Responses to cybercrime in Azerbaijan with special reference to the United Kingdom

Elvin Balajanov

Submitted in accordance with the requirements
for the degree of Doctor of Philosophy

The University of Leeds
School of Law
September 2018

The candidate confirms that the work submitted is his/her own and that appropriate credit has been given where reference has been made to the work of others.

Acknowledgements

I take this opportunity to express my sincere gratitude and respect to all those who contributed their support to completing this research project.

Initially, I would like to thank Professor David Wall and Dr Audrey Guinchard for their kind acceptance to examine this thesis.

I wish to express my deepest gratitude to my supervisors, Dr Subhajit Basu and Professor Clive Walker for their enthusiastic supervision, insightful guidance and constructive criticism. Dr Subhajit Basu has given me valuable advice and stimulated suggestions and encouragement throughout my PhD studies. I highly acknowledge his crucial help and inspiration.

I am especially indebted to Professor Clive Walker and I express my deepest appreciation for his expert advice, thought-provoking comments and sincere dedication. My research project has largely benefitted from his immense academic input accompanied by an individual approach. He has also actively assisted me with generous support, helpful ideas and irreplaceable enthusiasm.

I am also grateful to my supervisors for their patience and kind support in the writing of this thesis.

I would like to express my gratitude to my country and the Ministry of Education of the Republic of Azerbaijan for the funding of my studies. Without this funding, the realisation of this research project could not have been possible.

Last but not the least, I wish to thank my beloved family and friends for their love, care and encouragement through the learning and writing process of this thesis.

Finally, I owe many thanks to the University of Leeds, School of Law for the constant support and to all those who indirectly guided me throughout these years.

Abstract

The primary objective of this research is to explore and analyse policy and legal responses of Azerbaijan to cybercrime, provide detailed and insightful recommendations to enhance the effectiveness, efficiency and legality of Azerbaijani responses to cybercrime based on the existing experience and insights of the UK.

It is contended that although the application of Information and Communication Technologies has been significantly encouraged in Azerbaijan effective and efficient control and prevention of cybercriminal activities had not been adequately assured. This thesis has, thus, focused on finding out whether necessary institutions are in place, and whether national policies and laws are sufficient to address the challenges of cybercrimes and are being implemented in accordance with national and international laws, standards and principles.

Based on the research findings it is asserted that Azerbaijan has failed to respond appropriately to cybercrime due to the lack of both policy and legal frameworks as well as insufficient human, institutional and technological capacity and resources, and low levels of cooperation at the national and international levels.

As one of the countries having encountered an increasing impact of threats from cybercrimes, Azerbaijan needs to enhance its capacity to control and prevent these threats more effectively and efficiently. Notwithstanding that the country has taken multiple measures to address the problem of cybercrime, these measures are not effectively coordinated and remain fragmented and incomplete.

However, it has also become apparent that there is not a single solution to the problems posed by cybercrime, which Azerbaijan has failed to adopt. Cybercrime requires a holistic response: a combination of a strategy, policies and laws, extra-legal measures, sufficient human, institutional and technological capacity and resources, as well as effective and efficient cooperation at the national and international levels.

Table of Contents

CHAPTER 1: Introduction

1.1 Introduction and central thesis

Since the beginning of the 21st century, the development of Information and Communication Technologies (ICT) and the Internet has been at the forefront of the policy to reduce the dependency of the Republic of Azerbaijan on oil revenues and further advance non-oil industries along with ensuring economic competitiveness and sustainability of the country. Rapidly evolving information society and ever-increasing reliance on the delivery of technology-mediated services have also brought new types of vulnerabilities, which 'need to be properly defined, thoroughly analysed, remedied or reduced'.[1] Information inequality, unequal access to information sources and ICTs, language barriers in cyberspace, lingual and terminological threats to the language in a multilingual environment, problems of protecting personal data in information databases and systems and ensuring the information-psychological security of society can be exemplified amongst the list of impediments Azerbaijan has been encountered.[2] These vulnerabilities have the potential to harm every society in new and perilous ways.

