge of potentially malicious activities occurring in its territorial control. This is emphasised by the ICJ in Corfu Channel where it pronounces that:

> the fact of…exclusive territorial control exercised by a state within its frontiers has a bearing upon their methods of proof available to establish the knowledge of that state as to such events.[66]

Though there are two types of knowledge, the International Group of Experts on the Tallinn Manual have expressed difficulty in reaching a consensus as to whether obligations of due diligence are triggered if the state has only constructive knowledge of the cyber acts in question.[67] The ICJ, on the other hand, seems to support the use of constructive knowledge. In Corfu Channel, the ICJ's judgment relied on a series of objective inferences and determined that the laying of mine fields causing significant damage could not have been done so without the knowledge of Albania.[68] The Court made determinations based on the fact Albania had knowledge of the harm, it failed to notify the UK of such harm, and it failed to warn the UK of danger posed by the mines.[69] Taken together, these factors indicate Albania's failure to comply with its obligations of due diligence. To add to this, the ICJ in Bosnian Genocide found that '…a state's obligation to prevent, and the corresponding duty to act, arise at the instant that the state learns of, or should normally have learned of, the existence of a serious risk...'.[70] In its contentious decisions then, the ICJ expressly recognises constructive knowledge as a qualifying trigger to due diligence obligations. States are responsible for taking the appropriate measures to acquire knowledge of the harm and then to respond to the harmful conduct, and this responsibility is arguably higher in cyberspace.

[65] Corfu Channel, supra note 1, at p. 18.
[66] Ibid.
[67] Michael Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare 1.0, (Cambridge University Press, 2013) p. 28, para 11.
[68] Corfu Channel, supra note 1, at p. 19 – 20.
[69] Ibid.
[70] Bosnian Genocide case, supra note 31.

The use of constructive knowledge in cyberspace seems particularly useful because establishing the existence of actual knowledge is usually hindered by technical limitations. Knowledge is constructed by smaller fragments of information that together provide an overall idea as to whether the state ought to have known about the harmful cyber conduct. For instance, a state that has specialised cyber task forces responsible for monitoring suspicious activity regarding illicit financing, will be held to a higher standard of responsibility than a state that does not have the resources to equip themselves in the same way. This is because the state has the ability to protect other states from such activities that could breed even more violent acts of terrorism and as a result, affect the preservation of positive peace. The state is expected to act in order to mitigate the potential for violent behaviour to occur and to engage in measures to reduce this potential which would otherwise legitimise structural violence within a society. If there are indicators that the state possesses the relevant mechanisms to engage in preventive measures and deter harmful cyber conduct but fails to do so, it will be held to have had constructive knowledge of the transboundary harm.

In order for states to acquire knowledge of transboundary harm, the content of the customary obligation to prevent has two distinct obligations. The state is required to equip itself with the appropriate legal and administrative apparatus normally able to guarantee respect for the international norm on prevention, and secondly, to use that apparatus with the diligence required under the circumstances.[71] On the one hand, the obligation to prevent transboundary harm is an obligation of conduct because it requires the state to employ all means reasonably available to them so as to acquire knowledge to prevent malicious cyber conduct as far as possible. On the other hand, the obligation to prevent harmful cyber conduct is equally an obligation of result because it is the obligation of a state to adopt legal, administrative or other measures to be able to acquire knowledge and exercise its jurisdiction on its territory, or any other area under its exclusive control, in order to protect the rights of other states. In other words, states are under an 'absolute' duty to implement such measures.[72] This, however, does not mean that states are under an absolute duty to prevent transboundary cyber terrorist harm. Furthermore, 'as a general rule, it is fair to say that an obligation of result in preventing terrorist activities will not be reasonable, let alone realistic'.[73] It is, however, the violation of the obligation to prevent harmful cyber conduct against another state that gives rise to the responsibility of the territorial state, regardless of whether damage is caused. The violation of the obligation to prevent transboundary harm does not mean states are legally responsible for the

[71] Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', in *German Yearbook of International Law,* Vol. 35, edited by Delbrück, Joel and Wolfrum, Rüdiger, Duncker & Humblot GmbH, 1992, Berlin Germany, at p. 26.
[72] Ibid.
[73] Vincent-Joel Proulx, 'Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?', *Berkeley Journal of International Law*, Vol. 23:3, 2005, at p. 106 – 153, at p. 146.

transboundary cyber harm. The state is responsible for its failure to prevent the unlawful cyber act, by its failure to establish the necessary laws and institutions to prevent the transboundary cyber harm, rather than the unlawful act itself.

In sum, the obligation to prevent transboundary harm is two-fold. The obligation of the state to acquire adequate apparatus to ensure it can carry out its duties is an obligation of result. Where the state is bound by an obligation of due diligence to utilise those apparatus to prevent or thwart those harmful operations when necessary is an obligation of conduct. Whether the state has knowledge, actual or constructive, of harmful cyber conduct occurring on or from its territories is contingent upon what measures are in place and how the state uses these measures to acquire knowledge of the transboundary cyber harm in order to prevent it from threatening positive peace. Therefore, the state's response to the cyber harm engages its responsibility and determines whether it has fulfilled obligations both to prevent transboundary cyber harm and under the standard of due diligence to discharge itself of duties under international law.

4.1.2 Best Efforts

When carrying out obligations of due diligence, states, in mitigating harm, notifying other states and ceasing harmful cyber operations, are expected to act only within their means. States are not expected to carry out duties that would otherwise exceed their capabilities. In doing so, states are not held to an absolute obligation to prevent transboundary harm. Rather, states are only expected to perform their best efforts, and this accounts for the fact that states possess varying degrees of technological expertise.[74] Not only does this ensure states do not engage in unreasonable measures to achieve a particular outcome that exceeds what they are capable of, best efforts imply that states do not shoulder an unduly heavy burden to prevent all forms of transboundary harm in absolute.

In this sense then, due diligence places no expectation on the state to produce certain results from the action it takes because the primary rule often lacks precise definition on how to achieve a particular result owing to its flexible nature. Instead, states are expected to perform their duties by striving to achieve a result, rather than actually having to achieve a particular result. The obligation of conduct requires states to take action that demonstrates their ability to prevent the harm, rather than imposing an obligation of result that otherwise guarantees an outcome.[75] States do not have a duty to prevent harmful cyber activity, and this includes cyber terrorist activity, but they have a duty to take reasonable steps to attempt to do so. In the words of Riccardo Pisillo-Mazzeschi, 'the obligation

[74] Paul Stokes, 'State Responsibility for Cyber Operations: International Law Issues', Event Report, *British Institute of International and Comparative Law*, October 9, 2014, at p. 12.
[75] Bosnian Genocide case, supra note 31, p. 43.

of diligent conduct is an obligation to "make every effort" as opposed to the requisite to effectively achieve an outcome in exercising diligence'.[76] From this, it can be said that international law concerns itself with the behaviour of the state rather than the outcome of that behaviour.[77] Accordingly, states are expected to carry out obligations of due diligence based on what is normally reasonable and what is normally expected of the state in typical circumstances.[78] Reasonableness is described as the 'golden thread',[79] and ensures that obligations of due diligence do not produce results that are counterproductive to its overall objectives.

4.1.3 Technical Capacity

States with the adequate technical means and capacity are expected to have mechanisms in place to appropriately monitor terrorist activities and this applies to areas where particularly serious instances of terrorist activity are foreseeable. The state's response to transboundary harm is shaped by the resources available to it, including the state's economic and technological abilities. The more resources the state has available to it, the more the state is expected to utilise such means to engage in measures of prevention and mitigate the harm as much as possible. A state that is economically developed may have sophisticated technological capacity to equip itself with appropriate mechanisms to address harmful terrorist activities. However, a state that does not have the technical capacity to prevent is not expected to act in the same way as developed states insofar that engaging in measures of prevention would be unreasonable to do so. As held by the ICJ in Bosnian Genocide, the state is only required to take measures that are 'reasonably available' and 'within its power'.[80] Due diligence obligations are thus contingent upon the level of development of a state.[81] If the resources available to the state improve or diminish, the level of due diligence expected of the state fluctuates in accordance with its capabilities.

4.1.4 Dereliction of Duty

In the event that the state does not fulfil its duties and fails to prevent transboundary harm, there is a dereliction of duty. As discussed, states do not owe an absolute duty to prevent transboundary harm, but a duty to take diligent measures to avoid harm. States are expected to take necessary regulatory and policy measures to avoid transboundary harm, as well as engaging in duties to notify and inform other potentially affected states. A failure to do so can amount to a lack of due diligence and constitute

[76] Pisillo-Mazzeschi, supra note 71, at p. 48.
[77] See Tim Stephens and Duncan French, 'ILA Study Group on Due Diligence in International Law', *International Law Association,* Second Report, (July 2016), at p. 2.
[78] Ibid, at p. 8 – 9.
[79] Ibid.
[80] Bosnian Genocide case, supra note 31, at para 403.
[81] Stephens and French, supra note 77, at p. 9.

a violation of the obligation to prevent transboundary harm. The state becomes responsible not for the harmful act itself, but for its failure to prevent the harmful act from manifesting. Where the state fails to cease operations by non-state actors that would otherwise violate the sovereignty of another state if it was conducted by the territorial state, then the state fails to comply with the obligation to prevent and thus commits an internationally wrongful act.[82] The state's lack of technical capacity, however, is not a permissible defence for the dereliction of its duties. Various measures can be taken as long as the state demonstrates an effort to alleviate the harmful effects of the transboundary harm. Thus, the duty rests on the state to ensure its territory is not being used for acts injurious to the rights of other states.

Hence, the state must engage in measures of prevention in order to prevent the harm if the OCTA is underway or alleviate the harmful effects if the OCTA has occurred, before they facilitate the commission of harmful conduct in the form of terrorist violence.[83] The state's willingness to engage with duties of prevention demonstrates its efforts at preventing acts of terrorism and cyberterrorism and to determine whether it has satisfied or breached the primary rule. The state must exercise its best efforts to prevent transboundary harm and mitigate the harm with all resources available to it in the given circumstances, even if that does little to thwart the harm. If states lacking the technical capacity to prevent refrain from taking any deterrent action, then the obligation to prevent falls foul not only of themselves, but the rest of the international community at risk of suffering from transboundary cyberterrorism.[84]

4.2 Factors Affecting the Standard of Due Diligence

Due diligence comprises three different objective elements that affect the level of diligence expected of the state.[85]

4.2.1 Effectiveness of State Control

A key feature of statehood is the existence of government having effective control. A state exercising effective control demonstrates the ability to govern as an entity and reflects the legal order in its territory.[86] States should exercise due diligence over activities within their legal or regulatory control,

[82] Jan Arno Hessbruegge, 'The Historical Development of the Doctrines of Attribution and Due Diligence in International Law', 36 *NYU Journal of Int'l L. & Pol.* 265 (2004), at p. 306. The author explains that 'acts or omissions of non-state actors are themselves generally not attributable; however, the state may incur responsibility if it fails to exercise due diligence in preventing or reacting to such acts or omissions.'
[83] Nathalie Horbach, 'The Confusion about State Responsibility and International Liability', *Leiden Journal of International Law*, Vol. 4, No. 1, (April, 1991), at p. 69.
[84] Buchan, supra note 42, at p. 446.
[85] Pisillo-Mazzeschi, supra note 71, at p. 44.
[86] Nicholas Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', *Journal of Conflict & Security Law* 1-20 (2016), at p. 12.

and this includes activities in cyberspace and those committed by non-state actors.[87] In Nicaragua, the ICJ held that the US had 'effective control' over the rebel contras, where it had 'devised their strategy and directed their tactics' by providing material support and substantially contributing towards a violation of international law.[88] The ICJ reaffirmed this test in the Bosnian Genocide case and held that the state's capacity to influence forms a vital part of the assessment when it comes to diligent conduct over transboundary harm.[89] Thus, where violations of international law are committed by non-state actors under the instruction or 'effective control' of the state on its territory, the state is held legally responsible for those harmful acts.

States must demonstrate effective control over harmful activities occurring within its territorial control and take all necessary measures to ensure its effectiveness.[90] In other words, the greater the influence the state has over the harmful act, and the more effective the state's control, the greater the responsibility of the state to prevent such harm from manifesting and affecting the achievement of peace. This, of course, remains subject to the technological and economical ability to perform such duties. On the contrary, state's that have limited control over their territory due to its lack of resources or otherwise, cannot be expected to exert the same level of due diligence when it comes to the prevention of harmful activities. The state's technical capacity thus influences the ability of the state to engage in measures of prevention when it comes to transboundary harm. There are clear delineations to the standard of behaviour required of the controlling state and the responsibilities deriving from its effective control or lack thereof. The effectiveness of state control is thus a contributing factor towards the level of due diligence expected of the state.

4.2.2 Likelihood of Harm

The more likely the harm, the higher the expectation is on the state to act in order to prevent the harm from manifesting. Obligations of due diligence are ignited only once the state can foresee that the risk of an activity causing harm exists.[91] As such, due diligence requires states to take preventive action 'when they possess scientific evidence that significant transboundary damage is likely' or 'where there is insufficient evidence but where the consequences may be severe and irreversible'.[92] That is to say, the state must act on the knowledge that it possesses, if that knowledge indicates that harm is likely to manifest. The greater the likelihood of harm, the more that state must do to mitigate

[87] Tallinn Manual 1.0, supra note 67, Rule 1, para 5.
[88] Nicaragua v. United States of America, supra note 32, at para 20.
[89] Bosnian Genocide case, supra note 31, at para 403.
[90] Joanna Kulesza, *Due Diligence in International Law*, Brill Nijhoff, 2016 (Queen Mary Studies in International Law, Vol. 26), at p. 264.
[91] Ibid, at p. 264.
[92] Tim Stephens and Duncan French, 'ILA Study Group on Due Diligence in International Law,' *International Law Association* First Report, 7 March 2014, at p. 26.

the transboundary cyber harm. It must be made clear that the likelihood of harm, however, does not extend to the scope of harm. States are not obligated to foresee the level of harm that comes their way since this would likely be difficult to determine with any accuracy, particularly in cyberspace where activity thrives on transiency and instantaneity. The characterisation of the risk is irrelevant. Rather, the state must demonstrate that it has acted diligently by preventing foreseeable significant damage, or at least, attempt to minimise the risk of such harm from affecting other states and potentially affecting the maintenance of international peace and security. Only then will the state discharge itself of obligations under the standard of due diligence.

For instance, a state may become aware of anonymous users operating from its own cyber infrastructure to flood the internal systems of another state, with terrorist propaganda to expose violent and gruesome content in support of ISIS. However, the territorial state does not know how graphic the content is or the volume of content being shared. It might, however, predict that the bombarding of another state's systems with terrorist content has the potential to result in some serious harm if the propaganda contains incitement or instigation of terrorist violence. Thus, once the territorial state learns of such cyber harm manifesting, it must act with immediacy to prevent the harm from continuing and affecting the rights of the victim state, and possibly other states. The territorial state must engage in all appropriate measures to prevent the harm from manifesting. This might include advising the victim state to temporarily suspend access to its internal systems whilst the threat is being investigated, blocking and removing the terrorist propaganda, and notifying and warning other states of the harm. The level of diligence expected of the state is contingent upon the how likely the harm is to manifest. In doing so, the state must exercise its best efforts to discharge itself of obligations under the primary rule and to fulfil its duties under the due diligence standard.

4.2.3 Importance of International Legal Rights and Interests Requiring Protection

The final factor affecting the level of diligence due is the importance of the international legal right or interest that requires protection. What is deserving of protection correlates with its significance as a legal right or a legal interest under international law. An international legal right refers to the rules of international law that pertain to a state's ultimate authority and competence to govern its people and matters within its territory. The state's international legal right includes but is not limited to both sovereignty and the right to non-intervention. The importance of international legal rights means they require utmost protection by other states, of which the highest level of due diligence can be expected from the territorial state to protect a violation of such right from occurring.

A legal interest, however, is not the same as a legal right and the former is a broader concept than the latter. Interests can be described as stakes or involvements that concern the state of which the

lack of protection of such interests can affect state functions. This includes critical national infrastructure, properties belonging to the state, financial interests and state-owned services for instance. The more significant the legal interest, the stricter the expectation of the state to act diligently to protect the interest from harm or damage. International law protects interests of the state, which, by definition, equates these as legal interests. In the context of due diligence obligations, protected legal interests refers to the interests of another state and not the state where that harmful conduct originates. It is important to distinguish here that due diligence, as an obligation owed to the victim state, concerns interests that would otherwise not be subject to harm but for the harm emanating from the territorial state. Whilst there is no formal hierarchy of interests, the standard of diligence expected of states is arguably higher for matters concerning the security of the state that serve a public interest over the likes of private interests where the state has limited capacity to act.[93]

It is important to note, however, that a lack of protection regarding a legal interest can trigger the violation of an international legal right and the following example demonstrates exactly how.

The 2017 WannaCry Ransomware attack on the NHS exemplifies the importance of international legal rights and interests requiring protection and the states corresponding duties of due diligence. This operation involved a cyberattack using the malware 'WannaCry' that upon its launch, affected around 300,000 computers in over 150 countries through the encryption of computer files.[94] Primarily, the cyber-attack affected the UK's National Health Service (NHS) and prevented users from accessing patient records as well as preventing the use of critical medical equipment. Upon infecting numerous computer systems, an automated message displayed a request for $300 cryptocurrency in exchange for the restoration of access to the NHS healthcare systems. The impact of this cyber-attack resulted in compromised database systems, severe disruption in providing medical services as well as growing international concern over the ease of WannaCry to severely disrupt national public services.[95] WannaCry thus affected the critical national infrastructure of the UK.

There is scope to contend such a hostile cyber operation against the legal interests of the state has the capacity to violate sovereignty and thus, an international legal right belonging to the victim state. On this point, the Tallinn Manual 2.0 condemns violations of sovereignty which it refers to as whenever a cyber operation causes damage to cyber infrastructure in another state. It does so by

[93] Ibid, at p. 3. The ILA Report uses the example in Chapman (UNRIAA IV, 632) that the interest requiring protection was a consular official of the United States, of which their position relating to government office may increase the standard of diligence expected.

[94] See Will Smart, 'Lessons Learned Review of the WannaCry Ransomware Cyber Attack', *Department of Health & Social Care, NHS England Report* (February 2018).

[95] See National Audit Office, 'Investigation: WannaCry Cyberattack and the NHS', *NAO Department of Health* (25 April 2018). Available at https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (accessed 1 July 2020).

elaborating on 'damage' as a permanent loss of function that requires physical repair of the damaged infrastructure.[96] This, however, cannot be said of the WannaCry malware, which did not result in any physical damage. Rather, the cyberattack can be distinguished as a series of substantial disruption of functions that relied significantly on the timely delivery of medical care. By causing extensive delays to medical care and severely disrupting the provision of public services belonging to the UK, the effects of WannaCry could be considered sufficient to constitute harm.[97] Moreover, consequences of a physical nature are no longer the prevailing norm for quantifying violations of sovereignty. The characteristics of a virtual domain lends itself to non-conventional consequences that cannot be equated to a physical world, even by analogy. The argument can thus be put forth that the WannaCry operation not only affected the legal interests belonging to the UK, but it also violated the sovereignty of the affected states that suffered from the disruption, which as a significant international legal right of states, requires protection under international law.

Whilst the cyber-attack did not cross the threshold for the use of force, its imposition massively compromised the functioning of the healthcare system that provided lifesaving treatment within the domestic state infrastructure.[98] Equally, the WannaCry attack jeopardised numerous interests of the state. Notwithstanding the national health system generally, but the privacy of individuals medical data and records, access to medical services hindered such as appointments and procedures, effective functioning of public medical care and the integrity of the state to perform its government functions, all of which are significant interests requiring protection.[99] At least in the UK, the WannaCry attack caused substantial disruption likely to constitute 'damage' that is sufficient to cross the threshold of harm to ignite obligations of prevention owed by the territorial state, speculated as North Korea.[100] Subject to the obligation to prevent transboundary harm and where the interests requiring protection are significant then, North Korea is responsible for exercising its best efforts to prevent the attack from manifesting and continuing to cause harm. This includes the duty to notify and warn other states of WannaCry, to exchange any intelligence information it may have acquired and to cooperate with other states to prevent the continuation of this threat. If North Korea knowingly allowed the WannaCry attack to be launched from its territories and failed to put an end to such harm, and the

[96] Schmitt, Tallinn Manual 2.0, supra note 31, at Rule 4.
[97] Michael Schmitt and Sean Fahey, 'WannaCry and the International Law of Cyberspace', *Just Security* (December 22, 2017). Available at https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/ (accessed 1 July 2020).
[98] See generally Schmitt and Fahey, ibid; Michael J. Adams and Megan Reiss, 'How Should International Law Treat Cyberattacks like WannaCry?', *Lawfare Blog,* (22 December 2017). Available at https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry (accessed 1 July 2020).
[99] National Audit Office, supra note 95.
[100] Schmitt and Fahey, supra note 97.

consequences of that harm are serious and adverse, it commits an internationally wrongful act by its failure to comply with its obligations of due diligence.[101]

But of course, the duty of due diligence depends on the circumstances that prevail. If, for instance, the WannaCry malware did not obstruct the functioning of the national healthcare system but instead led to a large data breach resulting in the loss of sensitive personal information, is this an international legal right or interest requiring protection? There are various incidents which resemble such an operation, the likes of Sony Pictures hack (2014), Marriott Hotels hack (2018) and the Yahoo! hackings (2014) among several others, are examples of retrieving sensitive information as the objective of such large-scale cyber operations.[102] Personal data, financial data and sensitive information might not seem significant compared to the obstruction of health and medical services, certainly not when the latter hinges on life or death. Yet, the volume in which hacking for personal information takes form is an increasingly menacing offence within unlawful cyber operations that seems to occur ubiquitously, both in private and public sectors. Owing to the fact that it would most certainly fall within the duties of the state to safeguard the rights of its citizens by protecting legitimate public interests, the state is under an obligation to act with due diligence to prevent such acts from occurring.

The importance of the legal right or interest requiring protection is determined on the basis of several factors that shifts its position of value under international law. The obligation to prevent harm serves to protect the fundamental rights and interests of the international community, the national security of the state, as well as the safety of its civilian population. In other words, the state can take action to prevent transboundary harm where the absence of doing so would affect the legitimate rights and interests of the state. The ICJ in Nicaragua commented on this point by clarifying that any conduct taken by the state in response to harm must constitute '"measures… necessary to protect" essential security interests'.[103] The court further elaborated that factors qualifying this determination are bound by both reasonableness and necessity.[104] Since the degree of diligence owed by the state is influenced by the rights or interests requiring protection, measures designed to protect these rights

[101] Ibid.

[102] See generally Clare Sullivan, 'The 2014 Sony Hack and the Role of International Law', 8 *Journal of National Security Law & Policy 437* (2016); Nicole Perlroth, Amie Tsang and Adam Satariano, 'Marriott Hacking Exposes Data of up to 500 Million Guests', *The New York Times* (Nov.30, 2018), available at https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (accessed 22 July 2020); Michael Schmitt, 'International Law and Cyber Attacks: Sony v. North Korea', *Just Security* (17 December 2014). Available at https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (accessed 13 July 2020).

[103] Nicaragua, supra note 32, at para 271.

[104] Ibid, at para 224. The court stats that 'it is difficult to deny that self-defence against an armed attack corresponds to measures necessary to protect essential security interests. But the concept of essential security interests certainly extends beyond the concept of an armed attack and has been subject to very broad interpretations in the past. The Court has therefore to assess whether the risk run by these "essential security interests" is reasonable, and secondly, whether the measures presented as being designed to protect these interests are no merely useful but "necessary"'.

and interests must consider the risk of doing so and any measures taken must cross the threshold beyond that of 'mere useful' to constitute necessary. Ergo, the state is confined to take only the most appropriate measures to prevent transboundary harm and in doing so, to satisfy the requisites that are established by the ICJ in its contentious decisions concerning obligations owed by the state.

V. Measures of Preventing Transboundary Harm

The obligation to prevent transboundary harm encompasses specific duties of prevention that are directly relevant to the circumstances before it.[105] For states to ensure the hygiene of cyber infrastructure, they are responsible for '[preventing or punishing] non-state actors that use its cyber infrastructure to perpetuate malicious cyber activities against other states.'[106] As a result, there are a number of responsibilities that fall on the state once it learns of transboundary cyber harm including the duty to notify and warn other states, the duty to cooperate and exchange information, as well as the duty to investigate, punish and prosecute those responsible.

5.1 Duty to Notify and Warn Other States

When the state becomes aware of potentially harmful activity occurring on its territory, an essential duty is for the state to notify and consult with other affected states.[107] The territorial state from where the harm originates must communicate and inform other states that may fall victim to the cyber conduct. In doing so, the state takes the responsibility to mitigate the harmful conduct and reduces the risk of continued harm for other states. Where possible, the state must warn other states of the incoming harm so that the affected state can minimize, if not prevent the harmful effects as much as possible. It might be the case that the state does not have the capacity to prevent the harm in its entirety because it lacks the resources or material capacity to do so. In such instances, it can still fulfil its duties by notifying and warning other states of the harm. The obligation to prevent transboundary harm is one of conduct and not one of result, thus requiring the state to do all that it reasonably can under the given circumstances. It does not require the state to exceed its capabilities when it comes to obligations under the primary rule. As long as the state exercises its best efforts at mitigating the

[105] Ilias Plakokefalos, 'Prevention Obligations in International Environmental Law', *Yearbook of International Environmental Law*, Forthcoming Amsterdam Law School Research Paper No. 2013 – 37 (July 5, 2013).
[106] Tsagourias, supra note 86, at p. 12.
[107] Pulp Mills case, supra note 36. Argentina claimed that under the Statute of the River Uruguay, Uruguay was under an obligation to notify both the Commission on the River Uruguay and Argentina on any plans that might have environmental effect on the river. This is reiterated by the ICJ in Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica Along the San Juan River (Nicaragua v. Costa Rica) (Int'l Ct. Justice Dec. 16, 2015), at para 104. The ICJ held that '…in conformity with its due diligence obligation, [the state must] notify and consult in good faith with the potentially affected state, where that is necessary to determine the appropriate measures to prevent or mitigate that risk'.

harm, even if all that it can achieve is to notify and warn other states of the transboundary cyber harm, it will fulfil its duties under the obligation to prevent transboundary harm.

The obligation to notify, however, must adhere to certain requisites. The case of Pulp Mills has established that it is the state of origin that must notify the possibly affected states through its official channels of communication.[108] It is the territorial state from where the transboundary harm emanates that is responsible for informing other states of the potential harm that may derive from its territories and this communication must come directly from the state itself. Particularly, in the realm of cyberspace where events are expeditious and instantaneous, the need to notify affected states without delay and with the most efficient means available is paramount. That is to say, the state may still violate the duty to notify and warn other states if it does not engage in such measures in a timely manner where such information still retains value to the affected states.

5.2 Duty to Cooperate and Exchange Information

Under general international law, the duty to cooperate is another core prevention principle deriving from customary international environmental law.[109] The obligation to cooperate requires states to foster a collaborative relationship with other affected states and to establish what measures can be taken to thwart the continuation of harmful conduct.[110] The territorial state is expected to take measures to jointly manage the harm by collaborating with the appropriate agencies of the affected states. Accordingly, one ancillary responsibility that derives from the duty to cooperate is the duty to exchange information.[111] If the state is privy to information that can deter the harm, then it must engage in its duties to share that information with relevant authorities and states that are potentially affected by the harm. This might include cooperating with national counterterrorism agencies, financial bodies, organisations tackling money laundering and other relevant units and task forces in order to share information with affected states and contribute towards the cessation of transboundary terrorism. Sharing information such as domestic and foreign intelligence, financial activity reports and user data are just some sources that can provide information in mitigating harm for affected states.

[108] Ibid, at para 110.
[109] The duty to cooperate is a supplement of the duty of due diligence. Deriving from international environmental law, the duty to cooperate historically concerns transboundary natural resources, which, if they are to be exploited in a manner whereby the rights and interests of all states involved are recognised. See The Mox Plant Case (Ireland v. United Kingdom) ITLOS (3 December 2001).
[110] Bosnian Genocide case, supra note 31.
[111] See Plakokefalos, supra note 105, at p. 17 – 21. The author identifies various obligations of prevention that emanate from international environmental law, including the obligation to exchange information which they conclude as forming 'part of general international law'.

Although the duty to exchange information derives from matters of international environmental law,[112] it is becoming increasingly essential to share information in a timely manner when it comes to the prevention of cyber operations.[113] The territorial state may acquire information specifying the details of the incident including when and how it occurred, the number of victims that were targeted, the value of personal and financial assets stolen, and intel of the perpetrator or terrorist group for example and this is all information that must be shared with other states as soon as possible. This is because in the realm of cyberspace where cyber operations often happen within a matter of seconds, detection of its character tends to be difficult to establish until after the cyber incident has occurred and harm has been inflicted. The obligation to prevent thus tends to concern the performance of states prevention duties after the transboundary cyber harm has materialised. Therefore, it is imperative for states to act fast and take appropriate measures imminently to prevent the cyber operations from manifesting and causing more harm to other states. Whilst these duties are not exclusive to cyberspace, they are prevention obligations that have been crystallised in customary law with evidence of state practice and therefore, can be applied to cyberspace operations.[114]

5.3 Duty to Investigate, Prosecute and Punish

Where possible, the state is also expected to investigate, prosecute and punish those responsible for harmful acts.[115] In order to engage in this duty, states are expected to possess the appropriate legal, administrative and judicial apparatus that allows them to prevent, prohibit, investigate and punish harmful transboundary activities. The duty to investigate requires the state to carry out formal inquiries to discover and examine an incident of transboundary harm in order to establish the facts surrounding it. The state must probe relevant areas of investigation and engage in diligent fact-finding procedures using the appropriate mechanisms available. Investigation can establish the perpetrator of harm in order for appropriate forms of punishment to be imposed. The enforcement of punitive measures is a means of protecting both the victim state and the affected individuals in light of transboundary harm.[116] As such, it is imperative that measures of prevention are exercised with immediacy so that information relating to the perpetrator of the cyber harm can serve practical use and provide leads for the investigation. The inquiry, however, may still be hindered by the anonymity of cyberspace, which makes for identifying the perpetrator of the transboundary harm a difficult task

[112] Mox Plant (Ireland v United Kingdom) (provisional Measures) International Tribunal of the Law of the Sea (2001) 41 ILM 405. The International Tribunal of the Law of the Sea contended the failure to cooperate and exchange information and to find measures to prevent harm being caused could constitute a violation of the duty to cooperate to ensure the protection of the marine environment.
[113] Akiko Takano, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications', *MDPI Laws* 2018, 7, 36, at p. 9.
[114] Corfu ChanneL, supra note 1.
[115] S/RES/1373 of 13 September 2001, at para 2(e).
[116] Mexico/ General Commission Claims, supra note 6.

to establish.[117] IP addresses can be bounced and the location of the perpetrator or the computer system of where that cyber operation originated from may not be genuine. In such cases, it is generally accepted that the geo-location of the computer used to launch the cyber operation can provide ample evidence to attribute legal responsibility to the state, particularly where that state failed to prevent or mitigate instances of harm that were serious and significant.

VI. Conclusion

The obligation to prevent transboundary harm is a principle of customary international law that has developed through state practice and *opinio juris*. This chapter has identified the nature, content and scope of the obligation and identified that the rule embodies the notion that states are not to knowingly allow its territory to be used for acts injurious to the rights of other states. The discussion revealed that a number of states agree that sovereignty applies in cyberspace, and as a result, as do the rules emanating from this principle including the obligation to prevent transboundary harm. The chapter explored this obligation and identified that the principle applies on the basis of two factors; conduct which – if it had been committed by a state – would be internationally wrongful, and conduct giving rise to sufficiently serious consequences for the legal rights of the victim state.

This chapter revealed that the obligation to prevent transboundary harm is activated. in response to a violation of an international legal right belonging to another state. This violation must be a primary rule of international law such as the principle of sovereignty or the principle of non-intervention. Importantly, such a violation can result from an act of cyberterrorism committed by non-state actors. Whether a cyber act is sufficiently serious or significant to engage the duty of prevention is contingent upon the harm constituting more than a mere or minor inconvenience. The obligation to prevent transboundary harm is triggered only if the harm crosses this de minimis threshold. Equally, this chapter showed that the obligation to prevent transboundary harm has some normative value of striving towards peace by imposing duties onto states to reduce the potential for harmful acts to perpetuate a culture of violent behaviour.

This chapter also showed that in order to meet this obligation, states are expected to perform their duties subject to the standard of due diligence, which is triggered by actual or constructive knowledge of the harmful activity. Determining the state's performance of its obligations is also contingent on the state's efforts and its technical capacity. Obligations of due diligence further take into consideration the effectiveness of state control, the likelihood of the harm and the importance of the international legal right or interest that requires protection. These factors ensure that the state

[117] See Buchan, supra note 42.

is not under an unduly heavy burden to prevent transboundary harm and thus ensures reasonableness in the discharge of duties under the obligation. The more difficult question that remains is whether the obligation to prevent transboundary harm applies to OCTAs that lack harmful effects comparable to that of traditional acts of terrorism. Accordingly, the next chapter explores the obligation to prevent transboundary harm applied to OCTAs to determine whether it can adequately prevent and suppress transboundary cyber terrorist activities under international law.

Chapter Six

APPLYING THE OBLIGATION TO PREVENT TRANSBOUNDARY HARM TO OCTAS

I. Introduction

As discussed in the previous chapter, customary international law imposes an obligation upon states to prevent the cyber infrastructure located within their territory from being used to interfere with the legal rights of other states. With this in mind, this chapter examines how the obligation to prevent transboundary harm applies to OCTAs under international law and how the theory of peace framework comes into play when assessing this principle of customary law.

The chapter adheres to the following structure. Section II examines whether OCTAs are of a kind and severity to trigger the application of the obligation to prevent transboundary harm. Section III explores the due diligence standard that conditions the performance of the obligation to prevent transboundary harm and in particular when it can be said that states have knowledge of OCTAs emanating from their cyber infrastructure and what efforts they must exert to prevent and suppress this type of malicious cyber activity. Section IV sets out the factors that affect the level of due diligence that states must exercise when it comes to the prevention of OCTAs namely, the effectiveness of state control over their cyber infrastructure, the likelihood of harm resulting from the OCTA and the importance of the international legal rights and interests requiring protection. In light of this discussion, this section examines the different types of measures a state can take to prevent OCTAs including the duties to notify, the duty to cooperate and the duty to investigate. Section V then applies the obligation to prevent transboundary harm to OCTAs. Lastly, section VI offers conclusions.

II. OCTAs as Transboundary Harm

The obligation to prevent transboundary harm applies where two conditions are met: first, where a non-state actor engages in harmful conduct which, if committed by a state, would amount to an internationally wrongful act; and second, where that harmful conduct gives rise to sufficiently serious consequences. These issues will now be discussed in turn as it relates to OCTAs.

2.1 OCTA's Interference with Legal Rights as Violations of International Law

There are some OCTAs which would constitute a breach of international law and obstruct the achievement of international peace and security. As discussed in Chapter 5, sovereignty is a primary rule of international law the breach of which constitutes an international wrongful act. The principle of sovereignty refers to 'the whole body of rights and attributes which a state possesses in its territory,

to the exclusion of all other states, and also in its relation with other states'.[1] The principle of sovereignty therefore prohibits states from interfering in the sovereign affairs of other states, that is, interference with their exercise of inherently governmental functions.[2] What amounts to an inherently governmental function differs between states depending upon their internal political constitution but certain functions are core to states, for example, organizing democratic elections or determining which acts are permitted to enter or leave state territory.[3]

The principle of sovereignty applies to cyberspace, and this has been affirmed by a number of states. State sovereignty encompasses all cyber infrastructure that is physically located within its territory and this extends to the computer networks and systems supported by that infrastructure.[4] Moreover, state sovereignty covers cyber infrastructure located within state territory regardless of whether it is privately or publicly owned or operated. A more difficult question is to identify when remotely launched cyber operations against this cyber infrastructure amount to a violation of the principle of sovereignty. The majority of the Tallinn Manual experts were of the view that it is only those cyber operations that produce sufficiently harmful effects within a state's computer networks and systems that trigger a breach of this rule.[5] This view, however, sets the threshold too high. Instead, the view of the present author contends that any state-sponsored non-consensual cyber operation against cyber infrastructure located within another will trip a violation of the principle of sovereignty. This is a view that has been most forcefully advocated by Buchan[6] but has also been increasingly recognized in state practice.[7]

If this intrusion approach to sovereignty is adopted, there are certain types of terrorist operations – including those committed in and through cyberspace – that would constitute a breach of the principle of sovereignty. A cyber operation launching a terrorist recruitment campaign on the computer networks of another state is an example of conduct which would breach sovereignty. To be clear, it is the non-consensual trespass into a domain protected by state sovereignty that qualifies this

[1] Corfu Channel case (U.K. v. Alb.) (hereinafter referred to as 'Corfu Channel case'), Merits, 1949 ICJ REP. 4, 43 (Apr. 9) (Individual Opinion by Alvarez J.).
[2] Island of Palmas case (United States v. The Netherlands), Scott, Hague Court Reports 2d 83 (1932) (Perm. Ct. 4rb. 1928), 2 U.N. Rep. Intl. 4rb Awards 829, 4 April 1928.
[3] Nicholas Tsagourias, 'Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace', *ESIL Reflections* Vol. 9, Issue 4 (December 17, 2020).
[4] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* (2nd Ed. CUP, 2017).
[5] Ibid, at Rule 6.
[6] Russell Buchan, *Cyber Espionage and International Law* (Hart Publishing, 2018), at Chapter 3.
[7] See Republique Française Ministère Des Armées, Droit International appliqué aux operations dans le cyberspace, 9 September 2019. Available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf (accessed 18 November, 2019); Nournews, General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat, (18 August 2020). Available at https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat (accessed 25 February 2021).

conduct as a breach of the principle of sovereignty. Equally, a cyber operation which, if committed by a state, runs websites on the cyber infrastructure of other states for the purposes of terrorist financing would amount to a violation of the principle of sovereignty, provided of course the websites are operated without the consent of the host state. Both examples would likewise obstruct the achievement of peace by fostering an environment that encourages and perpetuates violent terrorist behaviour and subjects the societies therein to structural violence by preventing the conditions necessary to creating positive peace.

It may also be the case that OCTAs violate the principle of non-intervention. The principle of non-intervention prohibits coercion within the *domaine réservé* of another state. The prohibition of intervention contains two elements. First, the harmful activities must be coercive in that it compels the target state to engage in an activity it would not otherwise engage in or to refrain from activities that it would, but for the coercion, undertake.[8] Second, the harmful activities must be directed at the *domaine réservé* of the target state. The notion of *domaine réservé* reflects the areas of state activity that are internal and reserved for within its domestic jurisdiction, such as its 'political, economic, social and cultural system, and the formulation of foreign policy'.[9] Thus, OCTAs that coercively intervene in matters that fall within a state's sovereign affairs would amount to a violation of international law.[10] Not least do such OCTAs threaten the national security of states, they create conditions that encourage violent behaviour and legitimize structural violence beyond national borders. Take for example, the situation where a terrorist group launches a cyber operation which encrypts the data of valuable files that are necessary for a state to deliver essential public services. The terrorist group demands payment of a ransom in the form of cryptocurrencies for the return of such data. The coercion of the target state's government to pay the ransom in exchange for the data is an intervention of the *domaine réservé* of the victim state and a prime example of how an OCTA of this kind can be used to perpetuate violent terrorism.

Equally, OCTAs may violate certain Security Council resolutions. The Security Council's adoption of Resolution 1373 (2001) notably declared that 'any act of international terrorism constitutes a threat to international peace and security', which subsequently lead to a universal condemnation of international terrorism by the international community.[11] As established in Chapter 4, the binding

[8] Michael Schmitt and Sean Watts, 'Beyond State-Centrism: International Law and Non-State Actors in Cyberspace', *Journal of Conflict & Security Law (*2016), 1 – 17, at p. 6; see also Chapter 5 discussion on sovereignty and cyberspace.
[9] Military and Paramilitary Activities in and against Nicaragua (hereinafter referred to as 'Nicaragua v. United States of America'), Merits, Judgments, I.C.J. 14, Reports 1986, para 288 (quoting Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Order, 1984 I.C.J. 169, para 41 (May 10)).
[10] See Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace', *EJIL:Talk!* (August 26, 2019).
[11] United Nations Security Council Resolution S/RES/1373 of 28 September 2001.

nature of Resolution 1373 imposes legal obligations upon states to prevent and suppress the financing of terrorist acts and to refrain from providing any form of support to those involved in terrorism, including by suppressing recruitment of terrorist members.[12] Thus, if a terrorist group was recruiting individuals via social media who were then responsible for the commission of several terrorist acts directing violence against a state's government, the territorial state from where that cyber infrastructure is located would be in violation of Resolution 1373. A terrorist operation of this kind would impede the achievement of peace in both its negative and positive concepts specifically by creating the ideal conditions to legitimize violence but also by propagating the development of structural violence to that of direct violence. Absent of any effort to prevent this OCTA, the territorial state would be supporting the violent behavior of the terrorist organisation that would constitute a material breach of its obligations pursuant to Resolution 1373. In a similar manner, part of Resolution 2253 (2015) imposes a legally binding obligation upon states to freeze assets of those associated to ISIS by which association includes the financing, planning, facilitating, preparing and perpetrating of acts in support of, the supplying of arms to and the recruiting for the terrorist group.[13] If a group of ISIS supporters from the UK were exploiting stolen credit card details online, of which such transactions were linked to the purchasing of firearms and weapons to send to insurgents in Iraq, the UK would be under an obligation to freeze the assets of said ISIS supporters. If the cyber terrorist financing operation was attributed to the territorial state – the UK – it would violate its obligations under Resolution 2253 and thus, breach international law.

Critically, there are also some OCTAs that would not violate a rule of international law. For instance, if a terrorist group runs a Just Giving page to request money to promote terrorist causes, it is difficult to see how this would violate an existing rule of international law. Where a terrorist group preys on individuals in internet chat rooms to indoctrinate and recruit them into a terrorist organization, this does not constitute a violation of international law. Equally, if a terrorist group uses Twitter to publish messages criticizing another government's administration, this does not breach a rule of international law. While these activities can be considered harmful insofar that they are the building blocks for terrorism, given that they would not represent a breach of international law, it is difficult to see how states are under an obligation to prevent such activities emanating from their territory. Sovereignty is about the interference with inherently governmental functions and non-intervention involves one state compelling another to think or act in a certain way. In light of this,

[12] Ibid, at para 1 (a) and para 2 (a).
[13] United Nations Security Council Resolution S/RES/2253 of 17 December 2015, at para 3 (a) and (c).

OCTAs of this nature would not infringe on the principle of sovereignty or non-intervention and therefore, would not amount to any violations of international law.

This said, it is pertinent to recognize that such OCTAs would nevertheless impede the achievement of positive peace by creating aspects of a culture that can be used to legitimize structural violence. Terrorists' exploitation of cyberspace to conduct OCTAs remains a primary impediment to achieving peace and whilst there are certain OCTAs that may not constitute a breach of international law, their role in encouraging violent terrorism cannot be overlooked. Given that OCTAs affect the achievement of positive peace and positive peace is the best promotion against violence, ensuring the prevention of OCTAs on an international level is a significant and sustainable remedy to achieving peace in the long term. Accepting this, the international community must be willing to prevent and suppress OCTAs in order to create the conditions necessary for eliminating violence and to diminish the potential of OCTAs from causing structural violence to direct violence. Absent of this, international terrorism will remain at the forefront of the international security agenda and continue to threaten peace for the entire international community.

The above analysis has shown that OCTAs exist on a scale and as we can see, the international law obligation upon states to prevent transboundary harm would apply to some but not all OCTAs. What this shows is that, in some circumstances, customary international law provides states with a certain amount of protection from OCTAs but, importantly, this protection has its limits.

2.2 De Minimis Threshold

Even if the harmful conduct of non-state actors would constitute a breach of international law, the obligation to prevent transboundary harm is only triggered where that act would cause a minimum level of harm. This is because states are not required to prevent acts of non-state actors that cause a mere or minor inconvenience to or interference with the legal rights of other states. Imposing a threshold application ensures that international law does not concern itself with trivial acts and equally safeguards states from having an unduly heavy burden when it comes to state responsibility of OCTAs. At the same time, imposing a de minimis threshold indicates that the obligation to prevent transboundary harm applies only when it considers the act in question to threaten the peace. In other words, the customary principle seems to have normative value of striving towards peace but only when peace is threatened by a particular type of harmful conduct.

A couple of examples will help to illustrate the application of the de minimis standard in the context of the obligation to prevent transboundary harm. A cyber operation which shares Facebook posts in support of ISIS launched via the computer systems of another state would violate sovereignty.

Such an operation would equally threaten the achievement of positive peace by enabling those who view that post to engage in violent behaviour which as a result, legitimises structural violence. The intrusion into another state's cyber sovereign space would constitute a breach of its sovereignty. Such an OCTA would not however, cross the de minimis threshold in order to trigger the obligation to prevent transboundary harm. Sharing propaganda of this nature would not amount to an interference with the legal rights of other states and thus, would not be sufficiently severe to necessitate international legal action vis-à-vis the obligation to prevent transboundary harm. Whilst an OCTA of this kind might not be serious enough to trigger customary law, it nonetheless continues to pose severe threats to the theory of peace in its positive concept and must still be subject to prevention under international law.

In another instance, a cyber terrorist operation which encourages individuals on Twitter to vote against a state's political party would encroach upon the legal rights of another state. By intervening with the internal affairs of that target state such an OCTA would amount to an international wrongful act. Sharing Tweets to discourage allegiance to a political party, however, is not sufficiently severe but instead, constitutes a mere or minor inconvenience that would not reach the minimum threshold of violence required to trigger state responsibility. While such OCTAs may encroach upon the legal rights of the target state and violate international law, they must still reach a sufficiently severe threshold of violence. Otherwise, OCTAs of this nature fall short of triggering the state's obligation to prevent transboundary harm even if they obstruct the achievement of positive peace.

On the contrary, a terrorist group inciting a population to rebel against a particular state through the use of cyber means is an infringement of another state's international legal rights that would also cross the de minimis threshold. Inciting violence of this nature constitutes coercive behaviour because it interferes in the affairs of another state with an intention to deprive that state of its free will in relation to the exercise of its sovereign rights.[14] Thus, such an OCTA would amount to a violation of the non-intervention principle. At the same time, inciting terrorist violence is sufficiently severe to cross the de minimis threshold and trigger the state's obligation to prevent transboundary harm. Of all OCTAs, incitement can be described as the most potent cause of structural violence because it directly encourages and instigates a culture of violent behaviour that perpetuates terrorism and potentially leads more serious and sinister terrorist operations. Incitement of terrorism is an OCTA that has such close proximity to an act of terrorism that, if committed by a state, would amount to an international wrongful act. In turn, this would require the territorial state from where that incitement

[14] Lassa Francis Oppenheim, *Oppenheim's International Law*, Vol. 1: Peace, 3rd edn, Roxburgh, R.F. (ed.), London: Longmans (1920-21), p. 221.

emanates to engage in measures to prevent or mitigate the harmful effects caused by the OCTA in order to discharge itself from its duties under the obligation to prevent transboundary harm.[15] Accepting this, it can be concluded that the obligation to prevent transboundary harm promotes positive peace insofar that it enforces obligations on the state to take action to prevent certain types of OCTAs, namely the incitement of terrorism.

The de minimis threshold thus ensures states are held responsible only for the most sufficiently serious acts of transboundary cyber harm that threaten international peace and security. The basis of the de minimis threshold can thus be seen as two-fold. First, it protects sovereign states from having to deal with trivial instances of transboundary cyber harm. Second, where such harm is more than de minimis the expectation is for states to safeguard the international legal rights of other states from OCTAs that could potentially have been prevented by the territorial state itself in order to minimise its threat against positive peace.

III. The Obligation to Prevent Transboundary Harm Conditioned by the Standard of Due Diligence in Cyberspace

The obligation to prevent transboundary harm is conditioned by the standard of due diligence. For this reason, the following discussion considers the elements of due diligence as they apply to OCTAs in cyberspace.