The digital environment also provides opportunities and fertile ground for criminality. Growing dependency of society on the use of ICTs and the unlimited and free flow of information in the digital world has created 'unparalleled opportunities for crime and misuse'.[3] There has been a substantive increase in the novel applications of technology for creating new forms of crimes and its use by criminals over the last three decades.[4] Additionally, 'qualitative differences'[5] between cybercrime and physical crime - increased scale, transnational scope, and

---

[1] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', JOIN (2013) 1 final, 7 February 2013.

[2] See for further information: Rasim Aliguliyev, Yedgar Jafarov, 'Azerbaijani language in the multilingual internet environment'; Afruz Gurbanova, 'Termonological threats against Azerbaijani language in the era of Globalization'; Rasmiyya Mahmudova, 'Negative influences of information and solutions', (Second Republic scientific-practical conference on the multidisciplinary problems of Information security dedicated to the 150th anniversary of the International Telecommunication Union' 14 May 2015).

[3] Thomas J Holt, Adam M. Bossler and Kathryn C Seigfried-Spellar, *Cybercrime and Digital Forensics* (Routledge 2015) 5.

[4] Ibid.

[5] Milton Mueller, *Networks and States* (MIT Press 2010) 161.

distributed control - enhance the vulnerability of ICT infrastructure and opportunities arising from the exploitation of these vulnerabilities result in greater online victimisation.[6] Accordingly, the regulation and governance of the Internet, ensuring the safety and security of both the society and the information infrastructure are among the highest priorities in today's technologically growing world.

Notwithstanding that general ICT developments and applications in Azerbaijan appear to be plentiful, there is an imbalance between the encouragement of the application of ICTs and the level of ensuring the cybersecurity of users.[7] Citizens, government and businesses in Azerbaijan have been exposed to the growing number of cyber-attacks and cybercrime according to many international and security network reports and secondary sources.[8] However, at the national level, the understanding of the current cyber threat landscape and its impact on the country seems to be obscured, which may potentially render the responses of the country to cybercrime fragmented and inadequate. Noticeably, methodologically sound national surveys measuring the scale and impact of cybercrime are currently unavailable. In addition, comprehensive research on the topic of cybercrime and responses to it has not been produced.

It is the central thesis of this research study that the country has not yet responded appropriately to cybercrime. Although the application of ICTs has been significantly encouraged by the State effective and efficient control and prevention of cybercriminal activities are not adequately assured. This can be due to the lack of a comprehensive national strategy, as well as insufficiency of national policies, laws and resources in addressing the challenges of cybercrimes.

Effective and efficient control and prevention of cybercrimes require a holistic approach: a combination of a strategy, policies and laws, extra-legal measures, sufficient human, institutional and technological capacity and resources, as well as cooperation at the national and international levels. It is contended that Azerbaijan

[6] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007) 130.
[7] See Section 3.2, Chapter 3 for a detailed discussion.
[8] See Section 2.5, Chapter 2 for a detailed discussion.

needs to adopt a holistic approach and enhance its responses accordingly to confront and overcome the growing threats and risks posed by cybercrime.

In response, this study will adopt a socio-legal approach to explore and analyse the responses of Azerbaijan to cybercrime and produce analysis as to how to enhance the effectiveness, efficiency and legality of these responses. To reach these objectives, this study involves doctrinal as well as empirical research of policy, legal and practical responses of the country to cybercrime.

1.2 Principal research questions and chapter structure

To achieve the stated objectives within the confines of the central thesis, this study seeks to answer five principal research questions in the corresponding chapters, which will, cumulatively, provide an answer to the central thesis statement.

What is cybercrime and how is it perceived in Azerbaijan? How much of a problem is cybercrime for the country? Chapter 2 considers a broad discussion of both the reality and the perception of cybercrime in Azerbaijan. Understanding the nature and scale of threats and vulnerabilities is crucial for measuring the importance of investing in protection and prevention against cybercrimes.[9] Therefore, the impact and extent of cybercrimes, as well as underlying factors linked to changes in extent and impact of cybercrime in the country are studied in addition to the definition and typologies of cybercrimes. Besides, design and legal challenges, as well as opportunities in fighting cybercrime are also elaborated within this chapter. Setting standards for the main measurement criteria to be used for the evaluation of responses to cybercrime in the forthcoming chapters is also an integral aspect of this chapter.

What are the developments in Azerbaijan in terms of cybercrime strategy and policies? Chapter 3 seeks to elaborate and scrutinise official policy responses of the country to cybercrimes. This Chapter critically analyses the measures undertaken in Azerbaijan to prevent and control cybercrimes from the policy and

[9] Cabinet Office, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world (London 2011).

strategy perspectives. The Chapter further discusses and analyses the measures, such as legal, institutional, and preventive measures that can be viewed as parts of its anti-cybercrime policy responses, and its translation into a national strategy.

To what extent are regulatory and substantive criminal laws equipped to handle cybercrimes? Chapter 4 explores the legal responses of the country to cybercrimes. This Chapter overviews and evaluates the appropriateness of national legislation and frameworks, in particular, the relevant constitutional rights, liberties and regulatory laws, and the criminalisation approach as well as the mechanism of substantive criminal laws from the theoretical/doctrinal and critical perspectives.

Which procedural instruments and powers are in place in Azerbaijan to investigate and adjudicate cybercrime? Do they provide an effective and efficient response? Chapter 5 focuses on evaluating the appropriateness of criminal procedural laws and investigatory powers applied in Azerbaijan. Critical analysis of procedural measures and instruments also refers to the instruments offered by the Council of Europe Convention on Cybercrime (2001). Besides, the chapter assesses national approaches regarding jurisdictional issues and international cooperation provisions, as well as the provisions on the collection and admissibility of digital evidence that also go beyond the regulations of the Convention.

What can be done to augment the strength of Azerbaijan in controlling and preventing cybercrime? What lessons can be drawn from the UK? Having scrutinised the policy and legal responses of Azerbaijan to cybercrimes, defined and summarised the deficiencies and needs for possible improvements in Chapters 2, 3, 4, and 5, potential blueprints and recommendations are introduced in Chapter 6. The Chapter also draws lessons based on the existing experience and insights of the UK to make further recommendations for enhancing the responses of the country to cybercrime.

Chapter 7 summarises the main findings and analysis presented in the preceding chapters and provides a final examination of the central thesis as well as limitations in the research. Furthermore, possible avenues and recommendations for future research are proposed in this chapter.

1.3 The Originality of the Study

The legal and policy responses of the Republic of Azerbaijan to cybercrime have not been previously subject of systematic and comprehensive academic research. This study aims to investigate the growing problem of cybercrime in Azerbaijan, to analyse the appropriateness of its responses, and to draw lessons from the UK following that analysis. On these grounds, this study contributes significantly to the expansion of academic knowledge and makes recommendations to enhance the capacity of the country against the threats and risks posed by cybercrimes to the country. Thus, the originality of this study is ensured in several ways.

This is the first academic study to explore the problem of cybercrime and its perception in Azerbaijan. To evaluate the appropriateness of crime prevention strategies, policies, laws, programmes and actions, it is essential to start the research by examining whether they are based on 'a broad, multidisciplinary foundation of knowledge about crime problems, their multiple causes and promising and proven practices'.[10]

Little academic research has been conducted referring to cybercrime and its prevention in Azerbaijan. Only one book was published in 2007 on computer crimes and prevention issues.[11] It discusses computer crimes from the international perspective and studies international experience of fighting computer crimes. During study visits and fieldwork in Azerbaijan throughout this research, the researcher established that there was no further relevant literature in the Azerbaijan National Library (ANL) and the Library of the Baku State University (BSU). Neither the catalogue of published books in Azerbaijan supplied by ANL nor by the BSU possesses information about a published book related to cybercrime control and prevention. Existing criminal law literature and books illuminate the issue from the perspective of the legislative framework and give only a general