3.1 State's Knowledge

Knowledge is the 'decisive element' of due diligence, which upon its acquisition, engages the states responsibilities for OCTAs under international law.[16] Obligations of due diligence apply where states have actual knowledge of OCTAs. However, actual knowledge is unlikely in the context of cyber terrorist related activities due to the privilege of anonymity and the speed of cyber communications, which makes acquiring knowledge of OCTAs a challenging task in cyberspace. It is often the case that the target state has difficulty furnishing genuine proof of facts giving rise to responsibility from circumstances within the exclusive territorial control of another state. Ultimately, states are unlikely to have knowledge of all OCTAs happening on their territory or under any other areas of their exclusive control. As such, a more liberal recourse to inference of factual and circumstantial evidence is

[15] This benchmark is similarly reiterated in the Tallinn Manual, which stipulates that harmful conduct must be sufficiently serious to constitute harm and cross the de minimis threshold to trigger international legal obligations. Schmitt, M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* 2nd Ed. CUP, (2017), at Rule 6, para 16.
[16] Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', *Baltic Yearbook of International Law,* Vol. 14, (2014), pp. 23 – 29, at p. 27.

permissible through constructive knowledge, which is otherwise based on the premise of what the state should have reasonably known at the time of the OCTA in question.[17]

The use of constructive knowledge is supported by the ICJ. In Corfu Channel, the ICJ explained that 'the state cannot evade such a request [to explain a violation of international law] by limiting itself to a reply that it is ignorant of the circumstances of the act and its authors'.[18] Rather, there must be a 'series of facts linked together and leading logically to a single conclusion' for an inference of facts to be drawn.[19] Where a state's counterterrorism unit discovers OCTAs emerging from or transiting through its territory, the state shall be seen as having actual knowledge of the OCTA emerging from under its exclusive control. The state may not be aware of the OCTA, but the obligation to prevent transboundary harm is triggered where it objectively should have known of the conduct. In the cyber context, the state is presumed to have knowledge of the OCTA where a state diligently monitors its cyber infrastructure as a result of previously having its systems targeted by terrorist attacks or by detecting intrusions into protected services.[20] Equally, a state may be presumed to have knowledge of a threat where its cyber infrastructure has become a well-known sanctuary for terrorist groups to launch OCTAs. In such cases, knowledge can be constructed and imputed to a state because the state ought to have discovered the terrorist activity by actively seeking knowledge of it.[21]

Yet, in the context of cyberspace, knowledge of terrorist activities can be problematic, particularly where the occurrence of certain operations is concealed. Terrorist groups can easily relocate to safe-haven territories such as Syria, Iraq and Libya, where acquiring knowledge of terrorist activities is obscured by those providing protection as well as the means and skills necessary to continue terrorist operations.[22] This being said, for states that are well-known safe havens to terrorist groups intending to orchestrate and launch harmful cyber operations, knowledge can be reasonably presumed. For instance, it is widely known that, during the height of ISIS' proliferation, ISIS used the territory of Syria to commit various terrorist operations necessary for its effective functioning. This conclusion can be drawn from the fact that in 2017, ISIS gained control of the territory of Syria (and Iraq), and formed its military base for ISIS fighters and created a sprawling tent camp to house thousands of family members of ISIS fighters.[23] Given this, Syria could be considered to have constructive knowledge of

[17] Corfu Channel, supra note 1, at p. 18.
[18] Ibid.
[19] Ibid.
[20] Irene Couzigou, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations', *International Review of Law, Computers & Technology* 32:1 37 – 57, (2018) at p. 42.
[21] Corfu Channel, supra note 1, at p. 18.
[22] United Nations Security Council Meeting 8330th, 'ISIL Now 'A Covert Global Network' Despite Significant Losses, United Nations Counter-Terrorism Head Tells Security Council', SC/13463 (23 August 2018).
[23] Wilson Center Online, 'Timeline: The Rise, Spread, and Fall of the Islamic State', (October 28, 2019). Available at https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state (accessed September 5, 2020).

terrorist operations occurring on or from its territories because it knew or should have known about the harmful conduct committed by ISIS. Because evidence of ISIS' harmful conduct is widely known, it would be incongruent for Syria to deny evidence of harmful terrorist operations occurring on or from its territories given that news of ISIS' operations is reported through official government channels and likewise through the media around the world.

The obligation to prevent transboundary harm thus requires states to have knowledge of ongoing OCTAs emerging from its territories via the monitoring of harmful activities in order to appropriately address any potential threats to peace.[24] In order for states to acquire knowledge they must, first of all, possess the appropriate mechanisms capable of preventing non-state actors from using their cyber infrastructure to commit OCTAs and second, states must be able to use such mechanisms diligently to prevent and suppress OCTAs emanating from within their territory.[25]

The first duty requires states to equip themselves with the appropriate means to detect, prevent, mitigate and punish OCTAs committed by terrorist groups within their territory that is contrary to the international legal rights of other states.[26] States are expected to have suitable tools within their means to adequately deal with the prospect of harmful OCTAs and this is arguably one approach to ensuring that the potential of violent behaviour can be minimised. Knowledge of an OCTA allows the state to take preventive action and to an extent, create conditions that might add positively to peace by reducing the likelihood of structural violence to take place within that state.

Possession of relevant apparatus to monitor and acquire knowledge of specific OCTAs differs depending on the cyber terrorist activity in question. Cyber terrorist recruitment might involve specialist task forces set up to monitor forum and chat rooms and that provide a reporting tool for online users to alert authorities of suspected terrorist recruitment activity. Task forces may also be responsible for conducting surveillance of possible terrorist recruitment campaigns taking place online through different social media platforms in order to obtain knowledge of terrorist recruitment. For cyber terrorist financing, anti-money laundering task forces might be implemented to monitor suspicious transactions, detect unlawful money movements and disrupt illicit flow of finances. In particular, states might possess the specific counterterrorism financing task forces that coordinate and cooperate with private financial institutions to monitor criminal activity related to cyber theft and

[24] Pulp Mills on the River Uruguay (hereinafter referred to as 'Argentina v. Uruguay'), Judgment, I.C.J. Reports 2010, p. 14, at para 197.
[25] Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', in *German Yearbook of International Law*, Vol. 35, edited by Jost Delbrück, and Rüdiger Wolfrum, Duncker & Humblot GmbH, 1992, Berlin Germany, at p. 26 – 27.
[26] Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law*, 21 (3), pp. 429 – 453 (2016), at p. 432.

cyber fraud. For states where funds are electronically directed to contribute towards operations in conflict zones, measures may be implemented to effectively monitor the movement and storing of these funds as a means to acquire knowledge and to combat terrorist financing. When it comes to cyber terrorist propaganda, which can be considered the most public of all three OCTAs, knowledge of its dissemination is widely visible on social media platforms. This said, acquiring knowledge of more substantive materials such as training and recruitment manuals, bomb-making guides and propaganda magazines must still be obtained through diligent monitoring mechanisms to inform states of OCTAs occurring on or from their territories. By requiring states to have the appropriate mechanisms in place to detect OCTAs, methods to acquire knowledge can be seen as a general promotion of positive peace as it relates to the obligation to prevent transboundary harm.

Whilst these measures are legitimate means of ensuring that states engage in the monitoring of activities that have the potential to affect the legal rights of other states, the question of its encroachment into civil liberties and human rights remains a matter of contention. Surveillance of civilian activity for the purposes of security is a widely debated issue in the face of counterterrorism measures. Though, it must be emphasised that the duty of due diligence applies only in relation to acts that are governed by international law. This is affirmed by the ICJ in Bosnian Genocide, which held that 'it is clear that every state may only act within the limits permitted by international law'.[27] The remits of state knowledge – what the state 'knew or ought to have known' – cannot then 'legitimise violations of international human rights or other rules'.[28] In this sense, states are expected to respect the right to privacy and to protect those rights, particularly in light of balancing their obligations under international human rights law with the obligation to prevent transboundary harm in relation to cyber terrorist activities.[29]

Determining whether the state has knowledge of OCTAs depends on the type of activity in question and the scale and extent of such operations. Where terrorist propaganda incites violence against a state's government, there is an expectation that the territorial state is aware or ought to be aware of this OCTA occurring on or from its cyber infrastructure because the propaganda is open and accessible to a global audience. Where a terrorist group is unlawfully collecting donations through what appears to be a legitimate charity, it is less reasonable to assume that states should know of the existence of this type of activity. This is because terrorist financing is clandestine, and terrorists go to

[27] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnian and Herzegovina v. Serbia and Montenegro) Judgment, I.C.J. Reports 2007, at para 430.
[28] Bannelier-Christakis, supra note 16, at p. 31.
[29] Whilst this thesis acknowledges the contention between the matter of international human rights law and its conflict with the duty for states to prevent harmful acts, it does not engage in depth with these issues as they fall outside the scope of this thesis. That said, the author suggests that such a discussion would make for an interesting and pertinent study which would add to the existing literature surrounding cyberterrorism.

great lengths to conceal their involvement. Repeat or continuous occurrences of OCTAs from a state's network can, however, serve as evidence that the state knew or should have known of the OCTA in question.[30] Moreover, the state is still expected to actively engage in knowledge seeking as part of its obligations under due diligence. In any event, if the state knew or should have known of OCTAs emanating from its territory, it is bound by an obligation to cease the continuation of such operations or at least, to mitigate its harmful effects in order to safeguard the international legal rights of other states.

3.2 Best Efforts

The second duty is for states to utilise the mechanisms within its capacity to address OCTAs. The possession of appropriate legal, judicial and administrative mechanisms does not automatically imply that states are to use such instruments diligently to acquire knowledge. The state may have a dedicated cyber task force in place to review financial reports of suspected terrorists. However, if the state does not review the relevant documents diligently and in a timely fashion, the state is not using its mechanisms appropriately and thus may not be able to acquire knowledge to prevent the OCTA before it causes harm.[31] At the same time, the state may detect suspicious activity that provides information of an ongoing terrorist recruitment campaign through fact-finding missions and it may choose not to act upon this information to prevent its territory being used to launch such operations. In such instance, the territorial state fails in its obligation to appropriately and reasonably take preventive measures to address the OCTA under the circumstances.

Since the states' enforcement of these laws is conditioned by the standard of due diligence, states are required to use their best efforts and do what is reasonable in the given circumstances to address the threat of OCTAs.[32] States have a choice of the best measures to take in order to stop the misuse of their territory for injurious cyber terrorist conduct under the given circumstances. For instance, to mitigate the harmful effects of cyber terrorist financing perpetuated through the illegal access into a government financial institution, the state can attempt to arrest the perpetrator of the terrorist financing and compel them to return the theft of funds, or the state can cease the funds and terminate the terrorist financing itself. It would be unreasonable, however, for the state to cease the funds if it meant doing so would require directing all its financial and technical resources at preventing this OCTA

[30] Couzigou, supra note 20, p. 43.
[31] *Corfu Channel*, supra note 1, at p. 22. The ICJ determined that 'Albania's obligation to notify shipping of the existence of mines in her waters depends on her having obtained knowledge of that fact in sufficient time…'.
[32] See Vincent-Joel Proulx, 'Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?', *Berkeley Journal of International Law*, Vol. 23:3, 2005, at p. 106 – 153, at p. 146. The author contends that 'obligations of prevention 'are usually construed as best efforts obligations, requiring states to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur'".

and leaving no such resources available to the authorities to engage in other areas of governance when it comes to the prevention of transboundary cyber harm. The state can only be expected to use what is available within its means to prevent the OCTA. If the state chooses not to put an end to the terrorist financing, it violates its obligations of due diligence to suppress the OCTA originating from its territory and affecting the legal rights of other states.

3.3 Technical Capacity of State

Technologically developed states are expected to do more to prevent or suppress OCTAs emanating from their territories than states with less technological capacity. This 'correlative increase' is significant when it comes to the prevention of terrorist activities in cyberspace, particularly because if a states cyber capability improves over time, the standard of due diligence will elevate in light of this development.[33] Equally, if a state's capabilities diminish, so will the standard of due diligence expected of it in performance of its obligations.

Technologically developed states have the material ability and allocated resources that can address and prevent incoming transboundary cyber harm. The UK, which prioritises cyber defence as a significant national security interest, has sophisticated mechanisms of deterrence that can guarantee a greater chance of successful defence in the face of transboundary cyber offensives. The same can be said of states such as Finland, Estonia, and the Netherlands, which have in place committed cyber defence strategies and protected networks leading to less reported cybercrime incidents.[34] On the contrary, some states in South-East Asia such as Vietnam and Cambodia, as well as African states such as The Democratic Republic of the Congo or Zimbabwe have less developed cyber capabilities. This is due to more pressing national security interests like civil unrest or ongoing poverty that take priority over ensuring good cyber hygiene.[35] For these states, there may be existing deficiencies in deterrence mechanisms or even a lack of, that can be used to hamper the efforts of terrorist groups.[36] Given this, states that have less economic resources available to cyber technology may not be capable of acquiring knowledge of OCTAs in the same manner as its neighbouring states, which have adequate resources dedicated to cyber deterrence.

---

[33] Buchan, supra note 26, at p. 445.

[34] International Telecommunication Union (ITU) Report, Global Cybersecurity Index (GCI), (2017) at p. 15. The report presents the leading countries based on their GCI score, demonstrating the highest commitment in all five pillars of the index to cybersecurity.

[35] Ibid.

[36] See Nicholas Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', *Journal of Conflict & Security Law*, 1-20, (2016). At p. 1, the author discusses failed states and the capacity for these territories to become *'*breeding grounds for non-state actors to pursue nefarious activities*.'*

The state, however, cannot evade responsibility by justifying inaction on the basis of limited technical capacity.[37] The moment the state becomes aware of an OCTA, the state must do all that is possible within their means to avert the harmful effects to the best of their abilities irrespective of their cyber capabilities.[38] Given this, the notable disparity between states cyber capabilities is not an obstacle to triggering obligations of due diligence. The expectation is not for the state to prevent the OCTA in absolute since 'the diligence that is due under the legal standard cannot exceed the state's capabilities.'[39] Instead, the state must try to minimise the harm as much as possible in the given circumstances. If the state cannot prevent the OCTA, at the very minimum, the state should notify and warn other states that are likely to be affected by the OCTA. This means cooperating with other states by sharing information of when the OCTA occurred, the nature of harm imposed and the different targets that might be affected as a means of mitigating the harmful effects of the OCTA where possible. The state must also utilise its resources to engage in investigative measures to determine the origins of the OCTA and to identify the individuals responsible in order to effectively prosecute and punish those involved. The state must take legislative and administrative practices, including prosecuting the violation of domestic laws surrounding the commission of OCTAs and cooperating with law enforcement agencies and private companies to share information and data as part of the investigative procedure.

Furthermore, where OCTAs originate from different territories, each state from where that terrorist activity emanates must contribute towards the mitigation of harm by engaging in due diligence obligations. Take, for example, an elaborate terrorist financing operation targeting several state-owned bank accounts that is located in multiple different states. Given the scale of this operation, it is difficult for one state to be able to prevent the harm. Each state that is involved must take all reasonable measures to contribute towards the mitigation of harmful effects, even if they cannot prevent the terrorist activity. States that do not have the technical resources to thwart the terrorist financing must, at the very least, notify and warn other states as well as cooperate where possible. For states that do have the technical capacity to prevent or mitigate the harm but decide to defer its communication of such information to other states, they can violate the obligation to notify and subsequently breach its obligations under the due diligence standard. Since the obligation is one

[37] Corfu Channel, supra note 1, at p. 18. The ICJ held that 'the state cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and its authors'.
[38] Bosnian and Herzegovina v. Serbia and Montenegro, supra note 27, at para 430.
[39] Michael Schmitt, 'In Defense of Due Diligence in Cyberspace', *Yale Law Forum* 68 (2015), at 74.

of conduct and not result, it is the paramount responsibility of the state to act when it has knowledge of its territory being used to commit harmful terrorist activities.[40]

3.4 Transit States

The obligation to prevent transboundary harm applies to OCTAs that are routed through the cyber infrastructure of another state. States must prevent their territory being used by terrorists to launch OCTAs and this obligation encompasses the prevention of harmful cyber activity travelling through its territory.[41] In certain cases, the same presumption of knowledge can be made that the state knew or should have known of the transiting OCTAs through its territorial cyber infrastructure. This includes where a transit state has experienced repeated or continuous OCTAs through cyber infrastructure belonging to its territory, which constitutes evidence that the transit state knew or should have known of the cyber terrorist operations.[42]

The notion that states must not allow its territory to be used for acts contrary to the rights of other states embodies the breach of an international obligation belonging to the target state. Thus, the obligation to prevent transboundary harm applies only in relation to an OCTA that, if committed by the territorial or transit state itself, would amount to an internationally wrongful act. In other words, the OCTA must be unlawful if committed by the territorial or transit state in order to impose an obligation on that state to prevent or cease the conduct.[43] Where a terrorist group is launching a cyber terrorist financing operation by rerouting its network through cyber infrastructure located on the territory of state A before it reaches state B, state A is bound by an obligation to try and put an end to the OCTA where it knew or should have known of the OCTA. Such an operation would violate the customary principle of non-intervention by encroaching into the domestic affairs of a state if it were perpetrated by the transit state and is therefore, unlawful.

It must be noted, however, that the obligation to prevent transboundary harm is more challenging to apply when it comes to transit states due to the clandestine nature of some OCTAs and the difficulty of tracing cyber activities. This matter is addressed by the Tallinn Manual 2.0, which recognises that knowledge of the transit state is difficult to establish when OCTAs are routed through privately owned Internet service providers (ISP), or possibly encrypted.[44] This said, the Experts nonetheless concluded that transit states still bear the same legal obligations as that of the territorial state. Thus, the transit

[40] Bosnian and Herzegovina v. Serbia and Montenegro, supra note 27, at para 438. The ICJ held that the state cannot 'do nothing' when its territory is being used to commit harm against other states.
[41] Nicaragua v. United States of America, supra note 9, at para 157.
[42] Couzigou, supra note 20, at p. 43.
[43] Nicaragua v. United States of America, supra note 9, at para 157.
[44] Tallinn Manual 2.0, supra note 4, at Rule 6 para 14.

state shoulders the due diligence obligation where it knew or should have known of an OCTA that meets the de minimis threshold, and where it can take reasonable measures to effectively terminate it.[45]

IV. Factors Affecting Exercise of Due Diligence in Cyberspace

As customary international law has established; states are subject to specific duties of prevention once they learn of OCTAs occurring on or from its territories. This includes the duty to notify and warn, the duty to cooperate and exchange information and the duty to investigate, prosecute and punish. Whilst due diligence is a positive obligation, it is assessed on an ex post facto basis to determine the state's compliance and responsibility with such duties.[46] As such, assessing states' due diligence relies on examining factors including the effectiveness of state control over its territory, predictability of harm and the international legal rights and interests the state is required to protect.[47]

4.1 Effectiveness of State Control

The degree of control the state exercises over its territory, which includes its cyber infrastructure, is an important factor to determine whether the state has acted with due diligence in response to OCTAs. The state must behave in a way to ensure it minimises the possibility of transboundary harm that results from OCTAs occurring under its jurisdiction and control that can affect the international legal rights of other states. For instance, if the state does not exercise effective control over its territory or any other area under its exclusive control, and where that territory is used for cyber terrorist recruitment affecting the rights of other states, the state is not responsible for the cyber terrorist recruitment itself, but for its failure to exercise due diligence to prevent terrorist recruitment within its jurisdiction. Rule 6 of the Tallinn Manual 2.0 asserts that control must belong to that of the government distinguishing it from a private entity.[48] In other words, the state must be in actual control of the cyber infrastructure used to launch harmful terrorist activities because it operates said infrastructure or that infrastructure is on territory, premises or objects it factually controls in order for obligations of due diligence to attach and trigger state responsibility. The more control the state has over its cyber infrastructure, the higher the state's responsibility to engage in measures of prevention to mitigate the harmful effects of OCTAs and in turn, to achieve peace.

As an obligation of conduct, the obligation to prevent transboundary harm requires the state to adopt appropriate mechanisms in order to enable the state to exercise effective control over its

[45] Ibid, at para 13.
[46] Ibid, at p. 7.
[47] Pisillo-Mazzeschi, supra note 25, at p. 44.
[48] Tallinn Manual 2.0, supra note 4, at Rule 6 para 10.

territory and subsequent cyber infrastructure.[49] It is a duty upon states to adopt laws prohibiting OCTAs and to establish institutions capable of detecting and punishing this activity. Where possible, states should enact specific legislation as well as establish particular administrative and judicial apparatus related to the prevention, prohibition, investigation and punishment of OCTAs emanating from or transiting through its territory. The obligation to prevent transboundary harm should also include the creation of counterterrorism mechanisms that are specialised in the detection of and reaction to OCTAs. Thus, the expectation of diligent state conduct involves the exercise of state control applicable to both public and private operators, where the monitoring of activities undertaken by such operators, are to safeguard the rights of other states in a way that can encourage the conditions for positive peace including by reducing the possibilities where violence can occur.[50] Though, the obligation to prevent transboundary harm cannot impose a burden on the state to implement mechanisms that would otherwise subject the state to exercise a degree of control that is beyond their capability. This would result in disproportionality for the state when it comes to fulfilling its duties under the due diligence standard. The degree of control exercised by the state is thus relative to its capacity to enforce control and subject to its technological capacity and available means.

Accordingly, where OCTAs are launched from the cyber infrastructure falling within the exclusive jurisdiction of a state, that state is expected to have greater responsibility to engage in duties of cooperation by sharing information and conducting investigations for the purposes of prosecuting and punishing those responsible for the terrorist activities than other states that would otherwise not have actual control of its infrastructure where that harmful conduct is launched. As such, states cannot hide behind the inadequacy of their legislative and administrative apparatus as grounds for their failure in preventing OCTAs.[51] Where the state fails to adopt reasonable measures to prevent or thwart OCTAs and where damage occurs in another state and potentially causes or exacerbates structural violence, the state is responsible for its failure to prevent OCTAs from occurring. If the state knowingly allowed OCTAs to be launched from cyber infrastructure under its exclusive control and failed to prevent such harm, its failure to comply with due diligence obligations can amount to an internationally wrongful act.

4.2 Likelihood of Harm

The state must determine the likelihood of harm posed by the OCTA. This is contingent upon whether the state can foresee the risk of harm posed by the OCTA in question. The level of due diligence

[49] Pisillo-Mazzeschi, supra note 25, at p. 26 – 27.
[50] Argentina v. Uruguay, supra note 24.
[51] Alabama Arbitration Case (United States of America v United Kingdom) (14 September 1872), Papers relating to Foreign Relations of the United States 1872 (United States Government Printing Office Washington 1873) part 2 Vol IV.

expected of the state is proportional to the likelihood of harm that the OCTA presents: the standard of due diligence is stricter for OCTAs that present a greater possibility of harm. This is particularly the case where the consequences of the harm are severe, and the state has the means at its disposal to prevent or minimise the risk of continued obstructions to achieving peace.[52] Since the obligation to prevent transboundary harm is triggered only when a specific harm occurs, there must be evidence linking the OCTA with an act of terrorism.[53] The foreseeability of ISIS causing harm is validated by the information received from the territorial state from where that OCTA is launched. The onus is on the state to act in response to this information and to mitigate the harmful effects both to the target state and to other states as much as possible in order to reduce the potential for structural violence to occur.[54] If the information obtained indicates a large-scale terrorist operation is underway then this would amount to sufficient evidence to indicate significant transboundary damage is likely and possibly indicate a progression from structural violence to that of direct violence. The larger the scale and extent of the OCTA, the greater the likelihood of harm requiring the state to act more diligently in response before it evolves even further to hampering peace in both concepts.

Yet, a difficulty with tackling OCTAs is accurately assessing the threat of the harmful conduct with any accuracy. When it comes to surveillance of those responsible for OCTAs, monitoring specific individuals online can be problematic due to the temporal nature of cyberspace. Online user accounts are often created with false credentials, which can easily be deleted and recreated, and this is often done numerous times to avoid any trace of the individual's authentic details from being detected. Terrorist groups often operate from numerous accounts to expand their reach and maximise the potential of connecting to and hiring of new recruits, to raise funds as well as to spread violent propaganda. In addition, there is the prevailing issue of terrorists communicating using encrypted messages, which prohibits access to communications due to their encoded security proving to be a serious hindrance to effective counterterrorism governance.[55] The challenges of establishing the likelihood of harm of OCTAs means measures of prevention, namely the duty to investigate, prosecute and punish can be more difficult to carry out when states cannot accurately define the likelihood of harm.

---

[52] Couzigou, supra note 20, at p. 48.
[53] Duncan French and Tim Stephens, ILA Study Group on Due Diligence in International Law, First Report, 7 March 2014, at p. 26. Due diligence requires states to take preventive action 'when they possess scientific evidence that significant transboundary damage is likely' or 'where there is insufficient evidence but where the consequences may be severe and irreversible'.
[54] Proulx, supra note 32, at p. 145 – 152.
[55] Dan Sabbagh, 'MI5 Chief Asks Tech Firms for 'Exceptional Access' to Encrypted Messages', *The Guardian Online*, 25 February 2020. Available at https://www.theguardian.com/uk-news/2020/feb/25/mi5-chief-asks-tech-firms-for-exceptional-access-to-encrypted-messages (accessed 25 Feb 2020).

4.3 International Legal Rights and Interests Requiring Protection

States are required to protect international legal rights and interests of other states, and the level of due diligence expected of the territorial state from where that OCTA emanates is determined on the significance of said rights and interests. The threat of an international legal right, namely sovereignty or the right to non-intervention, requires the state to act with a higher level of due diligence to protect that right than that of a legal interest.

When terrorist groups launch OCTAs from the territory of one state into another, there is serious potential for that OCTA to lead to a violent terrorist operation that could produce harmful effects and interfere with the legal rights and interests of other states. The state from where the harmful conduct is launched is expected to use its economic and technical resources to protect the legal rights of the target state to the extent that is feasible and practical under the circumstances. Upon acquiring knowledge of its cyber infrastructure being used to launch OCTAs, the territorial state must take reasonable measures in exercising diligence to prevent the violation of sovereignty against the target state. Since the degree of diligence required of states varies in accordance with the primary rule in question, what is considered to be reasonable in exercising diligence to prevent the violation of sovereignty will be more demanding than what is expected for the prevention of harm to property or financial interests.[56] Though, the violation of an international legal right must still meet the de minimis threshold and amount to more than a mere or minor convenience in order to trigger state responsibility.