[10] Article 11, *United Nations Guidelines for the Prevention of Crime* (United Nations Economic and Social Council Resolution 2002/13 - annex).
[11] See Vagif Gasimov, *Information security: computer crimes and cyberterrorism* (*İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq)* (Baku: Elm 2007).

description of the elements of the Criminal Code articles concerning cybercrimes.[12] Thus, underlying causes, material conditions, challenges of addressing the problem of cybercrime have not been attended to. Similarly, databases available online on the websites of the institutions researching the law and containing online sources possess the insufficient amount of research papers or articles related to this field of studies in Azerbaijan.[13] Compared to the existing research and literature, this study investigates the problem of cybercrime in Azerbaijan by measuring the nature of threats, scale and impact, underlying causes of cybercrimes, as well as challenges and opportunities in addressing the problem.

Next, the provision of a comprehensive study of policy and legal responses of Azerbaijan to cybercrime is another factor making this study original. To attain the objectives, this research tries to evaluate the appropriateness of responses to cybercrimes in Azerbaijan, which has not been studied comprehensively so far.

Notwithstanding that, some papers have addressed the issue from international perspectives, equivalent types of thorough studies of policy and legal responses are not available in Azerbaijan. *'Problems of Information Society*'[14] and '*Problems of Information Technology*[15], scientific-practical journals published by the Institute of Information Technology of the Azerbaijan National Academy of Sciences, and *the Journal of Information Security*[16] include articles and research papers which appeal to cybercrime matters by discussing mainly the international and technological perspectives. For example, an article written in 2013 briefly describes

[12] See for example, Firudin Samandarov*, Commentary on the Criminal Code of the Republic of Azerbaijan, Second part (Azərbaycan Respublikası Cinayət Məcəlləsinin kommentariyası, İkinci hissə) (*Baku, Hüquq Yayın Evi, 2016) 486-503; Isfandiyar Aghayev, *Criminal Law: special part (Cinayət hüququ: xüsusi hissə)* (Baku: Nurlar, 2018).

[13] The 'Socio-political sciences series' of the Journal of the Baku University News published by the Baku State University between 1992 and 2015 have not included any article or research paper directly concerning 'cybercrimes' or 'computer crimes'. Published articles can be accessed online via: http://publish.bsu.edu.az/az/content/sosialsiyasi_elmlr_seriyas_illrl. Moreover, Journal of International Law and Integration Problems and Baku State University Law Review (http://lr.bsulawss.org/archive/) have not contained articles focusing on cybercrime (or computer crimes) to date.

[14] Available online at http://jpis.az/?&lng=en.

[15] Available online at http://jpit.az/.

[16] The journal has been published by the State Agency for Special Communication and Information Security of the Special State Protection Service of the Republic of Azerbaijan and the Interstate Commission for the Protection of the State Secret by the President since 2015.

the main features of existing national cybersecurity strategies of developed countries 'with the aim of identifying the best practices in the development of national cybersecurity strategies'.[17] Neither Azerbaijan's approach to the issue nor their relevance to addressing the challenges of cybercrime in Azerbaijan has been debated in the article. However, the author mentioned the importance of cooperation between public and private sectors in effectively ensuring the cybersecurity in a general sense. Another paper, 'Necessity of global cybersecurity convention or the opportunities for Budapest Convention to become a global standard',[18] analyses the advantages and disadvantages of the Convention on Cybercrime and proposes forecast for future development of events and possible solutions by examining the disagreement among the leading states of the world on new global cybersecurity convention.[19] However, it does not reflect upon the role of the Convention in combating cybercrimes for Azerbaijan. This research studies not only the role of the Convention, but also the relevant normative-legal acts and regulations for an understanding of the criminalisation approaches adopted. Besides, procedural powers and instruments, jurisdiction related issues, legal aspects of electronic evidence, international cooperation and cybercrime prevention-related measures and provisions are subjected to detailed analysis.