Take for example ISIS gaining access into the UK's BBC website to disseminate propaganda by uploading beheading videos of hostages. Such videos contain serious levels of violence that intend to shock or disgust viewers, as well as encourage others to commit violent acts, constituting an incitement of terrorism. Since the BBC is a state-owned enterprise of the UK that broadcasts public services, it is in the interests of the territorial state to protect the UK's sovereignty, an international legal right that requires a high level of protection. When the state from where ISIS is launching its operations becomes aware of such harmful conduct emanating from its territory, it is under a duty to notify and warn the UK at the very minimum. The territorial state is expected to cooperate with the UK by sharing relevant information it has acquired through investigations into the ISIS operation including when the operation was launched, what part of the BBC's network faced intrusion, and the nature of the videos that surfaced on the BBC's website and so forth. The degree of due diligence expected of the territorial state to perform its obligations is particularly high where the potential for

[56] Bosnian and Herzegovina v. Serbia and Montenegro, supra note 27, p. 43.

a violation of international law is concerned. Since protection of an international legal right is paramount, the harmful effects of the terrorist activity must be minimised in order for the safeguarding of the victim state's sovereignty.

At the same time, harm to property or financial interests, which are also legal interests, can violate sovereignty and amount to a breach of international law. If ISIS launches a terrorist financing operation targeting a state's financial institutions, the target state's sovereignty as well as its financial interests are subject to harm. The financial institutions, however, do not have to belong to the state. Private entities that are appointed to manage financial interests of the state will equally be summoned by the state to take necessary action to prevent and terminate harmful cyber conduct as a means of protecting the legal rights and interests of the target state. By its failure to prevent injurious cyber activities emanating from cyber infrastructure under its exclusive control, it is the territorial state from where that financing operation is launched that violates the sovereignty of the target state. Thus, where the violation of sovereignty is a result of harm to financial interests belonging to a state, it is reasonable to expect that the territorial state exercises a high level of due diligence to prevent such harmful cyber activities from threatening the international legal rights and interests of the state in question.

V. Obligation to Prevent Transboundary Harm in Relation to OCTAs

In the face of OCTAs, the state is under a legal obligation to engage in specific measures that enable it to prevent or at the very least mitigate its harmful effects. The following section explores this obligation in relation to each OCTA.

5.1 Cyber Terrorist Recruitment

Terrorist recruitment campaigns typically take place through online chat rooms and forums. The state may acquire knowledge through implementing cyber task forces responsible for detecting pro-terrorist dialogue among these platforms. The state may also possess the mechanisms capable of automatically detecting cyber recruitment through language processing and learning techniques to filter recruitment related posts.[57] This would enable the state to analyse large datasets of suspected posts related to terrorist recruitment activities in an attempt to identify the user accounts and to determine the origins of these recruitment efforts. Indeed, the extent to which a state can engage in measures to acquire knowledge is contingent upon its technical capacity and the type of legal and administrative mechanisms it has in place to accomplish such. If the state is known to frequently have

[57] See e.g. Jacob R. Scanlon and Matthew S. Gerber, 'Automatic Detection of Cyber-Recruitment by Violent Extremists', *Security Informatics*, 3:5 (2014).

cyber terrorist recruitment campaigns occurring on its territory or transiting through its cyber infrastructure, then it will be held responsible for what it should have known of the recruitment. For instance, if a technologically advanced state is informed by its authorities that there are several online user accounts suspected of terrorist recruitment and such accounts are emanating from IP addresses located on its territories, it is reasonable to expect that the territorial state would block those IP addresses.

Diligent conduct involves the state making reasonable efforts to inform itself of activities of cyber terrorist recruitment and their links to prospective acts of terrorism so that structural violence can be minimised. The obligation to prevent transboundary harm is triggered on the basis that the cyber terrorist recruitment can be linked to a prospective terrorist operation requiring the state to act in response to this information. To give an example, the territorial state is aware of ISIS launching a global recruitment operation targeting numerous online chat rooms, forums and social media sites to recruit young people as foreign terrorist fighters in Syria and Iraq. The state can foresee that the magnitude of this harm is serious and significant because social media posts are calling for recruits to join the conflict in Syria and Iraq. Given this, the state should anticipate the terrorist recruitment as presenting a serious likelihood of harm, and therefore, the state must minimise the risk of such harm from affecting the rights of other states and which could possibly lead to acts of more serious and sinister terrorist violence. Among the measures of prevention, the state is able to notify and warn other states that may be affected by the cyber terrorist recruitment. From intelligence gathered by counterterrorism units, the state is also able to share information with other states to inform them of the different online chat room sites and forums that must be taken down to prevent further communication. However, when it comes to detecting those responsible, encrypted messages used between recruiters and the recruited can hinder access to vital evidence, hampering the overall investigative process. The state cannot accurately determine the identities behind the encrypted messages to prosecute and punish those responsible nor can it accurately characterise the level of harm. This, however, does not undermine the state's effort to fulfil its obligations under the due diligence standard if it attempts to reduce the potential for violence to occur. As long as the state uses its best efforts to engage in measures that are reasonable under the given circumstances, that is sufficient to discharge itself of obligations under the primary rule, even if the state cannot investigate, prosecute and punish those responsible.

Another possible scenario is that the state has knowledge of cyber terrorist recruitment, but that it may not foresee the OCTA linking to a prospective terrorist attack. This may well be the case if terrorist groups do not disseminate propaganda indicating any prospective plans of a terrorist attack

to cause the maximum destructive impact on its targets. This would otherwise be an act of direct violence and threaten negative peace. Though this is possible, the state is still only expected to do what is reasonable under the circumstances in order to discharge itself of obligations of due diligence by minimising the potential of violence materialising to cause either structural violence or direct violence. This means that if the cyber terrorist recruitment is already underway, the state is expected to suspend the user accounts engaging in recruitment tactics without delay and accomplishing such might involve working with private companies to do so. States that do not have the technical means to act are, at the minimum, expected to inform and warn other states that may be affected by the terrorist recruitment. The ultimate objective is to reduce violence by striving towards peace and efforts to demonstrate doing so must meet a bare minimum standard that shows the state's willingness to engage in preventative measures. For example, if the state is aware that its cyber infrastructure is being used for covert terrorist recruitment because monitoring reports have indicated so and various other states are also affected, the territorial state must notify and warn those states so they can act upon this information to prevent the violation of sovereignty for these states. Unless there is evidence to show that the territorial state should have known of a prospective terrorist attack linked to the cyber terrorist recruitment and that it failed to acquire knowledge of such under reasonable circumstances, the state otherwise fulfils its obligations under the due diligence standard.

5.2 Cyber Terrorist Financing

As the most sophisticated OCTA, terrorist financing can typically require technical expertise to conduct operations such as gaining illegal access into data systems, intruding into protected networks and laundering money through illicit means. Cyber terrorist financing can be conducted both openly and publicly but also through clandestine means. Where terrorist groups operate behind false charities to publicly collect funds from donors and to launder monies and where this type of activity occurs frequently from the territorial state or transits through the state, the state might know or should be expected to know of such illegal activities. If the state has appropriate counterterrorism financing task forces in place to detect and deter such activity, it should be made aware of financing activities by its own agencies, having a higher expectation to acquire knowledge of this activity.

Take, for instance, that ISIS are illegally collecting funds by using false charities as a front to deceive authorities and to launder money for terrorist purposes.[58] The state becomes aware of ISIS engaging in terrorist financing through the use of monitoring mechanisms that detail fraudulent activity, from gathering data produced by task forces and by analysing intelligence reports of Financial Intelligence

[58] See Martin Rudner, '"Electronic Jihad": The Internet as Al-Qaeda's Catalyst for Global Terror', *Studies in Conflict and Terrorism*, 40(1):1-14, 2016.

Units. The territorial state has the necessary information to foresee that the risk of ISIS causing harm is likely and thus, requires preventive action. If the state has the appropriate resources to mitigate the harmful effects, such as effective counterterrorism finance regimes that allow authorities to enforce legislation and cease the terrorist financing, the state has the capacity to act and must do so to preserve the peace positively. If the state does not have the technical capacity to prevent the terrorist financing because it lacks such resources the state must, at a minimum, notify and warn other states of the cyber terrorist financing.

On the other hand, where terrorist groups conduct covert financing operations under the guise of operating as religious groups, community interests or small personal businesses for instance, knowledge is more difficult to acquire because detection of such activities is intentionally obfuscated. Contingent upon its technical capacity, the state must have in place measures to protect vulnerable sectors such as charities, targeted financial sanctions against known cyber terrorists and effective reporting of suspicious activities among inter-agencies as measures of prevention. Whilst the state is not expected to acquire absolute knowledge of all that occurs on its territories, efforts to inform itself of cyber terrorist financing include ensuring record-keeping, diligent reviewing of non-profit organisations, and the freezing and confiscating of laundered property.[59] All such measures contribute to the overall objective of ensuring positive peace can be maintained and to mitigate any potential for negative peace to be disrupted. In other words, the state must make an effort to reduce structural violence caused by OCTAs and to ensure that they do not progress to becoming acts of direct violence in the form of terrorist conflict.

The state cannot, however, hide behind the clandestine nature of cyber terrorist financing to justify inaction. This might include a terrorist organisation operating clandestinely behind a number of charities to raise funds publicly for charitable causes of which these funds are then diverted away from the charity and used for criminal and terrorism purposes. It may also be the case that charity funds are moved to different locations through different currencies in order to be diverted before reaching a terrorist organisation. Equally, a group of charities may be established to appear legitimate but instead used to launder money for terrorist purposes. These scenarios are exemplar of terrorists operating behind charities to manage large scale terrorist financing operations that can pose a serious level of harm. This is particularly problematic because online charities are extremely resilient. Exposed charities might be removed one day with the same bogus charity websites operating under an entirely new alias being set up the next day.[60] If the state from where those operations emanate possesses

[59] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*, FATF, Paris, France (2012 - 2019).
[60] See Michael Jacobson, 'Terrorist Financing and the Internet', *Studies in Conflict & Terrorism,* 33:4, 353-363, 2010.

knowledge of such operations that significant transboundary harm is likely, then due diligence requires states to take preventive action before the harm perpetuates.

The standard of due diligence further increases if the cyber terrorist financing can be shown to link directly to an orchestrated terrorist operation. If the state has knowledge of the OCTA and it is made aware of a forthcoming terrorist attack, particularly where the state is capable, the diligence expected of it is elevated. The state must take measures to reduce terrorist violence where possible and to encourage peace through positive means in order to protect other states against such violence. Take, for example, that the state is alerted by counterterrorism financing task forces indicating that funds were procured from donations of followers who believed their money would be defending oppression against illegitimately occupied lands in conflict zones of Syria and Iraq. The terrorist group is known to authorities because there are previous links for their involvement in the Syrian conflict, and intelligence indicates that the group are using the funds to organise members to travel to conflict zones. Given this information, the state can foresee a high likelihood of harm because the terrorist group is illegitimately acquiring funds to support foreign terrorist fighters in conflict zones. Not least does the territorial state have to act to protect the sovereign integrity of Syria, it must also protect the financial interests of the deceived donors particularly where the financing is enabling the commission of other OCTAs. In response, the state should attempt to cease the transfer of funds by interception and enforce targeted financial sanctions against the identified terrorists, where possible. The state should also notify and warn Syria of the prospective harm, sharing and exchanging the information available to it in order to mitigate the harmful effects as much as possible. The state must act to prevent the harm from occurring and/or continuing and affecting the rights of Syria and possibly of other states. Furthermore, since Syria is known as a safe-haven territory for ISIS, the expectation for Syria to respond to knowledge of OCTAs is higher than that of other states where they are not expected to know of such terrorist operations manifesting on their territories.[61]

On the contrary, if the territory of a less technically developed state is being used to launch a cyber terrorist financing operation, the diligence expected of it is reduced because of its limited capability to address the threat. For instance, the state is informed by open-source intelligence that a propaganda website hosted by ISIS is being used to solicit donations via bitcoin from its cyber infrastructure. Research indicates that various donations have been made to the bitcoin address. However, the identification of these transactions is prohibited due to the encrypted nature of using

[61] Wesley Morgan, 'Pentagon Sees Few Options for Preventing New ISIS Safe Haven in Syria', *Politico Online* ,19 October 2019. Available at https://www.politico.com/news/2019/10/19/pentagon-isis-syria-051369 (accessed 23 September 2020); Charles Lister, 'The Growing Threat of ISIS in Syria's Badia', *Middle Eastern Institute*, 17 April 2020. Available at https://www.mei.edu/publications/growing-threat-isis-syrias-badia (accessed 23 September 2020).

cryptocurrencies and the fact that the territorial state does not have the resources in place to investigate these transactions. In response, the state is expected to block and remove the site hosted by ISIS. However, it would be unreasonable to expect the state to dedicate all its available resources at investigating the bitcoin transactions if that meant the capacity for the state to act in response to other matters of national security interests would be compromised in doing so. The state cannot be expected to perform its obligations of due diligence in the same manner as a technologically advanced state with sufficient mechanisms in place to deter and detect the cyber terrorist financing, especially if the outcome would be disproportionate to the risk.

5.3 Cyber Terrorist Propaganda

Despite propaganda being the most widespread and common OCTA, the obligation to prevent transboundary harm applies only to materials containing incitement and encouragement of violent terrorism because they can, if committed by a state, constitute a violation of international law. Acquiring knowledge of such can be constructed from measures to identify propaganda materials through automated content detection, content analysis and self-reporting tools online. Since there is a vast array of terrorist materials surfacing online that pertain to different purposes, it would be impossible for states to remove all terrorist propaganda online. Instead, states are only required to prevent propaganda where they acquire evidence that such content encourages violent behaviour and incites political violence for the purposes of terrorism, with the possibility of causing serious harm. The more extreme the terrorist ideology that is portrayed in the message and the more violence that appears in the propaganda, the more serious and significant the harm posed by the terrorist material.

For instance, in their monthly publication of Rumiyah, ISIS encourages radical supporters and members located in the West to carry out knife attacks, arson attacks, theft, truck attacks and hostage takings.[62] The territorial state where Rumiyah is launched, and subsequently those states where the propaganda is circulated, are under a duty to act diligently to prevent the propaganda from being further disseminated online and potentially causing harm to other states. Not least does propaganda contain incitement to terrorism, it has the potential to instigate more serious and violent acts of terrorism because it perpetuates aspects of a culture that can be used to legitimise structural violence. The state must take preventive measures including shutting down host websites and removing other types propaganda such as social media posts or Tweets related to the specific incitement found in the Rumiyah publication. The state must also share knowledge of this propaganda incitement with other states where that material might be shared and where possible, investigate the origins of the

[62] Tyler Welch, 'Theology, Heroism, Justice, and Fear: An Analysis of ISIS Propaganda Magazines Dabiq and Rumiyah', *Dynamics of Asymmetric Conflict*, 11:3, 186 – 198, at p. 193 – 194.

propaganda and from what domain the content is being launched. The expectation is for the state to engage in all measures of prevention at its disposal. If it has the technical capacity to do so, the state must act with immediacy to minimize the risk of an ensuing terrorist attack by suppressing all forms of propaganda related to ISIS' incitement of terrorism at that time.

For technologically advanced states, the suppression of terrorist propaganda that contains incitement involves the diligent removal of such content and where possible, tracing the origins of that material to its original source. In particular, where the state has knowledge over a prospective terrorist operation or where that state is known for its territory to be used to launch terrorist operations, the state is expected to know of specific cyber terrorist propaganda inciting political violence. This is because the state should have in place internet referral units, counterterrorism task forces and relevant authorities and agencies to monitor, detect and deter such materials from perpetuating on or from its territory and to appropriately utilise such mechanisms for prevention. If the state becomes aware of terrorist videos that glorify suicide bombings being circulated online and authorities detect such materials originating from its own cyber infrastructure, the territorial state is required to remove the video as soon as possible. Such content encourages acts of terrorist violence and has the possibility of impeding the achievement of peace in both concepts. It might also be responsible for tracing the circulation of the video and engaging in inter-agency cooperation to notify and warn other states where that video may have been shared. The state is equally expected to engage in measures of prevention if it became aware of a propaganda website hosting beheading videos, a video game designed for children encouraging violence through the use of weapons, Facebook or Twitter posts declaring war on ISIS opposition, or bomb making guides for instance. If states have limited technical capacity to engage in investigate measures after the removal of content, the expectation is that they have at the minimum, notified and warned other affected states where possible.

Where the terrorist propaganda is surfacing online but the state cannot establish a link with the material and a prospective terrorist operation, the state must exercise discretion as to its removal from online sources. Given that terrorist propaganda is widespread, the expectation is for the state to diligently monitor propaganda and to effectively distinguish those materials that present a greater likelihood of harm as necessary of removal. It would seem incongruent for the state to allow a website hosting suicide bombing videos to remain online, even though the videos are not directly linked to a prospective terrorist attack. Terrorist materials of this nature encourage violence and allows for those exposed to it to be subject to violence in the structure of their society. The plausibility of such materials to provide encouragement for terrorist violence remains a national security interest, even

if the state is unaware of a prospective terrorist operation. The same can be said of bomb-making materials or recruitment manuals, which provide terrorist groups with the knowledge and competence to commit acts of terrorist violence. Whilst a number of terrorist materials have been made unavailable over the last few years (including some that were used during this research),[63] there remain bomb making materials, recruitment guides and both ISIS magazines Dabiq and Rumiyah that can still be accessed by ISIS supporters and terrorist members online as recent as 2021.[64] Furthermore, in 2020, a digital library with over 90,000 items of ISIS terrorist material was discovered, including materials on how to plan and carry out an attack and content supporting individuals to become better terrorists.[65] Whilst deterrence of online propaganda will always be difficult due to the dissemination of materials across a decentralised system, states must not be complacent in their efforts to prohibit the incitement of political violence, particularly given its continued abundance. Accepting this, the importance of prohibiting such materials through the obligation to prevent transboundary harm is an invaluable legal mechanism for states in the fight against terrorism.

There is no question that the removal of all materials that incite terrorist violence from online websites is a difficult and piecemeal task. Nonetheless, it remains centrally important that states, in corporation with private internet companies and service providers, make a continued and concerted effort to eliminate dangerous pages from search engines and take down terrorist material surfacing on different websites as soon as it either knew or should have known of such. Where websites are hosted in foreign territories, the need for diligent conduct of states to notify and warn affected states from having its cyber infrastructure being used to launch terrorist materials is paramount when it comes to discharging its duties under the obligation to prevent transboundary harm. Whilst ISIS propaganda may have deteriorated in the face of territorial losses, bomb-making guides and propaganda magazines are increasingly being sought after, particularly as a result of the COVID-19 pandemic.[66] Accepting this, states must remain vigilant in the detection and deterrence of cyber terrorist propaganda. States must fulfil its duties under the obligation to prevent transboundary harm

[63] For example, some ISIS magazines under the name Inspire are no longer accessible online as of July 2018.
[64] Counter Extremism Project, 'Infamous ISIS Bomb-Making Video Located on Several Sites', April 17, 2019. Available at https://www.counterextremism.com/blog/infamous-isis-bomb-making-video-located-several-sites (accessed 16 September 2020); Abu Amru Al Qa'idy, 'A Course in the Art of Recruiting – Revised July2010' available at https://archive.org/stream/ACourseInTheArtOfRecruiting-RevisedJuly2010/A_Course_in_the_Art_of_Recruiting_-_Revised_July2010_djvu.txt (accessed 11 January 2021); Dabiq, 1437 Safar, 'Terror', Issue 12 at p. 43. Available at http://clarionproject.org/wp-content/uploads/islamic-state-isis-isil-dabiq-magazine-issue-12-just-terror.pdf (accessed 11 January 2021); Rumiyah, Issue 2, Muharram 1438. Available at http://clarionproject.org/wp-content/uploads/Rumiyh-ISIS-Magazine-2nd-issue.pdf (accessed 16 February 2017).
[65] Shiroma Silva, 'Islamic States: Giant Library of Group's Online Propaganda Discovered', *BBC News*, 3 September 2020. Available at https://www.bbc.co.uk/news/technology-54011034 (accessed 3 September, 2020).
[66] Mia Bloom, 'How Terrorist Groups Will Try to Capitalise on the Coronavirus Crisis', *Just Security*, 3 April 2020. Available at https://www.justsecurity.org/69508/how-terrorist-groups-will-try-to-capitalize-on-the-coronavirus-crisis/ (accessed 16 September 2020).

as a means of safeguarding its territory and the rights of other states in the face of OCTAs and to strive towards the achievement of both negative and positive peace.

VI. Conclusion

The obligation to prevent transboundary harm applies to certain OCTAs. Where a terrorist group launches an OCTA which, if committed by a state would amount to an internationally wrongful act and where that OCTA gives rise to sufficiently serious consequences, the territorial state is in principle under an obligation to prevent the OCTA in question. However, the obligation to prevent transboundary harm is triggered only where the state knows or ought to have known that the OCTA was or is emanating from the cyber infrastructure located within its territory. Moreover, the expectation of the state is to engage in measures of prevention based on what is reasonable in the given circumstances. Furthermore, the more resources the state has, the greater the expectation of the state to notify and warn, to cooperate and exchange information and to investigate, prosecute and punish those responsible for the OCTA. Only when the state has shown it has acted diligently to prevent or terminate the OCTA using the means available to it will the state discharge itself of its duties under the obligation to prevent transboundary harm.

This chapter has shown that the obligation to prevent transboundary harm can be used to prevent and suppress OCTAs and to a certain extent this rule of customary international law compensates for the gaps left by treaty law. This said, as an obligation of due diligence, the obligation to prevent transboundary harm does not impose an obligation of result on states. In other words, states are not required to prevent all OCTAs emanating from their cyber infrastructure. Instead, they must only make reasonable efforts to prevent and suppress OCTAs that are international wrongful acts and that violate international law. It can be said then that the obligation to prevent transboundary harm has some, albeit limited, application to the regulation of OCTAs. Therefore, this chapter has found that it remains necessary for international law to continue to engage proactively in measures to ensure the prohibition of OCTAs can secure international peace and security.

CONCLUSION

I. Introduction

This research has sought to explore whether current international law is adequate at addressing OCTAs, that is, cyber terrorist recruitment, financing and propaganda activities. This thesis began by providing the definitions to terrorism, cyberterrorism and OCTAs. Then, this thesis provided the contextual background by situating OCTAs within the framework of international peace and security through the theory of negative and positive peace. It proceeded to examine whether current international law in the form of regional treaties and conventions and UN resolutions could be understood to apply to OCTAs regarding their prevention and suppression. This thesis has found that while provisions of international law are stronger than initially thought, existing legal frameworks remain insufficient at providing adequate protection for states against OCTAs. As a result, this thesis has argued that, to an extent, the obligation upon states to prevent transboundary harm under customary international law can be used constructively to prevent and suppress international terrorism and especially terrorists' use of cyberspace for the purposes of OCTAs.

The thesis concludes with an overview of the arguments through its chapter breakdown regarding how OCTAs are addressed under international law and whether the obligation to prevent transboundary harm applies to OCTAs. Then, the conclusion emphasises the core findings of the thesis by addressing the contributions made by the research and discussing what the analysis has shown. Finally, this thesis suggests future areas for research.

II. Overview of Chapters

Since the rise of ISIS' and its growing social media campaign in 2014, the international community, the United Nations and international law scholars alike have been emphasising on the threat and dangers posed by violent terrorist attacks conducted both in cyberspace and on the ground.[1] There has been, however, insufficient attention paid to the operational cyber terrorist activities that facilitate, enable and catalyse these atrocious acts of terrorist violence, otherwise known as OCTAs.[2] This research has endeavoured to elevate the discourse surrounding OCTAs by demonstrating their role in the

[1] United Nations Security Council Resolution 1368, S/RES/1368 of September 12, 2001; Gabriel Weimann, *Terrorism in Cyberspace; The Next Generation*, (Columbia University Press, 2015); Imran Awan, 'Cyber Extremism: ISIS and the Power of Social Media', *Social Science and Public Policy* 54: 138 – 149 (2017); Susan Brenner, 'Cyberterrorism: How Real is the Threat?', *Media Asia*, 29:3, 149 -154 (2002); Martin Rudner, '"Electronic Jihad": The internet as Al-Qaeda's Catalyst for Global Terror'*, Studies in Conflict and Terrorism*, (2016).

[2] International Law Association (ILA), Study Group on Cybersecurity, Terrorism and International Law, Study Group Report (July 31, 2016).

commission of violent terrorism and to explore the extent to which they are prevented and suppressed by international law.

Chapter 1 set the parameters of this thesis by providing the definitions behind the core elements of terrorism, cyberterrorism and OCTAs. Based on these interpretations, OCTAs can be understood as terrorists' use of cyberspace for the purposes of recruitment, financing and propaganda activities. This thesis distinguished between two types of OCTAs; OCTAs that are integral to terrorism, and OCTAs that fall within the wider general definition of terrorism. In doing so, this thesis aimed to redefine the discourse surrounding cyberterrorism by drawing attention to the prevalence of OCTAs in all forms in order to better counter international terrorism and to ensure international peace and security.

The primary aim of the international legal system is to achieve and maintain international peace and security. However, terrorism and the advent of cyberterrorism, specifically in the form of OCTAs, has significantly endangered the achievement of these aims. In light of this, Chapter 2 has situated OCTAs within the theoretical framework of Johan Galtung's peace concept and has recognised that such activities are obstructions to achieving both negative and positive peace.[3] Although direct violence is no longer a prevailing threat to peace, an exploration into OCTAs determined that they are more than capable of providing the conditions for direct violence to materialise and equally, hinder the creation of positive peace. OCTAs encourage and perpetuate violent behaviour and they have a serious and dangerous potential to lead to direct violence between states. OCTAs also pave the way for structural violence to materialise within the state, where its manifestation allows for aspects of a culture that can be used to legitimise structural violence. This then has the potential to cause conflict between interstate relations and impede development of the full potential of individuals who are subject to such violence. In short, Chapter 2 argued that OCTAs enable terrorist groups to carry out acts of violent terrorism, and thereby hinder the achievement of international peace and security.

The chapter continued to discuss the significance of international law in preventing OCTAs within the framework of international peace and security. International law governs the way in which states behave through rules of international law. The chapter thus highlighted the importance of implementing rules as a means of maintaining a functioning legal order and therefore, peace and security. The discussion emphasised that the international legal system provides states with an instrument for implementing common policies aimed at achieving community objectives, particularly relating to peace and security. In turn, this allows international law to function as a tool of governance through the enforcement of treaty law, customary law and legal instruments in the form of UN

[3] Johan Galtung, 'Violence, Peace and Peace Research', 6 *Journal of Peace Research* (1969).

resolutions. The chapter accentuated the role and significance of law as paramount to achieving normative values and an effective means by which states can secure international peace and security. Based on this, Chapter 2 also presented OCTAs as a threat to international law's regulatory framework and aims and thus, require prevention under international law.

Given there is no international or domestic law pertaining specifically to OCTAs, Chapters 3 and 4 turned to an analysis of the existing law surrounding cyberterrorism, including an examination of legislation in the form of international and regional treaties and UN resolutions.

Chapter 3 examined three different regional treaties relating to cybercrime and cybersecurity: the Convention on Cybercrime (2001),[4] the African Union Convention on Cybersecurity and Personal Data Protection (2014)[5] and the Arab Convention on Combating Information Technology Offences (2010).[6] This included reviewing additional documents in the form of a Guidance Note and an Explanatory Report attached to the Convention on Cybercrime to further understand whether the prohibition of OCTAs could be construed from such instruments.[7] In particular, the analysis provided a literal reading of specific provisions relating to cyber offences committed by terrorists using the general rule of interpretation under Article 31 VCLT 1969.[8] Applying this method of interpretation was important because it allowed for a consistent reading of treaty provisions to determine whether they could be construed to apply to OCTAs.

This examination revealed that the Convention on Cybercrime and the African Union Convention mostly prohibit acts of cyberterrorism committed through the use of computer systems including fraud, hacking and phishing offences.[9] Both treaties are restricted to offences that are cyber dependent and require a high level of computer proficiency such as data interference or impairment to a computer system. Because the African Union Convention was drafted by reference to the Convention on Cybercrime, the prohibited offences in both treaties were similar. Cyber offences were criminalised only if they could be shown to result in tangible consequences. As a result, neither of these treaties could be interpreted to apply to OCTAs that did not produce a level of harm in the form of damage to either a computer system or computer data. While the Convention on Cybercrime stipulates against the use of cyberspace and cyber infrastructure for cyber terrorist attacks, Guidance Note 11 hypothesizes through examples that could produce structural violence and thus, the

[4] Council of Europe, Convention on Cybercrime, ETS No. 185 (November 23, 2001).
[5] The African Union Convention on Cybersecurity and Personal Data Protection (2014).
[6] The Arab Convention on Combating Information Technology Offences (2010).
[7] Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189 (Strasbourg, 28.I.2003); Council of Europe, T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention, (November 15, 2016).
[8] Article 31 (1) of the Vienna Convention on the Law of Treaties 1969
[9] Article 29 (2) of the African Union Convention on Cyber Security and Personal Data Protection (2014).

Convention could be said to have normative value that strives towards peace in both its negative and positive concepts.

By contrast, the analysis showed that the Arab Convention was the most applicable treaty to OCTAs, with a dedicated provision criminalising the use of technology for the purposes of terrorism. Under Article 15(2), the Arab Convention made it an offence to engage in the financing of and training for terrorist operations as well as facilitating communication between terrorist organisations.[10] This is a significant provision since the Arab Convention recognises terrorists' use of cyber technology to engage in certain terrorist activities and prohibits such activities within the scope of its application. Given this, the Arab Convention made a concerted effort to strive towards achieving positive peace by explicitly prohibiting such threats. This being said, only states in the Arab region that are party to the Convention are subject to the provisions therein and the prohibition does not extend beyond these states. Whilst the Arab Convention was exemplar of the type of legislation needed to prevent such activities, a treaty with the necessary provisions relating to the prohibition of OCTAs remains yet to be seen. With this in mind, Chapter 3 concluded that existing regional treaties had insufficient application to OCTAs and lacked relevant provisions relating to cyber terrorist recruitment, financing and propaganda activities.

Chapter 4 continued to explore the applicability of existing legislation to OCTAs through UN resolutions and related documents adopted by the Security Council and the General Assembly as it pertains to the actions of ISIS. As discussed throughout the chapter, their terrorist activities and violent acts of terrorism have been addressed in a number of resolutions, meetings and reports relating to the threat they present regarding the maintenance of international peace and security.[11] The adoption of Security Council resolutions demonstrated the recognition of ISIS using technology to commit terrorist acts and condemns the group for carrying out violent terrorist attacks.[12] In various instruments, the Security Council identified ISIS' use of cyberspace and cyber technology for the purposes of terrorist recruitment, financing and propaganda activities, among others. By acknowledging this, the Security Council understood that these activities are essential to the functioning of the terrorist group and provide sustenance to the group to further perpetuate acts of violent terrorism.

[10] Article 15 (2) of the Arab Convention on Combating Information Technology Offences (2010).
[11] United Nations Security Council Resolution 2322, S/RES/2322 of 12 December 2016.
[12] See for example S/PRST/2013/1 Statement by the President of the Security Council of 15 January 2013; United Nation Security Council Resolution 2133, S/RES/2133 of 27 January 2014; United Nations Security Council Resolution 2249, S/RES/2499 of 20 November 2015.

Importantly, however, the nature of resolutions adopted by the Security Council in response to ISIS' actions reflected the significance of its approach to preventing OCTAs. As such, this chapter made an important distinction between executive and legislative resolutions as well as the use of binding and non-binding language to determine whether such legal instruments impose obligations on states in relation to OCTAs. This analysis revealed that the Security Council's executive resolutions indeed recognised OCTAs and encouraged the need for states to address such activities as part of their efforts to counter terrorism. The condemnation of terrorist recruitment, financing and propaganda appeared in several Security Council resolutions as well as meetings and reports. The Council's recognition of OCTAs perpetuating violent behaviour affirmed its normative approach to preventing terrorism by striving towards peace. At the same time, the discussion found that there lacks a series of resolutions that impose binding obligations on states to specifically prohibit OCTAs. When it comes to measures to address OCTAs, the language used by the Security Council was found to be non-binding. Instead of 'deciding' or 'calling' on member states to prohibit OCTAs, the Security Council 'encourages' and 'expresses concern' at the increasing use of cyberspace for the purposes of OCTAs. In this case then, it can be said that the prohibition of OCTAs is not a mandatory responsibility for states and in fact, the Security Council considers OCTAs to be subsidiary activities that are less significant than terrorist attacks, despite being continually executed by ISIS.

That said, there are related Security Council resolutions that are binding with legislative effect. Resolutions 1373 (2001) and 1540 (2004) have legally binding effects and impose legal obligations on states in a general and abstract manner.[13] In particular, by condemning 'any act' of international terrorism as a threat to international peace and security, Resolution 1373 could be construed to apply to OCTAs.[14] However, its overly broad nature and the lack of explicit obligations relating to cyber terrorist recruitment, financing and propaganda left ample room to doubt whether states would willingly adhere to Resolution 1373 when it comes to prohibiting OCTAs. Thus, there remains creative ambiguity over the scope of its application and it is particularly uncertain whether Resolution 1373 can be interpreted to explicitly apply to OCTAs.

Furthermore, much like the instruments of the Security Council, efforts of the General Assembly revealed an acute understanding of the prevalence of OCTAs and their essential role in furthering and materialising terrorism.[15] However, the recommendatory nature of General Assembly resolutions limits their applicability and their effect as measures that can be adopted to enforce the prevention

[13] United Nations Security Council Resolution 1373, S/RES/1373 of 28 September 2001; United Nations Security Council Resolution 1540, S/RES/1540 of 28 April 2004.
[14] Ibid.
[15] United Nations General Assembly Resolution 60/288, A/RES/60/288 of 8 September 2006; United Nations General Assembly Resolution 68/276, A/RES/68/276 of 24 June 2014.

and suppression of OCTAs. In light of this discussion, Chapter 4 thus found that UN resolutions, while acknowledged OCTAs within the counterterrorism discourse, did not go far enough to adopt counterterrorism resolutions pertaining specifically to their prohibition under international law that could otherwise unequivocally impose legally binding obligations on states.

As a result of the scarcity of directly applicable law, Chapter 5 focused on the customary international law obligation to prevent transboundary harm as a legal mechanism that could be used to hold states responsible for malicious cyber terrorist activities originating from a state's sovereign territory, including from its cyber infrastructure. The general rule emanating from customary law is that it is 'every state's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states'.[16] Flowing from the principle of sovereignty, the application of this rule in cyberspace has been affirmed by a number of states including France, New Zealand, Australia and others, recognising that cyber operations causing physical harm or injury clearly violated the principle of sovereignty.[17] This assertion made by several states is important because it confirmed that sovereignty and its corresponding rules of international law, specifically the obligation to prevent transboundary harm, applied to cyberspace and therefore, to cyber activities.

An examination of the nature, content and scope of the principle demonstrated that the obligation to prevent transboundary harm applied only in relation to activities that, if committed by a state, would be internationally wrongful and that gave rise to sufficiently serious consequences for the violation of legal rights belonging to the victim state. This included harmful activities of a terrorist nature committed in cyberspace. When it comes to harmful cyber terrorist acts committed by non-state actors, those located from the cyber infrastructure under the exclusive control of one state have the capacity to breach the sovereign rights of those belonging to another state. This chapter highlighted an important distinction. While the level of harm presented by the cyber terrorist act must cross a de minimis threshold, it does not have to result in physical damage of cyber infrastructure.

[16] Corfu Channel (UK v. Albania), 1949, Judgment of April 9th, 1949 I.C.J. Reports 1949.
[17] See Republique Française Ministère Des Armées, Droit International appliqué aux operations dans le cyberspace, 9 September 2019. Available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf (accessed 18 November, 2019); New Zealand Department of the Prime Minister and Cabinet, 'The Application of International Law to State Activity in Cyberspace', 1 December 2020. Available at https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf (accessed 21 January 2021); Australia International Cyber Engagement Strategy, Annex A: Application of International Law in Cyberspace (2017) available at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html (accessed 19 November, 2019). See Chapter 5 for discussion on different States affirming the rule of sovereignty having application in cyberspace.

This is important because it means the obligation to prevent transboundary harm applies to acts of cyberterrorism that are harmful but that do not necessarily result in tangible consequences.

Moreover, this chapter recognised an important criterion for assessing the state's efforts in meeting duties under the obligation to prevent transboundary harm. Conditioned by the standard of due diligence, this principle takes into consideration the state's knowledge, its best efforts and its technical capacity to prevent the harmful cyber terrorist act in question. The chapter also underlined other factors affecting the execution of obligations including the effectiveness of state control, the likelihood of harm and the importance of the legal rights and interests that require protection. Such considerations, as this chapter has explored in detail, ensures that states are not bound to legal obligations that are unreasonable or excessive in relation to its responsibilities. Instead, the legal obligations of due diligence safeguard the state in the performance of its duties by recognising that it does not need to shoulder an unduly heavy burden to prevent all forms of transboundary harm in absolute. The chapter thus offered a critical discussion of this customary obligation and its practical application as it relates to measures of prevention regarding harmful cyber terrorist acts.

Finally, Chapter 6 applied the obligation to prevent transboundary harm to OCTAs. The chapter distinguished between the two types of OCTAs that could trigger state responsibility. On one hand, there are OCTAs that, if committed by a state, would interfere with the legal rights of other states and amount to violations of international law. The incitement to terrorism is one example, that if committed by a state could breach international law by way of sovereignty, the principle of non-intervention or equally, certain Security Council resolutions. On the other hand, there are OCTAs that are not international wrongful acts and do not amount to violations of international law. Sharing social media posts supporting ISIS helps promote terrorism, but does not constitute an international wrongful act, if committed by the state. This chapter therefore drew attention to the types of OCTAs that would be unlawful and whether such OCTAs could trigger state responsibility under the obligation to prevent transboundary harm.

Analysis has further demonstrated that the obligation is triggered on the premise of knowledge – either when the state knew or should have known of the OCTA. The chapter discussed the significance of constructive knowledge of OCTAs as the leading trigger to state responsibility. This was particularly insightful because this requirement reiterated the importance of states to engage in measures where the knowledge of OCTAs could be acquired and that it remains a duty of the state to ensure it is diligent in informing itself of potential transboundary harm. State responsibility, however, is still contingent on the state's knowledge of the OCTA causing serious adverse consequences for another state. These requirements emphasized that considerations as to state responsibility were based primarily on two

factors: the nature of the harmful act, and the circumstances of the state allowing it to respond and prevent. The obligation to prevent transboundary harm seems to normative value of striving towards peace but only when peace is threatened by a particular type of harmful conduct.

In relation to the circumstances of the state, this chapter highlighted that duties under the obligation to prevent transboundary harm were correlative; the more resources the state possesses, the higher the degree of diligence due for states to undertake duties to notify and warn, cooperate and exchange information as well as to investigate, prosecute and punish those responsible for OCTAs. This analysis incorporated the legal standard of due diligence because its flexible nature means adherence to the obligation varies depending on the context and the level of development of the state to ensure reasonableness.[18] Furthermore, the ILA suggests that 'the standard of due diligence [is] a useful yardstick by which to hold all states to varying degrees to a minimum standard of conduct.'[19] In any case, a higher level of diligence is expected of the territorial state where the violation of an international legal right such as sovereignty or non-intervention is concerned. On this view, international law is meant to be used to protect the international legal rights of sovereign states. Importantly, the chapter showed that the obligation to prevent transboundary harm relies on states to engage in necessary measures in order to discharge itself of its duties. At the same time, these duties ensure the state itself is protected from harmful conduct emanating from neighbouring states.

The chapter also shed light on how the obligation to prevent transboundary harm applied to each OCTA. In doing so, the discussion provided hypothetical examples of OCTAs and the measures that could be taken by states in response to these harmful cyber terrorist activities. As a result of this discussion, the chapter made practical application of the obligation to prevent transboundary harm in an attempt to understand the implications that this principle would have on states and the responsibilities they would be expected to undertake when faced with OCTAs. Because the chapter analysed the obligation to prevent transboundary harm in light of OCTAs, it provided a fresh interpretation to this customary principle under international law and applied it in a practical manner. As a result, Chapter 6 has postulated this alternative method of achieving state responsibility as a pragmatic and effective way of preventing certain types of OCTAs. This principle can contribute towards the fight against global terrorism and help to maintain international peace and security by

[18] Riccardo Pisillo-Mazzeschi, "Due Diligence and the International Responsibility of States", *35 German Y.B. Int'l L. 9* (1992), at p.45. The author States that 'as the content of certain obligations of diligent conduct becomes more specific and more detailed, also the concept of due diligence becomes more specific and tends to lose its characteristic of a general and flexible norm of behaviour'.

[19] Tim Stephens and Duncan French, 'ILA Study Group on Due Diligence in International Law', *International Law Association,* Second Report, (July 2016), p. 47.

decreasing the potential for acts of violent terrorism to materialise and therefore, diminishes threats towards peace in both its negative and positive concepts.

In conclusion, the thesis found that current international law offers a piecemeal regime to the protection of states against OCTAs. From the analysis of regional treaties, UN resolutions and customary international law, it demonstrated that there are few rules in place that can prohibit OCTAs. While some of the existing law does have normative value in that it strives towards peace in both its negative and positive conceptions and certain legal obligations can be said to create the conditions that can encourage positive peace, the peace theory remains an imperfect framework to the rules explored in this thesis concerning OCTAs. In addition to this, analysis showed that only OCTAs, that if committed by a state, and violate the international legal rights of another state are subject to rules of international law. This finding reiterates the focus of the international community that has been on the threat of cyber terrorist warfare. Despite contributing significantly to the functions of terrorist organisations and to the materialisation of terrorist violence, OCTAs, if committed by a state, do not trigger state responsibility unless they can be shown to constitute an act of terrorism in and by themselves. This demarcation of OCTAs reinforces the subordinate nature of certain terrorist activities as they relate to recruitment, financing and propaganda. In light of this, a pervading and continual danger to the maintenance of international peace and security is being greatly miscalculated. OCTAs will continue to perpetuate terrorist organisations by enabling their operations to catalyse into acts of violent terrorism. Accepting this, the international community must continue to address the issues relating to all forms of OCTAs and to hold states responsible in order to ensure their prevention and suppression for the maintenance of international peace and security.

III. Core Findings and Contributions

The aim of this thesis has been to determine whether the current legal landscape of international law is capable of addressing OCTAs. In doing so, this research has engaged specifically with the legality of OCTAs, the theoretical framework concerning OCTAs, the existing legislation for holding states responsible for OCTAs and the state's duties to prevent OCTAs under the obligation to prevent transboundary harm. By analysing and evaluating the existing framework of international law, this thesis has engaged and contributed to the discussion surrounding the regulation of OCTAs and determined the applicability of current rules to cyber terrorist recruitment, financing and propaganda activities. This thesis has concluded a number of findings demonstrating how this engagement is important for the literature in the field.

First, this thesis has reconsidered how international law can be interpreted to apply to OCTAs through the analysis of regional treaties, UN resolutions and customary international law. Through

using the general rule of interpretation under Article 31(1) VCLT 1969 concerning international law, this thesis has shown that regional conventions pertaining to cyber technology, cybercrime and informational technology can be understood to provide limited guidance on the prohibition of OCTAs. Discussion in Chapter 3 has revealed that the attention of existing law seems to be primarily focused on terrorist's use of cyberspace for the purposes of launching violent cyber-attacks. In this sense, existing rules of international law have shown that most legal provisions are concerned with cyber offences related to the damage of computer systems or computer data. As Chapter 3 has made it clear, the legally binding obligations contained within the regional conventions can thus be said not to include OCTAs.

Further analysis of Security Council and General Assembly resolutions as well as meetings and reports have shown that the UN's collective security system recognises OCTAs and consistently highlights their role within the commission of violent terrorism. Prior to reviewing the resolutions, the researcher expected UN resolutions to show limited consideration of OCTAs, particularly as their prohibition is not explicit within the UN's wider counterterrorism initiative. This is emphasised by the Security Council's adoption of resolutions that predominantly concern the condemnation of terrorist attacks.[20] Thus, the researcher found this revelation to be incongruous. The Security Council has expressed continued concern at the use of technologies for the purposes of terrorist recruitment, financing and propaganda and acknowledged the implications of OCTAs and their purpose within the wider goal of terrorism. Furthermore, the preambular paragraph in Resolution 2322 recognised the use of the internet *'*to facilitate terrorist acts' as a concern. [21] Therefore, the Security Council has acknowledged OCTAs as an issue on the periphery of the counterterrorism agenda. However, the Security Council stops short of 'declaring' that OCTAs should be prohibited. Thus, while OCTAs are identified as essential activities that further terrorism, the Security Council has not yet adopted a resolution imposing legally binding obligations for their prevention and suppression.

This being said, Resolution 1624 (2005) clearly demonstrated the Security Council's recognition of the incitement to commit terrorist acts as an OCTA that warrants international legal attention through state action.[22] Still, the Security Council's reluctance to use binding language to impose obligations on states to prohibit incitement reiterated their stance as it concerns OCTAs. As such, the view that OCTAs are treated as acts of terrorism that are less significant, less threatening and less dangerous than acts of terrorism in the form of terrorist attacks is reaffirmed by analysis of the UN's resolutions in Chapter

[20] See for example United Nations Security Council Resolution 1368, S/RES/1368 of September 12, 2001; United Nations Security Council Resolution 1373, S/RES/1373 of 28 September 2001; United Nation Security Council Resolution 2170, S/RES/2170 of 15 August 2014.
[21] United Nations Security Council Resolution 2322, S/RES/2322 of 12 December 2016.
[22] United Nations Security Council Resolution 1624, S/RES/1624 of 14 September 2005.

4. The discussion revealed that UN resolutions deal with the general area as it concerns OCTAs, but closer examination demonstrated that language used impose no legally binding obligation on states to prevent this type of activity. Further to this, the General Assembly's resolutions lack the required normative content and language to constitute opinio juris and thus, cannot be considered as evidence of customary law-making concerning the prevention of OCTAs. Whilst the Security Council and the General Assembly recognised the need for international cooperation to address OCTAs, Chapter 4 confirmed that current counterterrorism measures prohibit certain activities but not others; they do not adequately prevent and suppress all OCTAs under international law.

While regional treaties relating to cyber security and cyber technology offences, and the UN's resolutions of the Security Council and the General Assembly have revealed that current provisions are stronger at preventing and suppressing OCTAs than initially thought, they nevertheless remain insufficient and fragmented in their approach. As a result, the scarcity of applicable legislation has had an important and effective result on the continuation of OCTAs and the commission of violent terrorism in the present climate.[23] To this end, it remains vital that international law takes proactive measures to ensure that all OCTAs are prevented from perpetuating cyberterrorism in the fight against terrorism.

Second, this thesis has re-evaluated the utility of due diligence as a standard conditioning the obligation to prevent transboundary harm regarding OCTAs and thus applied it to a new situation. In doing so, it has found that obligations of due diligence are elastic in nature and can be stretched to apply to contemporary areas of international law.[24] This thesis has shown that due diligence obligations shrink or expand depending on certain factors that then shape the state's responsibilities.[25] In turn, this analysis drew attention to the fact that the obligation to prevent transboundary harm and its related duties do not apply to all OCTAs. The triggers to the obligation to prevent transboundary harm require both that the OCTA, if committed by a state, amounts to an international wrongful act and crosses the de minimis threshold of harm.

---

[23] See for example Arie W. Kruglanski, Rohan Gunaratna, Molly Ellenberg & Anne Speckhard, 'Terrorism in time of the pandemic: Exploiting Mayhem,' *Global Security: Health, Science and Policy,* 5:1, 121-132 (2020); International Crisis Group, 'COVID-19 and Conflict: Seven Trends to Watch', Special Briefing No. 4 (24 March 2020). Available at https://www.crisisgroup.org/global/sb4-covid-19-and-conflict-seven-trends-watch (accessed 11 February 2021); Brian Glyn Williams, 'Islamic State Calls for Followers to Spread Coronavirus, Exploit Pandemic and Protests,' The Conversation (23 June 2020). Available at https://theconversation.com/islamic-State-calls-for-followers-to-spread-coronavirus-exploit-pandemic-and-protests-136224 (accessed 11 February 2021).

[24] Robert Barnidge, *Non- State Actors and Terrorism: Applying the Law of State Responsibility and the Due Diligence Principle,* The Hague, (TMC Asser Press, (2008) at p. 139. The author contends that 'the due diligence principles means, or at least can be construed to mean, everything to everyone and nothing to no one.'

[25] Riccarrdo Pisillo-Mazzeschi, 'Due Diligence and the International Responsibility of States,' 35 German Y.B. Int'l L. 9 (1992), at p. 45.

In regard to the former, this research has found that the obligation to prevent transboundary harm applies only to those OCTAs, that if attributed to a state, would amount to a violation of international law. On this view, the referent rule is the principle of sovereignty, from which other rules emanate such as the right to non-intervention. In this sense then, only OCTAs that if committed by a state and encroach upon the international legal rights of other states necessitate international legal attention and trigger state responsibility through the obligation to prevent transboundary harm. This distinguishes from OCTAs that are not unlawful acts if attributed to the state. OCTAs of this kind pave the way for terrorist violence by contributing to terrorist operations. But these OCTAs do not have close proximity to an act of political violence and thus, do not violate any rules of international law if committed by a state.

As it relates to the latter, the OCTA in question – should it amount to an international wrongful act if attributed to a state – must still cross a minimum threshold of harm in order to trigger both obligations to prevent transboundary harm and due diligence. Only those OCTAs considered to cause sufficiently serious violence cross the de minimis threshold if committed by a state. Thus, legal duties arising from this principle only apply to states where such OCTAs meet these minimum requirements. This distinction is further illuminated by way of analysis of the due diligence standard, which considers various factors to assess the state's performance of its legal duties in relation to OCTAs. This discussion revealed that the obligation to prevent transboundary harm is important only for OCTAs that can trigger its application under international law. In this sense then, the obligation to prevent transboundary harm and the legal duties arising from the standard of due diligence are restricted explicitly for OCTAs that can be considered acts of terrorism, if committed by a state. This finding was significant because it reiterated the presumption that international law triggers state responsibility only where violations of international legal rights are concerned. For acts that fall below this threshold, they remain ungoverned by rules of international law despite constituting a threat to international peace and security.

Third, this thesis has reinterpreted the obligation to prevent transboundary harm by applying this principle to a new context of cyberspace, and specifically to OCTAs. This thesis has established that the obligation to prevent transboundary harm can be understood to apply to harmful activities that are not traditionally addressed under this principle. This obligation can be used to coerce states to act in response to cyber terrorist recruitment, financing or propaganda activities that originate on or from their sovereign territories in order to prevent the infringement of rights belonging to other states. This finding, to some extent, supports the view that OCTAs can indeed be subject to rules of international law. In the context of OCTA's as violations of international law, however, not all OCTAs interfere with

the legal rights of states. Therefore, while the analysis supports the view that some OCTAs can amount to violations of international law, it is difficult to argue that all OCTAs breach international law if attributed to a state. Nevertheless, this thesis has shown that where OCTAs do not breach international law, they should be seen as composite acts that are central to the development of terrorist operations and thus contribute immeasurably to the broader act of ultimate terrorist violence and must nevertheless be prohibited under international law.

This thesis has found that the use of customary international law is able to provide an appropriate and practical solution to a prevalent problem within international terrorism, that is, until rules governing terrorist's exploitation of cyberspace crystallise. This finding has demonstrated the utility of international law in preventing and suppressing OCTAs. Most importantly, the use of this customary obligation as a legal mechanism sheds light on the limitations of treaty provisions and their ability to keep up to date with emerging issues related to cyber technology and terrorism. This thesis has shown that the utility and function of international law is imperative to improving the international legal framework surrounding cyberterrorism and particularly OCTAs. Hence, it was not only helpful to identify the role of international law in countering terrorism, but it was also necessary to establish the function and purpose of using an existing principle of customary international law to prevent a widespread problem of terrorism. With these findings, this thesis has intended to contribute to an important aspect of countering terrorism. In particular, by contributing to the literature on the use of customary international law to address matters of cyberterrorism, this thesis has provided an alternative explanation to the regulation of OCTAs under international law.

Fourth, this thesis has reconceptualised how OCTAs endanger international peace and security. It has presented OCTAs as both international wrongful acts and as terrorist activities that are the building blocks to violent terrorism. This distinction has revealed that the latter category of OCTAs still lack adequate prohibition despite remaining a matter of public international law. For these OCTAs, they continue to contribute towards the effective functioning of terrorist groups and enable the commission of acts of violent terrorism. But by the lack of proximity to an act of political violence, it seems that the legal address of OCTAs remains shallow until they can be shown to meet the de minimis threshold of violence required to trigger states' obligations to prevent transboundary harm under international law. This is the case despite OCTAs posing a serious threat to the achievement of both positive and negative peace. In turn, this finding raises some serious concerns that affect the maintenance of international peace and security.

The lack of applicable international law to address OCTAs allows for the continued exploitation of cyberspace by terrorist groups. This means that terrorist groups can continue to launch OCTAs whilst

evading legal responsibility for conducting malicious acts of terrorism. On this issue, the gap in the law concerning the actions of non-state actors on the international legal scene remains a prevalent issue.[26] This view is affirmed by Kubo Mačák, who argues that in the absence of concrete rules within cyberspace 'a power vacuum [enables] non-state actors to move into the space vacated by states.'[27] Similarly, in the words of Michael Schmitt and Sean Watts, cyber operations have allowed 'significant gaps in resources and capacity between states on the one hand and non-state actors on the other [which has] prevented their interactions from demanding significant legal attention'.[28] This means that until states adopt legal rules governing cyberspace, non-state actors continue to remain largely ungoverned in an inherently state-centric landscape.

To add to this, states are under no explicit legal obligations to prevent OCTAs under the existing international legal framework. As shown in Chapters 3 and 4, analysis of existing provisions of current legal rules showed that there is no binding duty that makes it mandatory for states to prohibit OCTAs. In other words, international law does not define how states should behave in the face of OCTAs and subsequently, it does not enforce action requiring their prevention. If states are not subject to legal obligations, the prohibition of OCTAs is contingent upon the volition and will of states which does not guarantee the safeguarding and protection of international legal rights belonging to other states.

In light of the above discussion, this thesis has recognised the threat presented by OCTAs and their need to be prohibited under international law. OCTAs are indispensable to the commission of violent terrorism. OCTAs are the building blocks that facilitate the growth of terrorist organisations by providing ample tools to cultivate and orchestrate acts of violent terrorism. At the same time, the perilous nature of OCTAs means they can easily amount to acts of terrorism, if committed by a state. As such, the need for more adequate measures for states to prevent and suppress OCTAs under the existing international legal framework is chief in the fight against terrorism. With this in mind, OCTAs must be subject to rules of prohibition under international law in order to better counter terrorism and to ensure and maintain international peace and security for states. Accepting this, the following section suggests future areas of research that can contribute towards our understanding of OCTAs under international law.

---

[26] See for example Math Noortmann, August Reinisch, Cedric Ryngaert, *Non-State Actors in International Law*, (Hart Publishing, 2015); Tal Becker, *Terrorism and the State: Rethinking the Rules of State Responsibility*, (Hart Publishing, 2006); Kimberley Trapp, 'Shared Responsibility and Non-State Terrorist Actors,' *Netherlands International Law Review* 62: 141-160 (2015); Demetrius Delibasis, 'Cybersecurity and State Responsibility: Identifying a Due Diligence Standard for Prevention of Transboundary Threats', in Joanna Kulesza and Roy Balleste, ed. *Cybersecurity and Human Rights in the Age of Cyberveillance,* (Rowman & Littlefield, 2015).

[27] Kubo Mačák, 'Is the International Law of Cyber Security in Crisis?', 8th Int'l Conference on Cyber Conflict, *NATO CCD COE Publications*, (2016), at p. 133.

[28] Michael Schmitt and Sean Watts, 'Beyond State-Centrism: International Law and Non-State Actors in Cyberspace', *Journal of Conflict & Security Law*, Vol. 21, No. 3, 595-611 (2016), at p. 595-596.

IV. Recommendations for Areas of Future Research

Based on the above summary and key findings, this thesis proposes a number of recommendations and measures aimed at improving the international legal framework for preventing OCTAs and cyberterrorism generally.

The first recommendation suggests exploring the use of sanctions to target the state that is not taking effective action against OCTAs committed by non-state actors. Sanctions could, for instance, involve targeting those individuals that are involved in accommodating or cooperating OCTAs and placing such individuals on a blacklist. This could impose conditions that limits international financial transactions, otherwise known as economic sanctions. Thus, for states that are not fulfilling their responsibilities to prevent OCTAs, economic sanctions could be targeted against the host state. This could impose prohibitions on certain economic transactions with the country, including the import or export of certain goods and financial services. For instance, if a state were known to have its territory used by terrorist groups to launch OCTAs, and the state refused to take action to prevent such activities from affecting other states, the victim state or states could respond with countermeasures provided they comply with the restriction this doctrine imposes.

Second, it is suggested that exploring different types of terrorist groups can help to better understand the diversified use of social media and cyber technology to conduct OCTAs. Thus, it may be beneficial that further research be done on the role of different terrorist groups beyond ISIS and their legal accountability in cyberspace when it comes to transboundary harm that falls below the de minimis threshold. For instance, it would be interesting to examine Boko Haram or al-Shabaab and their use of OCTAs in their relative terrorist campaigns. Where possible, a comparative analysis between these different terrorist groups to analyse their use of social media and cyberspace for OCTAs and whether or not certain tactics are more or less effective to achieving terrorist objectives would also be a noteworthy study. Thus, a determination of the best measures that could be implemented under international law to prevent terrorists' use of social media and cyberspace for OCTAs could be recommended on the basis of this study.

Last, but by no means least important, pro-active law-making is needed at an international level by way of an international treaty prohibiting OCTAs. Terrorism will continue to dominate the security agenda and OCTAs are key to terrorism. While international law can play an important role in combatting OCTAs and thus, terrorism, this research has shown that international law provides incomplete protection. In light of this, it is imperative that precursors to terrorist attacks are addressed by binding rules of international law to ensure their prohibition. This involves the deterrence of OCTAs and the outlawing of such activities on an international level insofar that they constitute a violation of

the law. Thus, noteworthy research would involve the discussion of a cyberterrorist-related treaty and the necessity to prohibit OCTAs with absolute severity, as the principal and paramount impetus to achieving violent terrorist ends. Whilst the suggestion of a cyberterrorism treaty is unenthusiastic and well-trodden by international cyber scholars, it remains nonetheless pertinent that the emergence of such a treaty would equip states and the international community with the necessary legal tools to tackle OCTAs in order to ensure and maintain international peace and security.

BIBLIOGRAPHY

I. Primary Sources

1.1 Cases

Alabama Arbitration Case (United States of America v United Kingdom) (14 September 1872), Papers relating to Foreign Relations of the United States 1872 (United States Government Printing Office Washington 1873) part 2 Vol IV.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnian and Herzegovina v. Serbia and Montenegro) Judgment, I.C.J. Reports 2007, p. 43.

Arbitral Award of 31 July 1989 (Guinea-Bissau v Senegal) Judgment, [1991] ICJ Reports 53.

Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 655.

Corfu Channel (U.K. v. Albania), 1949, Judgment of April 9th, 1949: I.C.J. Reports 1949.

Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging (STL-11-01/I), Appeals Chamber, 16 February 2011.

Island of Palmas case (Netherlands v. United States), Permanent Court of Arbitration (Huber), 2 Reports of International Arbitral Awards (1928), p. 829.

Janes (U.S. v Mex.), 4 R.I.A.A. 82 (1926).

Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, ICJ Reports 1971, p. 16.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ GL No. 95 (1996), ICJ Rep 226, 8th July 1996.

Massey (U.S. v. Mex.), 4 R.I.A.A. 155 (1927).

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgments, I.C.J. Reports 1986.

The Mox Plant Case (Ireland v. United Kingdom) ITLOS (3 December, 2001).

North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3

Pulp Mills on the River Uruguay (Argentina v. Uruguay) (hereinafter referred to as Pulp Mills), Judgment, I.C.J. Reports 2010, p. 14.

Sovereignty over Pulau Litigan and Pulau Sipadan (Indonesia/Malaysia) (2002) ICJ Rep 625, ICGJ 54 (ICJ 2002), 17th December 2002.

Trail Smelter Arbitration (U.S. v. Canada), 3 RIAA 1905, 1965 (1941).

United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment of 24 May 1980, ICJ Reports 1980, p. 3.

R v Tsouli (2007) EWCA (Crim) 3300.

Youmans (U.S. v. Mex.), 4 R.I.A.A. 110 (1926).

1.2 International and Regional Treaties

The African Union Convention on Cybersecurity and Personal Data Protection (2014).

The Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information (CIS Agreement) (2001).

The Arab Convention on Combating Information Technology Offences (2010).

The Charter of the United Nations, 1945.

Conference on Security and Cooperation in Europe Final Act ('Helsinki Final Act'), Helsinki 1975.

Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage Convention or Montreal Convention), Sept. 23, 1971.

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention), March 10, 1988.

Convention for the Suppression of Unlawful Seizure of Aircraft (Hague Convention), Dec. 16, 1970

Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo Convention), Sept. 14, 1963.

Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention), March 1, 1991.

Convention on the Physical Protection of Nuclear Material (Nuclear Materials Convention), Oct. 26, 1979.

Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons (Diplomatic Agents Convention), Sept. 28, 1973.

Council of Europe, Convention on Cybercrime, ETS No. 185 (November 23, 2001).

International Convention against the Taking of Hostages (Hostages Convention), Dec. 18, 1979.

International Convention for the Suppression of the Financing of Terrorism, opened for signature 9 December 1999, 2178 ILM 229 (entered into force 10 April 2002).

International Law Commission Articles on Responsibility of States for Internationally Wrongful Acts (2001), ILC Yearbook 2001/ II (2) (ARSIWA).

International Law Commission Draft Articles on Prevention of Transboundary Harm from hazardous Activities, with Commentaries (2001).

The Organisation of American States (OAS) Comprehensive Inter-American Cybersecurity Strategy (2004).

The Shanghai Cooperation Organisation Agreement (2009).

The Statute of the International Court of Justice (1945).

United Nations Convention against Transnational Organised Crime (2000) adopted by General Assembly resolution 55/25 of 15 November 2000.

The Vienna Convention on the Law of Treaties (1969).

1.3 International Resolutions

United Nations General Assembly Resolution 49/60, A/RES/49/60 of 9 December 1994.

United Nations General Assembly Resolution 51/210, A/RES/51/210 of 17 December 1996.

United Nations General Assembly Resolution 60/288, A/RES/60/288 of 8 September 2006.

United Nations General Assembly Resolution 68/276, A/RES/68/276 of 24 June 2014.

United Nations General Assembly Resolution 70/291, A/RES/70/291 of 19 July 2016.

United Nations General Assembly Resolution 72/194, A/RES/72/194 of 23 January 2018.

United Nations General Assembly Resolution 72/284, A/RES/72/284 of 2 July 2018

United Nations Security Council Resolution 82, S/RES/82 of 25 June 1950.

United Nations Security Council Resolution 687, S/RES/687 of 3 April 1991.

United Nations Security Council Resolution 731, S/RES/731 of 21 January 1992

United Nations Security Council Resolution 748, S/RES/748 of 31 March 1992.

United Nations Security Council Resolution 794, S/RES/794 of 3 Dec. 1992

United Nations Security Council Resolution 827, S/RES/827 of 25 May 1993

United Nations Security Council Resolution 955, S/RES/955 of 8 Nov. 1994.

United Nations Security Council Resolution 1044, S/RES/1044 of 31 January 1996.

United Nations Security Council Resolution 1054, S/RES/1054 of 26 April 1996.

United Nations Security Council Resolution 1267, S/RES/1267 of 15 October 1999.

United Nations Security Council Resolution 1269, S/RES/1269 of 19 October 1999.

United Nations Security Council Resolution 1368, S/RES/1368 of 12 September 2001.

United Nations Security Council Resolution 1373, S/RES/1373 of 28 September 2001.

United Nations Security Council Resolution 1515, S/RES/1515 of 19 November 2003.

United Nations Security Council Resolution 1516, S/RES/1516 of 20 November 2003.

United Nations Security Council Resolution 1526, S/RES/1526 of 30 January 2004.

United Nations Security Council Resolution 1530, S/RES/1530 of 11 March 2004.

United Nations Security Council Resolution 1535, S/RES/1535 of 26 March 2004.

United Nations Security Council Resolution 1540, S/RES/1540 of 28 April 2004.

United Nations Security Council Resolution 1566, S/RES/1566 of 8 October 2004.

United Nations Security Council Resolution 1624, S/RES/1624 of 14 September 2005.

United Nations Security Council Resolution 1973, S/RES/1973 of 17 March 2011.

United Nation Security Council Resolution 2129, S/RES/2129 of 17 December 2013.

United Nation Security Council Resolution 2133, S/RES/2133 of 27 January 2014.

United Nation Security Council Resolution 2170, S/RES/2170 of 15 August 2014.

United Nations Security Council Resolution 2177, S/RES.2177 of 18 September 2014.

United Nations Security Council Resolution 2178, S/RES/2178 of 24 September 2014.

United Nations Security Council Resolution 2249, S/RES/2499 of 20 November 2015.

United Nations Security Council Resolution 2253, S/RES/2253 of 17 December 2015.

United Nations Security Council Resolution 2322, S/RES/2322 of 12 December 2016.

United Nations Security Council Resolution 2368, S/RES/2368 of 20 July 2017.

United Nations Security Council Resolution 2396, S/RES/2396 of 21 Dec. 2017.

United Nations Security Council Resolution 2462, S/RES/2462 of 28 March 2019.

United Nations Security Council Resolution 2482, S/RES/2482 of 19 July 2019.

1.4 EU Legislation

European Commission, 5th Anti-Money Laundering Directive (Directive (EU) 2018/843.

1.5 National Legislation

UK Statutory Instruments, The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 No. 1511.

1.6 International Official Reports and Documents

African Union Convention on Cyber Security and Personal Data Status List. Available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189 (Strasbourg, 28.I.2003).

Council of Europe, 'Charts of Signatures and Ratifications of Treaty 185 (Status as of 28/02/2019), available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=vI0e9aDG

Council of Europe, Chart of Signatures and Ratifications of Treaty 189, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=JQOolQVB

Council of Europe GLACY+ Report, 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime', (20 November 2016).

Council of Europe, Guidance Notes to Convention on Cybercrime (2001), available at https://www.coe.int/en/web/cybercrime/guidance-notes

Council of Europe, T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention, (November 15, 2016).

EUROPOL, 'Changes in Modus Operandi of Islamic State (IS) Revisited', The Hague, (November 2016), available at https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

GLACY+ report, Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime, 20 November 2016.

Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*, FATF, Paris, France (2012 - 2019).
Financial Action Task Force Report, Financing of Recruitment for Terrorist Purposes, January 2018, FATF Paris.

Financial Action Task Force Report, Terrorist Financing Risk Assessment Guide, July 2019, FATF Paris.

Gercke, M., 'Understanding Cybercrime: Phenomena, Challenges and Legal Response', ITU Publication (September, 2012).

International Labour Office, International Organization for Migration, and Officer of the United Nations High Commissioner for Human Rights Discussion Paper, 'International Migration, Racism, Discrimination and Xenophobia' (2001), at p. 2. Available at https://www2.ohchr.org/english/issues/migration/taskforce/docs/wcar.pdf (accessed 4 June 2018).

International Telecommunication Union (ITU) Report, Global Cybersecurity Index (GCI), (2017).

International Telecommunication Union (ITU) Publication 'Understanding Cybercrime: Phenomena, Challenges and Legal Response', (September 2012).

United Nations Development Program (UNDP) Regional Centre for Africa, 'Social Media in Africa: A Double-Edged Sword for Security and Development', Research Report, 5 November 2018.

United Nations General Assembly, Activities of the United Nations System in Implementing the United Nations Global Counter-Terrorism Strategy: Report of the Secretary-General, A/72/840 of 20 April 2018.

United Nations General Assembly, "Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism", annexed to UNGA, "Measures to Eliminate International Terrorism", 17 December 1996, UN doc. A/RES/51/210. Available at https://www.legal-tools.org/doc/c8397d/

United Nations General Assembly, General Assembly President Miroslav Lajcak (Slovakia), UNGA GA/12035, 'General Assembly Unanimously Adopts Resolution Calling for Strong Coordinated Action by Member States to Tackle Terrorism, Violent Extremism Worldwide', (June 26, 2018).

United Nations General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174, (22 July 2015).

United Nations General Assembly, Letter dated 3 August 2005 from the Chairman of the Sixth Committee addressed to the President of the General Assembly, A/59/894 of 12 August 2005.

United Nations General Assembly, Michael Wood, First Report on Formation and Evidence of Customary International Law, UN Doc. A/CN.4/ 4663 (17 May 2013).

United Nations General Assembly, Review of the Implementation of the Recommendations and Decisions adopted by the General Assembly at its tenth special session: Advisory Board on Disarmament Matters, A/60/285 of 22 August 2005.

United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States, S/2016/49 of 20 January 2016.

United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), Technical Guide to the Implementation of Security Council Resolution 1373 (2001) and other Relevant Resolutions' (2017).

United Nations Security Council, Letter dated 13 May 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counterterrorism addressed to the President of the Security Council, S/2015/338 of 14 May 2015.

United Nations Security Council, Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counterterrorism addressed to the President of the Security Council, S/2016/50 of 28 January 2016.

United Nations Security Council Meetings Coverage, 'ISIL/Da'esh Continues Evolution into Covert Global Network Enjoying Access to Millions of Dollars, Top Anti-Terrorism Official Tells Security Council', SC/13697 of Feb. 11, 2019.

United Nations Security Council Meeting Press Release 4618th Meeting, SC/7522 of 4 October 2002.

United Nations Security Council, United Nations Security Council 4413th Meeting, S/PV.4413 of 12 November 2001.

United Nations Security Council, United Nations Security Council 4710th Meeting, S/PV.4710 of 20 February 2003.

United Nations Security Council, United Nations Security Council 7587th Meeting, S/PV.7587 of 17 December 2015.

United Nations Security Council, United Nations Security Council 7831st Meeting, S/PV.7831 of 12 December 2016.

United Nations Security Council, United Nations Security Council 8148th Meeting, S/PV.8148 of 21 December 2017.

United Nations Security Council, United Nations Security Council Meeting 8330th Meeting, SC/13463 of 23 August 2018.

United Nations Security Council, United Nations Security Council 8560th Meeting, S/PV.8460 of 11 February 2019.

United Nations Security Council, Note by the President of the Security Council, S/23500 of 31 January 1992.

United Nations Security Council, Security Council Press Release, SC/12120 of 13 November 2015.

United Nations Security Council, Security Council Press Release, SC/12121 of 13 November 2015.

United Nations Security Council, Security Council Press Release, SC 12132 of 20 November 2015.

United Nations Security Council, Third Report of The Secretary-General on The Threat Posed by ISIL (Da'esh) To International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat, S/2016/830 of 30 September 2016.

United Nations Security Council, Fourth Report of the Secretary-General on The Threat Posed by ISIL (Da'esh) To International Peace and Security and The Range Of United Nations Efforts In Support Of Member States In Countering The Threat, S/2017/97 of 2 February 2017.

United Nations Security Council, Sixth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) To International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat, S/2018/80 of 31 January 2018.

United Nations Security Council, Statement by the President of the Security Council, S/PRST/2013/1 of 15 January 2013.

United Nations Security Council, Statement by the President of the Security Council, S/PRST/2016/6 of 11 May 2016.

United Nations Office on Drugs and Crime, The Use of the Internet for Terrorist Purposes, (United Nations, 2012).

II. Secondary Sources

2.1 Books and Book Chapters

Barnidge, R., *Non- State Actors and Terrorism: Applying the Law of State Responsibility and the Due Diligence Principle,* The Hague, TMC Asser Press (2008).

Becker, T., *Terrorism and the State: Rethinking the Rules of State Responsibility*, (Hart Publishing, 2006).

Bianchi, A., "Enforcing International Law Norms Against Terrorism: Achievements and Prospects" in Bianchi, A., *Enforcing International Law Norms Against Terrorism*, (Hart Publishing, 2004).

Bourne, M., *Understanding Security*, (Palgrave Macmillan 2014).

Brownlie, I., *Principles of Public International Law* (4th ed.) (Oxford: Clarendon, 1990).

Buchan, R., *Cyber Espionage and International Law* (Hart Publishing, 2018).

Buchan, R., *International Law and the Construction of the Liberal Peace*, (Hart Publishing, 2013).

Bussolati, N., "The Rise of Non-State Actors in Cyberwarfare", at p. 102, in eds. Ohlin, J. D., Govern, K., and Finkelstein, C., *Cyber War: Law and Ethics for Virtual Conflicts*, (OUP, 2015).

Chynoweth, P., 'Legal Research', in ed. Andrew Knight and Les Ruddock, *Advanced Research Methods in the Built Environment*, (Wiley-Blackwell, 2008).

Conway, M., "Cyberterrorism: Hype and Reality", in Leigh Armistead, ed., *Information Warfare: Separating Hype from Reality* (Dulles, VA: Potomac, 2007), 73 – 93.

Crawford, J., State Responsibility: The General Part, *Cambridge Studies in International and Comparative Law*, (Cambridge University Press, 2014).

D'Amato, A., *The Concept of Custom in International Law*, (Cornell University Press, 1971).

Darwin, J., 'Nationalism and Empire in the 1950s', pp 167 – 221, in *Britain and Decolonisation: The Retreat from Empire in the Post-War World, The Making of the 20th Century,* (Palgrave, 1988).

Deeb, M., *Syrian, Iran, and Hezbollah: The Unholy Alliance and Its War on Lebanon*, (Hoover Institution Press, 2013).

Dekker, I., 'Reconsidering the Legal Relevance of Structural Violence' in eds. De Waart, P. J. I. M., Denters, E. M. G., Schriver, N., *Reflections on International Law from the Low Countries*, (Martinus Nijhoff Publishers, 1998).

Delibasis, D., 'Cybersecurity and State Responsibility: Identifying a Due Diligence Standard for Prevention of Transboundary Threats', in Kulesza, J. and Balleste, R. ed. *Cybersecurity and Human Rights in the Age of Cyberveillance,* (Rowman & Littlefield, 2015), at p. 20.

Duffy, H., *The 'War on Terror' and the Framework of International Law*, (CUP, 2005).

Gardiner, R., *Treaty Interpretation*, (Oxford University Press, 2nd Ed, 2017).

Gray, C., "The Charter Limitations on the Use of Force: Theory and Practice", 86-91 in eds. Lowe et al., *The United Nations Security Council and War: The Evolution of Thought and Practice Since 1945*, (Oxford University Press, 2010).

Hafner, G., "The Definition of the Crime of Terrorism" in Nesi, G. ed, *International Cooperation in Counter-Terrorism: The United Nations and Regional Organisations in the Fight Against Terrorism*, (Ashgate, 2006).

Henkin, L., *How Nations Behave*, (Cambridge Polity Press,1979).

Higgins, R., "The General International Law of Terrorism", in Higgins, R. and Flory, M., *International Law and Terrorism* (London: Routledge, 1997).

Jennings, R., and Watts, A., *Oppenheim's International Law* (9th ed.) (Harlow: Longman, 1992) vol. 1.

Kelsen, H., *Collective Security Under International Law*, (Washington, DC, Naval War College, 1957) (New Jersey, Lawbook Exchange, 2011).

Klabbers, J., *International Law*, (Cambridge University Press, 2013).

Koskenniemi, M., 'The Place of Law in Collective Security', *Michigan Journal of International Law,* Vol. 17:455, (1996), in White, N., *Collective Security Law*, (Dartmouth, 2003).

Koskenniemi, M., *The Politics of International Law*, (Hart Publishing, 2011).

Kulesza, J., *Due Diligence in International Law*, Brill Nijhoff, 2016 (Queen Mary Studies in International Law, Vol. 26).

Lawler, P., *'*Peace Studies', in ed. Williams, P., *Security Studies: An Introduction* (Routledge, 2nd Ed, 2013).

Lowe, V., *International Law*, (Clarendon Law Series, 2007).

Lowe, V., Roberts, A., Welsh, J., Zaum, D., *The United Nations Security Council and War: The Evolution of Thought and Practice Since 1945*, (Oxford University Press, 2010).

Mani, V.S., 'The Role of Law and Legal Considerations in The Functioning of the United Nations', Indian Journal of International Law, 35, pp. 91-118, (1995) in White, N., *Collective Security Law*, (Dartmouth, 2003).

Moore, J. B., *Digest of International Law*, (Washington: Gov., Vol. 7, 1906).

Oppenheim, L. F., *Oppenheim's International Law*, Vol. 1: Peace, 3rd edn, Roxburgh, R.F. (ed.), London: Longmans (1920-21).

Orakhelashvili, A., *Collective Security*, (Oxford University Press, 2011).

Ratner, S., 'The Security Council and International Law', in Eds Malone, *The UN Security Council: From the Cold War to the 21st Century*, (Lynne Rienner Publishers, 2004).

Rapport, M., '*The French Revolution and Early European Revolutionary Terrorism'*, p.72, in ed Law, D. R., *The Routledge History of Terrorism,* Routledge (2015).

Ryngaert, C., "State Responsibility and Non-State Actors", in Noortmann, M., Reinisch, A. and Ryngaert, C. *Non-State Actors and International Law*, (Hart Publishing, 2015).

Saul, B., *Defining Terrorism in International Law*, (Oxford University Press, 2006).

Saul, B., and Heath, K., "Cyber Terrorism", in eds., Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace*, (Edward Elgar, 2015).

Schmitt, M., *Tallinn Manual on the International Law Applicable to Cyber Warfare 1.0*, (Cambridge University Press, 2013).

Schmitt, M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

Sender, O., and Wood, M., 'Custom's Bright Future: The Continuing Importance of Customary International Law', pp. 360 -370, in Curtis A. Bradley, *Custom's Future: International Law in a Changing World*, (Cambridge University Press, 2016).

Shaw, M., *International Law*, (Cambridge University Press, 6th Ed, 2008).

Tsagourias, N., and White, N., *Collective Security: Theory, Law and Practice*, (Cambridge University Press, 2013).

van Tigerstrom, B., *Human Security and International Law: Prospects and Problems*, (Hart Publishing, 2007).

Weimann, G., "The Emerging Role of Social Media in the Recruitment of Foreign Fighters", in ed. Capone, F., et al., *Foreign Fighters under International Law and Beyond*, T.M.C. Asser Press, (2016).

Weimann, G., *Terrorism in Cyberspace; The Next Generation*, (Columbia University Press, 2015).

White, N., *Democracy Goes to War: British Military Deployments Under International Law*, (OUP, 2009).

White, N., *Keeping the Peace*, (Manchester University Press, 1997).

White, N., 'The Relationship Between the UN Security Council and General Assembly in Matters of International Peace and Security', in ed. Weller, *The Use of Force in International Law* (Oxford University Press, 2015).

Wilkinson, P., "Terrorism", in ed. Cavelty, M. D., and Mauer, V., *The Routledge Handbook of Security Studies*, Routledge, (2010).

Wolfers, A., "National Security as an Ambiguous Symbol", in: Wolfers, Arnold (Ed.): *Discord and Collaboration. Essays on International Politics* (Baltimore: John Hopkins University Press): 147−165.

Wolfke, K., *Custom in Present International Law* (2nd ed.) (Martinus Nijhoff Publishers, 1993).

2.2 Journal Articles

Alfifi, M., Kaghazgaran, P., and Caverlee, J., and Morstatter, F., 'Measuring the Impact of ISIS Social Media Strategy', *Stanford Network Analysis Project* (2018).

Almohammad, A., 'ISIS Child Soldiers in Syria: The Structural and Predatory Recruitment, Enlistment, Pre-Training Indoctrination, Training, and Deployment', *ICT Research Paper*, February 2018.

Anderson, K., '"Cubs of the Caliphate" The Systematic Recruitment, Training and Use of Children in the Islamic State', *International Institute for Counter-Terrorism*, January 2016.

Argomaniz, J., 'European Union responses to terrorist use of the Internet', *Cooperation and Conflict* Vol. 50 (2), 250-268, (2015).

Awan, I. 'Cyber Extremism: ISIS and the Power of Social Media', *Social Science and Public Policy* 54: 138 – 149 (2017).

Banketas, E., 'Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight Against Terrorism', *The American Journal of International Law,* Vol/ 97, No.2 (Apr. 2003), pp. 333-34.

Bannelier-Christakis, K., 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', *Baltic Yearbook of International Law,* Vol. 14, (2014), pp. 23 – 29.

Barnidge, R., 'The Due Diligence Principle Under International Law', *International Community Law Review* 8: 81-121, (2006).

Baron, R. M. F., 'A Critique to the International Cybercrime Treaty', *Commlaw Conspectus*, Vol. 10, (2002).

Bianchi, A., 'Assessing the Effectiveness of the UN Security Council's Anti-Terrorism Measures: The Quest for Legitimacy and Cohesion', *The European Journal of International Law*, Vol. 17, No.5, EJIL 17, 881-919.

Biller, J.T., 'Cyber Terrorism: Finding a Common Starting Point', *Journal of Law, Technology & The Internet*, Vol. 4, No. 2, (2013).

Blaker, L., 'The Islamic State's Use of Online Social Media', *Military Cyber Affairs*, Vol. 1, Iss. 1, Article 4, (2015).

Blannin, P., 'Islamic State's Financing: Sources, Methods and Utilisation', *Counter Terrorist Trends and Analyses*, Vol. 9, No. 5 (May 2017), pp. 13 – 22.

Benotman, N., and Malik, N., 'The Children of Islamic State', *Quilliam International*, March 2016.

Bratpsies, R. M., and Miller, R. A., 'Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration', Bratpsies, R. M & Miller, R. A. eds., (Cambridge University Press, 2006); *Washington & Lee Legal Studies Paper* No. 2011-30 (23 January 2012).

Brenner, S., 'At Light Speed: Attribution and Response to Cybercrime/ Terrorism/ Warfare', *Journal of Criminal Law and Criminology*, Vol. 97, Issue 2, Winter, (2007).

Brenner, S., 'Cyberterrorism: How Real is the Threat?', *Media Asia*, 29:3, 149 -154 (2002).

Brent, K. A., 'The Certain Activities case: what implications for the no-harm rule?', *Asia Pacific Journal of Environmental Law*, Vol. 20, (2017), pp. 28 – 56.

Buchan, R., 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict and Law* 21 (3), pp. 429 – 453.

Buzan, B., 'Peace, Power and Security: Contending Concepts in the Study of International Relations', *Journal of Peace Research*, June 1984, Vol. 21, No. 2, Special Issue on Alternative Defense, pp. 109 – 125.

Carroll, P., and Windle, J., 'Cyber as an Enabler of Terrorism Financing, Now and in the Future', *Journal of Policing, Intelligence and Counter Terrorism*, 13:3, 285 – 300 (2018).

Charney, J. I., 'The Use of Force Against Terrorism and International Law', *The American Journal of International Law,* Vol. 95, No. 4, (Oct. 2001), pp. 835 – 839.

Cheng, B., 'United Nations Resolutions on Outer Space: "Instant" International Customary Law', 5 *Indian Journal of International Law* 23 (1965).

Cirkovic, E., 'Incomplete World Order: United Nations Security Council Resolution 2249 (2015) and the Use of Force in International Law', *Comparative Law Review*, Vol. 8, (2017).

Conway, M, 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism,* 40:1, 877-98, (2017).

Conway, M., 'Terrorism and the Internet: New Media – New Threat?' *Parliamentary Affairs*, Vol. 59, No. 2, 283-298, (2006).

Cook, J., and Vale, G., 'From Daesh to 'Diaspora': Tracing the Women and Minors of Islamic State', *International Centre for the Study of Radicalisation* (2018).

Cooper, W. H., 'The Dark Side of the Economy: A Comparative Analysis of the Islamic State's Revenue Streams', *Journal of Terrorism Research*, Vol. 8 (1), 34 – 42.

Corn, G., and Taylor, R., 'Sovereignty in Cyberspace', *AJIL Unbound*, Vol 111, (2017), pp. 207 – 212.

Couzigou, I., 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations', *International Review of Law, Computers & Technology*, 32:1, 37 – 57.

Crawford, E., 'From Inter-State and Symmetric and Intra-State and Asymmetric: Changing Methods of Warfare and the Law of Armed Conflict in the 100 Years Since World War One', *Yearbook of International Humanitarian Law*, Vol. 17, No. 2014, pp. 95 – 118 (2006), Sydney Law School Research Paper No. 16/44.

Dantiki, S., 'Power Through Process: An Administrative Law Framework for United Nations Legislative Resolutions', *40 Geo. J. Int'l L.* 655, (2009).

Darden, J. T., 'Tackling Terrorists' Exploitation of Youth', *American Enterprise Institute*, May 2019.

d'Aspremont, J. et al, 'Sharing Responsibility Between Non-State Actors and States in International Law: Introduction,' *Netherland International Law Review* 62:49-67, June 9, (2015).

Denning, D. E., 'Cyberterrorism: The Logic Bomb Versus the Truck Bomb', *Global Dialogue*, Oct. 2000.

Denning, D. E., 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', *Global Problem Solving Information Technology and Tools*, (Dec. 10, 1999).

Denning, D. E., 'Stuxnet: What Has Changed?', *Future Internet*, 4, 627 – 687 (2012).

Dinniss, H., 'The Threat of Cyber Terrorism and What International Law Should (Try To) Do About It', *Georgetown Journal of International Affairs,* Vol. 19 (Fall 2018), pp. 43 – 50.

Dion-Schwarz, C., Manheim, D., Johnson, P. B., 'Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats', *RAND Corporation* (2019).

Droogan, J., and Peattie, S., 'Reading Jihad: Mapping the Shifting Themes od Inspire Magazine', *Terrorism and Political Violence*, 30:4, 684 – 717.

Elberling,B., 'The Ultra Vires Character of Legislative Action by the Security Council', *International Organisations Law Review* 2: 337-360, (2005).

Ette, M., and Joe, S., 'Rival Visions of Reality': An Analysis of the Framing of Boko Haram in Nigerian Newspapers and Twitter', *Media War & Conflict 11* (4): 392 – 406, (December 2018).

Fidler, D., Buchan, R., and Crawford, R., 'ILA Study Group Report on Cybersecurity, Terrorism and International Law,' *International Law Association* (July 31, 2016).

Fidler, D., 'Cyberspace, Terrorism and International Law', *Journal of Conflict & Security Law,* Vol. 21, No.3, 475-493, (2016).

Fidler, D., 'Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection', *16 Georgetown Journal of International Affairs 8* (2015) Special Issue.

Fox, G. H., Boon, K., and Jenkins, I., 'The Contributions of United Nations Security Council Resolutions to the Law of Non-International Armed Conflict: New Evidence of Customary International Law,' *American University Law Review*: Vol. 67: Iss. 3, Article 1, (2018).

Galtung, J., 'An Editorial', *Journal of Peace Research* (1964), 1(1): 1-4.

Galtung, J., 'Theory and Practice of Security'*, Instant Research on Peace and Violence*, 1972, Vol. 2, No. 3, European Co-operations (1972), pp. 109 – 112, *International Peace Research Institute*, Oslo.

Galtung, J., 'Violence, Peace and Peace Research', 6 *Journal of Peace Research* (1969).

de la serna Galván, M. L., 'Interpretation of Article 39 of the UN Charter (Threat to the Peace) by the Security Council. Is the Security Council a Legislator for the Entire International Community?', *Anuario Maxicano de Derecho Internacional*, vol. XI, 2011, pp. 147 – 185.

Gehring, T., and Jachtenfuchs, M., 'Liability for Transboundary Environmental Damage Towards a General Liability Regime?', 4 *EJIL* 92-106 (1993).

Giantas, D., and Stergiou, D., 'From Terrorism to Cyber-Terrorism: The Case of ISIS', *Hellenic Institute of Strategic Studies*, (March 7, 2018).

Gill, P, Horgan, J., and Deckert, P., 'Bombing Alone: Tracing the Motivations and Antecedent Behaviours of Lone-Actor Terrorists', *Journal of Forensic Sciences*, March 2014, Vol. 59, No. 2.

Gillett, M., and Schuster, M., 'Fast-track Justice: The Special Tribunal for Lebanon Defines Terrorism', *Journal of International Criminal Justice* 9 (2011), 989 – 1020.

Hakmeh, J., 'Cybercrime and the Digital Economy in the GCC Countries', *International Security Department Research Paper,* Chatham House, June 2017.

Harper, K., 'Does the United Nations Security Council Have the Competence to Act as Court and Legislature?', *New York University Journal of International Law and Politics*, 27, (1994) pp. 103-157.

Heickerö, R., 'Cyber Terrorism: Electronic Jihad', *Strategic Analysis,* Vol. 38, 38:4, 554-565, (2014).

Hessbruegge, J. A., 'The Historical Development of the Doctrines of Attribution and Due Diligence in International Law', 36 *NYU Journal of Int'l L. & Pol.* 265 (2004).

Higgins, R., 'The Advisory Opinion on Namibia: Which UN Resolutions Are Binding Under Article 25 of the Charter?' *The International & Comparative Law Quarterly,* Vol. 21, No. 2, (April. 1972) pp. 270 – 286.

Hilpold, P., 'The Fight Against Terrorism and SC Resolution 2249 (2015): Towards a More Hobbesian or a More Kantian International Society?' *Indian Journal of International Law* (2015) 55 (4): 535 – 555.

Horbach, N., 'The Confusion about State Responsibility and International Liability', *Leiden Journal of International Law*, Vol. 4, No. 1, (April, 1991).

Hurd, I. 'The UN Security Council and the International Rule of Law', *The Chinese Journal of International Politics*, 361-379 (2014).

Hutchinson, T., 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law', *Erasmus Law Review* Vol. 8 No.3, (Dec 2015).

Jacobson, M., 'Terrorist Financing and The Internet', *Studies in Conflict & Terrorism*, 33:4, 353-363 (2010).

Jenkins, B. M., 'The New Age of Terrorism', in Brian Michael Jenkins (ed.), McGraw-Hill Homeland Security Handbook (RAND, 2006).

Jensen, E. T., and Watts, S., 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', *Texas Law Review*, Vol. 95: 1555 -1577 (2017).

Johnstone, I., 'Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit', 102 *Am. J. Int'l L*. 275 (2008).

Jones, S., Liepman, A., and Chandler, N., 'Counterterrorism and Counterinsurgency in Somalia: Assessing the Campaign Against Al Shabaab', *RAND Corporation* (2016).

Keene, D. S. 'Terrorism and the Internet: A Double-Edged Sword', *Journal of Money Laundering Control*, Vol. 14, Issue 4, pp. 359-370, (2011).

Kelsen, H., 'The Principle of Sovereign Equality of States as a Basis for International Organisation', *The Yale Law Journal*, (Vol. 53, No.2, March 1944) pp. 207-220.

Kierkegaard, S. M., 'Cracking Down on Cybercrime Global Response: The Cybercrime Convention', *Communications of the IIMA*: Vol. 5, Iss. 1, Article 7 (2005).

Koh, H. H., 'Why Do Nations Obey International Law?', *The Yale Law Journal*, Vol. 106, No. 8, (June 1997) pp. 2599-1659.

Kopelmanas, L., 'Customs as a Means of the Creation of International Law, 18 *British Yearbook of International Law* 127 (1937).

Kruglanski, A. W., Gunaratna, R., Ellenberg, M., & Speckhard, A., 'Terrorism in time of the pandemic: Exploiting Mayhem,' *Global Security: Health, Science and Policy*, 5:1, 121-132 (2020).

Lauterpacht, H., 'Revolutionary Activities by Private Persons Against Foreign States', *The American Journal of International Law,* Vol. 22, No. 1 (Jan. 1928), pp. 105 – 130.

Lentz, C. E., 'A Study's Duty to Prevent and Respond to Cyberterrorist Acts', *Chicago Journal of International Law,* Vol. 10, No.2, (2010).

Liu, I. Y., 'The Due Diligence Doctrine under Tallinn Manual 2.0', *Computer Law and Security Review* 33, 390-395 (2017).

Lotrionte, C., 'State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights', 26 *Emory Int'l L. Rev.* 825 (2012).

Lubell, N., 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' *89 Int'l L. Stud. 252* (2013).

Mačák, K., 'Is the International Law of Cyber Security in Crisis?', 8th Int'l Conference on Cyber Conflict, *NATO CCD COE Publications*, (2016).

Maçak, K., 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers', *Leiden Journal of International Law* (2017), 30, pp. 877-899.

Macdonald, S., Correia, S. G., Watkin, A., 'Regulating Terrorist Content on Social Media: Automation and the Rule of Law', *International Journal of Law in Context,* Vol. 15, 183 – 197 (2015).

Madriz, E., 'Terrorism and Structural violence', *Social Justice, Vol. 28, No. 3 (85), Law, Order, and Neoliberalism*, (Fall 2001) pp. 45 – 46.

McDonald, N., 'The Role of Due Diligence in International Law', *International and Comparative Law Quarterly* 68 (4): 1041 – 1054, October 2019.

McKendrick, K., 'Artificial Intelligence Prediction and Counterterrorism', *Chatham House Research Paper* International Security Department (August 2019).

Menkhaus, K., 'Al-Shabaab and Social Media" A Double-Edged Sword', *The Brown Journal of World Affairs*, Vol. 20, No. 2 (Spring/Summer 2014), pp. 309 – 327.

Merrills, J. G., 'Two Approaches to Treaty Interpretation', 57 *Australian Yearbook of International Law* (1968).

Milton, D., 'Fatal Attraction: Explaining Variation in the Attractiveness of Islamic State Propaganda', *Conflict Management and Peace Science* 1 – 21 (2018).

Minei, E., and Matsuitz, J., 'Cyberspace as a New Arena for Terroristic Propaganda: An Updated Examination', Poiesis Prax (2012) 9:163 -176.

Morris, J., and Wheeler, N. J., 'The Security Council's Crisis of Legitimacy and the Use of Force', *International Politics,* Vol. 44, Iss. 2-3, pp. 214 – 231 (March 2007).

Moynihan, H., 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention', *Chatham House Research Paper*, December 2019.

O'Connell, M. E., 'Enhancing the Status of Non-State Actors Through a Global War on Terror?', *43 Columbia Journal of Transnational Law* 435 (2004-2005).

O'Connell, M. E., 'Unlawful Killing with Combat Drones: A Case Study of Pakistan, in 'Shooting to Kill: The Law Governing Lethal Force in Context', in Simon Bronitt ed., forthcoming 2010, *Notre Dame Legal Studies Research Paper* No. 09-43, (Nov. 2009).

Öberg, M. D., 'The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ', *EJIL* Vol. 16 No. 5, 2006.

Ogbondah, C. W., and Agbese, P. O., 'Terrorists and Social Media Messages: A Critical Analysis of Boko Haram's Messages and Messaging Techniques', *The Palgrave Handbook of Media and Communication Research in Africa*: 313 – 345, Oct 24. 2017.

Papastavridis,E., 'Interpretation of Security Resolutions under Chapter VII in the Aftermath of the Iraqi Crisis', *The International and Comparative Law Quarterly*, Vol. 56, No. 1 (Jan., 2007), pp. 83-118.

Partan, D., 'The Duty to Inform in International Environmental Law', *Boston University International Law Journal*, 6 (1), 43-88.

Paust, J. J., 'Self-Defence Targetings of Non-State Actors and the Permissibility of U.S. Use of Drones in Pakistan', *Journal of Transitional Law and Policy*, Vol. 19 (2), (2010).

Pisillo-Mazzeschi, R., 'The Due Diligence Rule and the Nature of the International Responsibility of States', in *German Yearbook of International Law,* Vol. 35, edited by Delbrück, Joel and Wolfrum, Rüdiger, Duncker & Humblot GmbH, 1992, Berlin Germany.

Pearce, D., Campbell, E., and Harding, D., 'Categorizing Legal Research', *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission,* (1987).

Plachta, M., 'The Lockerbie Case: The Role of the Security Council in Enforcing the Principle Aut Dedere Aut Judicare', *EJIL* Vol. 12 No. 1, 125-140 (2001).

Plakokefalos, I., 'Prevention Obligations in International Environmental Law', *Yearbook of International Environmental Law*, Forthcoming Amsterdam Law School Research Paper No. 2013 – 37 (July 5, 2013).

Proulx, V. J., 'Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?', *Berkeley Journal of International Law*, Vol. 23:3, 2005, at p. 106 – 153.

Rediker, E., 'The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union', *Michigan Journal of International Law,* Vol. 36, Iss. 2 (2015).

Redmond, S., et al, 'Who Watches an ISIS Beheading – and Why', *American Psychologist,* Vol. 74, No. 5, 555 – 568 (2019).

Rosand, E., 'The Security Council as "Global Legislator": Ultra Vires or Ultra Innovative?', 28 *Fordham Int'l LJ*. 542 (2004).

Rudner, M. '"Electronic Jihad": The internet as Al-Qaeda's Catalyst for Global Terror'*, Studies in Conflict and Terrorism*, (2016).

Ryngaert, C., 'Non-State Actors: Carving Out a Space in a State-Centred International Legal System', *Netherlands International Law Review* 63: 183-195 (2016).

Scanlon, J. R., and S. Gerber, M. S., 'Automatic Detection of Cyber-Recruitment by Violent Extremists', *Security Informatics*, 3:5 (2014).

Scharf, M. P., 'How the War Against ISIS Changed International Law', *Case Western Reserve Journal of Int'l Law 48*, (2016).

Schmitt, M., Grey Zones in the International Law of Cyberspace, *42 Yale J. of Int'l L. Online 1*, 4 (2017).

Schmitt, M., 'In Defense of Due Diligence in Cyberspace', *Yale Law Forum* 68 (2015).

Schmitt, M., 'The Law of Cyber Warfare: Quo Vadis?', *Stanford Law & Policy Review*, Vol. 25: 269, (2014).

Schmitt, M., and Watts, S., 'Beyond State-Centrism: International Law and Non-State Actors in Cyberspace', *Journal of Conflict & Security Law (*2016), 1 – 17.

Schott, J., 'Chapter VII as Exception: Security Council Action and the Regulative Ideal of Emergency,' *Northwestern Journal of International Human Rights*, Vol. 6, Issue. 1, (2007).

Schwebel, S. M., 'The Effect of Resolutions of the UN General Assembly on Customary International Law', *Proceedings of the Annual Meeting, ASIL,* Vol. 73 April 26-28, 1979 (pp. 301-309).

Schott, J., 'Chapter VII as Exception: Security Council Action and the Regulative Ideal of Emergency', 6 *Nw. J. Int'l Hum. Rts.* 24 (2008).

Schweitzer, Y., Siboni, G. and Yogev, E. 'Cyberspace and Terrorist Organisations', *Military and Strategic Affairs,* Vol. 3, No. 3, (December 2011).

Shackelford, S. J., Russell, S., Kuehn, A., 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors', *Chicago Journal of Int'l Law*: Vol 17, No. 1, Article 1 (2016).

Shackelford, S., 'The Law of Cyber Peace,' *Chicago Journal of International Law*, (2017).

Sloan, F. B., 'The Binding Force of a Recommendation of the General Assembly of the United Nations', *25 Brit. Y.B. Int'l L.1* (1948).

Smart, W., 'Lessons Learned Review of the WannaCry Ransomware Cyber Attack', *Department of Health & Social Care, NHS England Report* (February 2018).

Smith, S. A., Note, 'What is Old is New Again: Terrorism and the Growing Need to Revisit the Prohibition on Propaganda, *37 Syracuse J. Int'l L. Com*. 299, 303 (2010).

Smits, J., 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research', *M-EPLI Working Paper*, No. 2015/06, (Sept. 2015).

Spencer, A. N., 'The Hidden Face of Terrorism: An Analysis of Women in Islamic State', *Journal of Strategic Security* Vol. 9, No. 3, Special Issue: Emerging Threats (Fall 2016), pp. 74-98.

Springer, V., Lalasz, C., Lykes, V., 'Social Action in Response to Terrorism: Understanding Xenophobic Violence from a Value-Added Perspective', *The Social Science Journal Vol. 49*, Iss. 2, June 2012, pp. 175 -182.

Stephens, T., and French, D., 'ILA Study Group on Due Diligence in International Law,' *International Law Association* First Report, 7 March 2014.

Stephens, T., and French, D., 'ILA Study Group on Due Diligence in International Law', *International Law Association,* Second Report, (July 2016).

Stokes, P., 'State Responsibility for Cyber Operations: International Law Issues', Event Report, *British Institute of International and Comparative Law*, October 9, 2014

Stromseth, J. E., 'An Imperial Security Council? Implementing Security Council Resolutions 1373 and 1390', *97 American Society of International Law Proceedings* 41 – 54 (2003).

Sucharitkul, S., 'State Responsibility and International Liability Under International Law', *18 Loyola of Los Angeles Int'l & Comp. L. J.* 821 (1996).

Sullivan, C., 'The 2014 Sony Hack and the Role of International Law', 8 *Journal of National Security Law & Policy 437* (2016).

Takano, A., 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications', *MDPI Laws* 2018, 7, 36.

Talmon, S., 'The Security Council as World Legislature', *American Journal of International Law*, Vol. 99:175, (2005).

Tams, C. J., 'The Use of Force Against Terrorists', *European Journal of International Law* (2009), Vol. 20, No. 2, 359 – 397.

Trapp, K., 'Shared Responsibility and Non-State Terrorist Actors', *Neth. Int. Law Review* 62: 141 – 160, (2015).

Tsagourias, N., 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace', *EJIL:Talk!* (August 26, 2019).

Tsagourias, N., 'Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace', *ESIL Reflections* Vol. 9, Issue 4 (December 17, 2020).

Tsagourias, N., 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', *Journal of Conflict and Security Law*, Vol 21 Iss. 3, 1 Dec 2016 p. 455-474.

Tsagourias, N., 'Security Council Legislation, Article 2 (7) of the UN Charter, and the Principle of Subsidiarity', *Leiden Journal of International Law*, 24 (2011), pp.539-559

Vale, G., 'Cubs in the Lions' Den: Indoctrination and Recruitment of Children Within Islamic State Territory', *International Centre for the Study of Radicalisation* (2018).

Väljataga, A., 'Tracing Opinio Juris in National Cyber Security Strategy Documents', *NATO CCDCOE*, Tallinn 2018.

Van Ginkel, B., 'Incitement to Terrorism: A Matter of Prevention or Repression?', *International Center for Counter-Terrorism Research Paper* 3 (August 2, 2011).

Walker, C., and Conway, M., 'Online Terrorism and Online Laws', *Dynamics of Asymmetric Conflict*, 8:2, 156-175, (2015).

Weber, A., 'The Council of Europe's Convention on Cybercrime', *Berkeley Technology Law Journal*, Vol. 18, Issue 1, (2003).

Weil, P., 'Towards Relative Normativity in International Law?', *The American Journal in International Law*, Vol. 77, No. 3, (July 1983) pp. 413-422.

Weimann, G., 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict & Terrorism*, 28: 129 – 149, (2005).

Weimann, G., 'Cyberterrorism: How Real is the Threat?', *United States Institute of Peace Special Report* 119 (December 2004).

Weimann, G., 'Virtual Disputes: The Use of the Internet for Terrorist Debates', *Studies in Conflict & Terrorism*, 29: 623 – 639 (2006).

Weimann, G. 'www.terror.net How Modern Terrorism Uses the Internet', *United States Institute of Peace Special Report 116*, (March 2004).

Weimann, G. and Masri, N., 'Research Note: Spreading Hate on TikTok', *Studies in Conflict & Terrorism* (2020).

White, N., 'Preventive Counter-Terrorism and International Law', *Journal of Conflict and Security Law*, Vol. 18, No. 2, 181-192, (2013).

Whittle, D., 'The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action', *European Journal of International Law*, Vol. 26, Iss. 3, August 2015, pp. 671 – 691.

Welch, T., 'Theology, Heroism, Justice, and Fear: An Analysis of ISIS Propaganda Magazines Dabiq and Rumiyah', *Dynamics of Asymmetric Conflict*, 11:3, 186 – 198, at p. 193 – 194.

Wu, P., 'Impossible to Regulate: Social Media, Terrorists, and the Role for the U.N.'*, Chicago Journal of International Law*, Vol. 16, No. 1, Article 11, (2015).

Yilmaz, M. E., 'Intra-State Conflicts in the Post-Cold War Era', *International Journal on World Peace,* Vol. 24, No. 4, (December 2007), pp. 11- 33.

2.3 Online Sources

Abu Amru Al Qa'idy, 'A Course in the Art of Recruiting – Revised July2010' available at https://archive.org/stream/ACourseInTheArtOfRecruiting-RevisedJuly2010/A_Course_in_the_Art_of_Recruiting_-_Revised_July2010_djvu.txt (accessed 1 May 2017).

Adams, M. J., and Reiss, M., 'How Should International Law Treat Cyberattacks like WannaCry?', *Lawfare Blog,* (22 December 2017). Available at https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry (accessed 1 July 2020).

Akand, D., and Milanovic, M.,'The Constructive Ambiguity of the Security Council's ISIS Resolution', *EJIL: Talk!: Blog of the Eur. J. Intl'l L.*, (November 21, 2015) available at https://www.ejiltalk.org/the-constructive-ambiguity-of-the-security-councils-isis-resolution/.

Aoláin, F., 'A Post-Morten on UN Security Council Resolution 2482 on Organized Crime and Counter-Terrorism', *Just Security* (August 12, 2019). Available at https://www.justsecurity.org/65777/a-post-mortem-on-un-security-council-resolution-2482-on-organized-crime-and-counter-terrorism/ (accessed 4 April 2020).

Australia International Cyber Engagement Strategy, Annex A: Application of International Law in Cyberspace (2017) available at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html (accessed 19 November, 2019).

BBC News, 'Estonia Hit by 'Moscow Cyber War', (May 17, 2007). Available at http://news.bbc.co.uk/1/hi/world/europe/6665145.stm (accessed 22 June 2018).

BBC News, 'IS 'Caliphate' Defeated but Jihadist Group Remains a Threat', (March 23, 2019), available at https://www.bbc.co.uk/news/world-middle-east-45547595 (accessed 2 June 2018).

BBC News, 'Islamic State and the Crisis in Iraq and Syria in Maps' (21 September 2017). Available at http://www.bbc.co.uk/news/world-middle-east-27838034 (accessed 28 September 2017).

BBC News Online, 'Manchester Attack: What We Know So Far', June 2, 2017. Available at https://www.bbc.co.uk/news/uk-england-manchester-40008389 (accessed May 1, 2020).

BBC News,, 'NHS Cyber-Attack: GPs and Hospitals Hit by Ransomware', 13 May 2017. Available at https://www.bbc.co.uk/news/health-39899646 (accessed 3 March 2020).

BBC News Online, 'Paris Attacks: What Happened on the Night', December 9, 2015. Available at https://www.bbc.co.uk/news/world-europe-34818994 (accessed May 1, 2020).

BBC News, 'PlayStation Outage Caused by Hacking Attack', 25 April 2011. Available at https://www.bbc.co.uk/news/technology-13169518 (accessed 3 March 2020).

BBC News, 'Stuxnet 'Hit' Iran Nuclear Plans', (22 November 2010). Available at https://www.bbc.co.uk/news/technology-11809827 (accessed 3 March 2020).

BBC News, 'Syria: The Story of the Conflict', (11 March 2016). Available at http://www.bbc.co.uk/news/world-middle-east-26116868 (accessed 28 September 2017).

BBC News, 'Syria War: New US Sanctions Target Assad Government's Foreign Backers', (17 June 2020). Available at https://www.bbc.co.uk/news/world-middle-east-53076994 (accessed 7 July 2020).

Berger, J. M., 'How ISIS Games Twitter', *The Atlantic* (2014), available at https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

Bloom, M., 'How Terrorist Groups Will Try to Capitalise on the Coronavirus Crisis', *Just Security*, 3 April 2020. Available at https://www.justsecurity.org/69508/how-terrorist-groups-will-try-to-capitalize-on-the-coronavirus-crisis/ (accessed 16 September 2020).

Carlin, J. P., 'Inside the Hunt for the World' Most Dangerous Terrorist: How a British Hacker Joined ISIS's Top Ranks and Launched A Deadly Global Cyber Plot', *Politico Magazine*, (21 November 2018) available at https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643

Counter Extremism Project, 'Infamous ISIS Bomb-Making Video Located on Several Sites', April 17, 2019. Available at https://www.counterextremism.com/blog/infamous-isis-bomb-making-video-located-several-sites (accessed 16 September 2020).

Counterextremism Project, Junaid Hussain, available at https://www.counterextremism.com/extremists/junaid-hussain.

Dabiq, 1437 Safar, 'Terror', Issue 12 at p. 43. Available at http://clarionproject.org/wp-content/uploads/islamic-state-isis-isil-dabiq-magazine-issue-12-just-terror.pdf (accessed 15 February 2017).

Dabiq, 1437 Shawwal, 'Break the Cross', Issue 15 at p. 25 available at http://clarionproject.org/wp-content/uploads/islamic-state-magazine-dabiq-fifteen-breaking-the-cross.pdf (accessed 15 February 2017).

Denning, D.E., "Cyberterrorism", Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives (May 23, 2000). Available at https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm (accessed 3 June 2020).

Dodd, V., et al., 'At Least 22 Killed, 59 Injured in Suicide Attack at Manchester Arena', *The Guardian*, May 23, 2017. Available at https://www.theguardian.com/uk-news/2017/may/22/manchester-arena-police-explosion-ariana-grande-concert-england (accessed May 1, 2020).

Don, B. W., Frelinger, D. R., Gerwehr, S., Landree, E., and Jackson, B. A., 'Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations,' Santa Monica, CA: RAND Corporation, 2007. Available at https://www.rand.org/pubs/technical_reports/TR454.html

EUROPOL, 'Europol and Telegram take on Terrorist Propaganda Online', Press Release (25 November 2019). Available at https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online (accessed 5 August 2020).

Fidler, D., 'Terrorism, the Internet, and the Islamic State's Defeat: It's Over, But It's Not Over', *Council on Foreign Relations* (November 28, 2017). Available at https://www.cfr.org/blog/terrorism-internet-and-islamic-states-defeat-its-over-its-not-over (accessed 17 August 2019).

Finnish Government Ministry for Foreign Affairs, 'Finland published its positions on public international law in cyberspace', 15 October 2020. Available at https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace (accessed 21 January 2021).

François Delerue, Aude Géry, “France's Cyberdefense Strategic Review and International Law, Lawfare”, 23 March 2018, available at https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law (accessed 18 November, 2019).

Finnish Government, ‘International law and cyberspace: Finland’s national positions’, 15 October 2020. Available at https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 (accessed 21 January 2021).

The Guardian Online, Quinn, B., and Arthur, C., ‘PlayStation Network Hackers Access Data of 77 Million Users’, 26 April 2011. Available at https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data (accessed 3 March 2020).

Government of the Netherlands, ‘Appendix: International law in cyberspace’, 26 September 2019. Available at https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (accessed 7 January, 2020).

Guerin, O., ‘ISIS in Iraq: Militants ‘Getting Stronger Again’, *BBC News Online,* December 23, 2019. Available at https://www.bbc.co.uk/news/world-middle-east-50850325 (accessed May 1, 2020).

Heisig, E., ‘Ohio Jury Finds Man Guilty of Trying to Create ISIS-inspired Terrorist Cell in U.S.’, Cleveland Online, (March 20, 2018) available at https://www.cleveland.com/court-justice/2018/03/ohio_jury_finds_man_guilty_of.html (accessed 4 June 2018).

Hern, A., and Gibbs, S., ‘What is WannaCry Ransomware and Why Is It Attacking Global Computers?’, The Guardian Online, 12 May 2017. Available at https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20 (accessed 3 March 2020).

Hincks, J., ‘With the World Busy Fighting COVID-19, Could ISIS Mount A Resurgence?’, *Time Online*, April 29, 2020. Available at https://time.com/5828630/isis-coronavirus/ (accessed May 1, 2020).

Hosenball, M., ‘British Hacker Linked to Attack On Pentagon Twitter Feed: Sources’, *Reuters*, (January 14, 2015), available at https://www.reuters.com/article/us-cybersecurity-pentagon-cybercaliphate/british-hacker-linked-to-attack-on-pentagon-twitter-feed-sources-idUSKBN0KN00X20150114

Inspire, ‘Shattered: A Story About Change’, (Issue 12, Spring 2014) at p. 32. Available at https://azelin.files.wordpress.com/2014/04/inspire-magazine-issue-12.pdf (accessed 2 May 2017).

Institute for Economics and Peace, ‘Positive Peace Report 2015: Conceptualising and Measuring the Attitudes, Institutions and Structures That Build A More Peaceful Society’*, Vision of Humanity* (2015). Available at http://visionofhumanity.org/app/uploads/2017/04/Positive-Peace-Report-2015.pdf (accessed 21 August 2020).

International Crisis Group, ‘COVID-19 and Conflict: Seven Trends to Watch’, Special Briefing No. 4 (24 March 2020). Available at https://www.crisisgroup.org/global/sb4-covid-19-and-conflict-seven-trends-watch (accessed 11 February 2021).

The Investigative Project on Terrorism, Sentencing Press Release, 'North Carolina Man Convicted of Attempting and Conspiring to Provide Material Support to ISIS', (February 4, 2019) available at https://www.investigativeproject.org/documents/case_docs/3895.pdf (accessed 4 June 2018).

Joyner, D., 'Legal Bindingness of Security Council Resolutions Generally, and Resolution 2334 on the Israeli Settlements in Particular,' *EJIL: Talk!: Blog of the Eur. J. Intl'l L.*, (January 9, 2017) available at https://www.ejiltalk.org/legal-bindingness-of-security-council-resolutions-generally-and-resolution-2334-on-the-israeli-settlements-in-particular/

Lexico Oxford Dictionary. Available at https://www.lexico.com/

Lister, C., 'The Growing Threat of ISIS in Syria's Badia', *Middle Eastern Institute*, 17 April 2020. Available at https://www.mei.edu/publications/growing-threat-isis-syrias-badia (accessed 23 September 2020).

Mallet, V., and Chilkoti, A., 'How Cyber Criminals Targeted Almost $1bn in Bangladesh Bank Heist', *The Financial Times Online*, (March 18, 2016) available at https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8 (accessed 23 May 2018).

Morgan, W., 'Pentagon Sees Few Options for Preventing New ISIS Safe Haven in Syria', *Politico Online* ,19 October 2019. Available at https://www.politico.com/news/2019/10/19/pentagon-isis-syria-051369 (accessed 23 September 2020).

Morris, N., 'ISIS Video 'Showing British Child Blowing Up Car With Prisoners Inside' Shows Jihadists are in Retreat, says PM', *The Independent*, 11 February 2016. Available at https://www.independent.co.uk/news/uk/home-news/isis-video-showing-british-child-blowing-up-car-with-prisoners-inside-shows-jihadists-are-under-a6867131.html (accessed 18 March 2020).

National Audit Office, 'Investigation: WannaCry Cyberattack and the NHS', *NAO Department of Health* (25 April 2018).

de Freytas-Tamura, K., 'Junaid Hussain, ISIS Recruiter, Reported Killed in Airstrike', *The New York Times*, (August 27, 2015) available at https://www.nytimes.com/2015/08/28/world/middleeast/junaid-hussain-islamic-state-recruiter-killed.html

New Zealand Department of the Prime Minister and Cabinet, 'The Application of International Law to State Activity in Cyberspace', 1 December 2020. Available at https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf (accessed 21 January 2021).

Nournews, General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat, (18 August 2020). Available at https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat (accessed 25 February 2021).

Oosthuizen, G. and Wilmshurst, E., 'Terrorism and Weapons of Mass Destruction: United Nations Security Council Resolution 1540', *Chatham House International Law Programme Briefing Paper* (Sept. 2004) at p. 3, available at https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/ILP0904bp.pdf

Perlroth, N., Tsang, A., and Satariano, A., 'Marriott Hacking Exposes Data of up to 500 Million Guests', *The New York Times* (Nov.30, 2018), available at https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (accessed 22 July 2020).

Phipps, C. and Rawlinson, K., 'Paris Attacks Kill More Than 120 People – As It Happened', *The Guardian Online*, November 14, 2015. Available at https://www.theguardian.com/world/live/2015/nov/13/shootings-reported-in-eastern-paris-live (accessed May 1, 2020).

President of Estonia, 'President of the Republic at the Opening of CyCon 2019', 29 May 2019. Available at https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/ (accessed 7 January 2020).

Rayner, G., ''Jihadi Junior' Confirmed to be Isa Dare, son of female British fanatic with links to Lee Rigby killers', *The Telegraph*, 4 January 2016. Available at https://www.telegraph.co.uk/news/worldnews/islamic-state/12080134/Jihadi-Junior-son-of-female-British-fanatic-with-links-to-Lee-Rigby-killers.html (accessed 18 March 2020).

Republique Française Ministère Des Armées, Droit International appliqué aux operations dans le cyberspace, 9 September 2019. Available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf (accessed 18 November, 2019).

Roguski, P., 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I', *Opinio Juris*, 24 September 2019, available at https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed 18 November, 2019).

Rumiyah Sha'ban 1438, 'The Ruling on the Belligerent Christians', Issue 9, available at https://qb5cc3pam3y2ad0tm1zxuhho-wpengine.netdna-ssl.com/wp-content/uploads/2017/05/Rumiyah-9.pdf (accessed 15 February 2017).

Rumiyah, Issue 2, Muharram 1438. Available at http://clarionproject.org/wp-content/uploads/Rumiyh-ISIS-Magazine-2nd-issue.pdf (accessed 16 February 2017).

The Economist Online, 'Internet Jihad: A World Wide Web of Terror', (July 12, 2007) available at https://www.economist.com/briefing/2007/07/12/a-world-wide-web-of-terror (accessed 9 June 2018).

Robertson, A., 'TikTok Removes Two Dozen ISIS Propaganda Accounts', *The Verge Online*, (21 October 2019). Available at https://www.theverge.com/2019/10/21/20925416/tiktok-islamic-state-terrorist-propaganda-recruitment-account-videos (accessed 14 August 2020).

Sabbagh, D., 'MI5 Chief Asks Tech Firms for 'Exceptional Access' to Encrypted Messages', *The Guardian Online*, 25 February 2020. Available at https://www.theguardian.com/uk-news/2020/feb/25/mi5-chief-asks-tech-firms-for-exceptional-access-to-encrypted-messages (accessed 25 Feb 2020).

Safi, M. and Chulov, M., 'Abu Bakr al-Baghdadi Killed in US Raid, Trump Confirms', *The Guardian Online*, October 27, 2019. Available at https://www.theguardian.com/world/2019/oct/27/abu-bakr-al-baghdadi-isis-leader-killed-us-donald-trump (accessed May 1, 2020).

Schmitt, M., and Fahey, S., 'WannaCry and the International Law of Cyberspace', *Just Security* (December 22, 2017). Available at https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/ (accessed 1 July 2020).

Schmitt, M., 'France's Major Statement on International Law and Cyber Assessment: Use of Force, Sovereignty and More', *Just Security* (16 September 2019). Available at https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/ (accessed 18 November, 2019).

Schmitt, M., 'International Law and Cyber Attacks: Sony v. North Korea', *Just Security* (17 December 2014). Available at https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (accessed 13 July 2020).

Schreier, J., 'Sony Estimates $171 Million Loss from PSN Hack', *Wired*, 23 May 2011. Available at https://www.wired.com/2011/05/sony-psn-hack-losses/ (accessed 3 March 2020).

Shead, S., 'TikTok Used by Islamic State to Spread Propaganda Videos', *BBC News*, (22 October 2019). Available at https://www.bbc.co.uk/news/technology-50138740 (accessed 14 August 2020).

Silva, S., 'Islamic States: Giant Library of Group's Online Propaganda Discovered', *BBC News*, 3 September 2020. Available at https://www.bbc.co.uk/news/technology-54011034 (accessed 3 September, 2020).

Sommers, J., 'Islamic State Propaganda Video Shows British Boy, believed to be Isa Dare, Blowing Up 'Car of Spies', *The Huffington Post UK*, 11 February 2016. Available at https://www.huffingtonpost.co.uk/2016/02/11/islamic-state-propaganda-isa-dare_n_9207036.html (accessed 18 March 2020).

The Telegraph, 'Georgia: Russia 'Conducting Cyber War', (Aug., 11, 2008), available at https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

United Nations Human Rights Office of the Commissioner, 'Counter-Terrorism Measures are Exacerbating Racism and Xenophobia, UN Rights Expert Warns', (31 October 2017) available at https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=22332&LangID=E

United Nations website, 'UN Documentation: Overview', last updated May 20, 2021. Available at https://research.un.org/en/docs/pressreleases (accessed 8 July 2021).

UNODC Website, 'Countering The Use of the Internet For Terrorist Purposes', available at https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html

The United States Department of Justice, Department of Justice Office of Public Affairs, 'North Carolina Man Convicted of Attempting and Conspiring to Provide Material Support to ISIS', Press Release Number 18-336 (March 20, 2018) available at https://www.justice.gov/opa/pr/north-carolina-man-convicted-attempting-and-conspiring-provide-material-support-isis (accessed 4 June 2018).

The Washington Post Online, Krebs, 'Terrorism's Hook Into Your Inbox', (July 5, 2007) available at http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html??noredirect=on (13 June 2018).

Weaver, M., Siddique, H., Jalabi, R., and Phipps, C., 'Brussels: Islamic State Launches Attack on Airport and Station – As It Happened', *The Guardian Online,* March 23, 2016. Available at https://www.theguardian.com/world/live/2016/mar/22/brussels-airport-explosions-live-updates (accessed 1 May, 2020).

The White House National Strategy for Counterterrorism of the United States of America, October 2018. Available at https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf (accessed 11 August 2020).

Williams, B. G., 'Islamic State Calls for Followers to Spread Coronavirus, Exploit Pandemic and Protests,' *The Conversation* (23 June 2020). Available at https://theconversation.com/islamic-state-calls-for-followers-to-spread-coronavirus-exploit-pandemic-and-protests-136224 (accessed 11 February 2021).

Wilson Center Online, 'Timeline: The Rise, Spread, and Fall of the Islamic State', (October 28, 2019). Available at https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state (accessed September 5, 2020).

Withnall A., 'ISIS Loses 'Prophesied' Town of Dabiq to Syrian Rebels After Short Battle', *The Independent*, (16 October 2016) available at http://www.independent.co.uk/news/world/middle-east/isis-dabiq-loses-apocalyptic-prophesy-town-of-dabiq-to-syria-rebels-short-battle-a7363931.html (accessed 2 May 2017).

Zetter, K., 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon,' *Wired*, 3 November 2014. Available at https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed 3 March 2020).