The tendency of not including Azerbaijan as a primary focus of research is also present in another paper, 'Coordination problems in information security of e-government', which focuses on actual problems of coordination and makes a number of recommendations aimed at their elimination in a broad way.[20] Critical evaluation of the present situation and the capacity of Azerbaijan concerning the topic have not been adhered to in the paper. Another paper, 'Multidisciplinary scientific and theoretical problems of information security', introduces brief discussion on some international, political, psychological, legal, economic, cultural

[17] Yadigar N. Imamverdiyev, 'Next generation national cyber security strategies', (2013) 8 *Journal of Problems of Information Society*, 42-51.
[18] Bakhtiyar N. Mammadov, Aysel N. Asgarova, 'Necessity of global cybersecurity convention or the opportunities for Budapest Convention to become a global standard', (2014) 1 *Journal of Problems of Information Society*, 3-9.
[19] Ibid.
[20] Yadigar N. Imamverdiyev, 'Coordination problems in information security of e-government', (2014) 2 *Journal of Problems of Information Society*, 24-30.

and ethical aspects and issues primarily related to training and child protection.[21] This study, however, is more comprehensive, especially given that it is focused on researching the law enforcement and investigations, international cooperation and the criminal justice system in practice in addition to the analysis of legislation and policy frameworks.

Evaluation of the appropriateness of legal and policy responses to cybercrime in Azerbaijan needs a critical approach and analysis from the researcher. Even though several key international bodies have criticised and expressed their concern about the deteriorations in Azerbaijan's human rights record,[22] all the research mentioned above papers and articles published in Azerbaijan omitted critical evaluation. Thereby, apart from critically evaluating the policy and legal responses of Azerbaijan, this study identifies the need for amendments, updates or changes and makes recommendations to develop more effective and efficient anti-cybercrime responses that do not compromise the national and international law, standards and principles.

The researcher has implemented both doctrinal and empirical research methods to present a comprehensive study of the appropriateness of responses to cybercrime in Azerbaijan. Besides a thorough analysis of a wide range of relevant primary and secondary sources, in-depth interviews with public and private sector representatives have been conducted in Azerbaijan. The approach of putting the law in context has not been adopted in any of the existing limited number of literature on cybercrime due to heavy reliance of the authors on the doctrinal

[21] Rasim M. Alguliyev, Yadigar N. İmamverdiyev, Rasim Sh. Mahmudov, 'Multidisciplinary scientific and theoretical problems of information security', (2017) 2 *Journal of Problems of Information Society,* 32-43.

[22] See for example, Human Rights Watch, *World Report 2018*, 54-59, https://www.hrw.org/sites/default/files/world_report_download/201801world_report_web.pdf; Freedom House, *Freedom on the Net 2017*, https://freedomhouse.org/sites/default/files/FOTN%202017_Azerbaijan.pdf; *Implementation of the European Neighbourhood Policy in Azerbaijan,* Brussels, SWD(2015) 64 final http://eeas.europa.eu/enp/pdf/2015/azerbaijan-enp-report-2015_en.pd; United Nations Human Rights Council, *Concluding observations (2016) CCPR/C/AZE/CO/4*. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/AZE/CO/4%20&Lang=En.

research methods. Thus, *the methodology applied for this study can be considered as another feature providing the originality of this study.*

Next, this is the first study designed to research the effectiveness, efficiency and legality of responses of Azerbaijan to cybercrime with special reference to the UK. It can also be argued that drawing lessons from the relevant UK legislation and practice to make further recommendations for enhancing the responses of the country to cybercrime is another feature making this study unique.

Generally, most of the papers written or research conducted to date have mainly referred either to documents or guidelines prepared by international and regional actors, such as UN, ITU, OECD, European Parliament, European Commission, or NATO, or to literature about Russia and in a very few cases to literature about the US.[23] As a post-Soviet country and as a country with close historical and geographical ties to the Russian Federation, both the legal frameworks and academia of the Republic of Azerbaijan have been impacted by Russia's relevant legislation and literature. It can be argued that exploration of Russia's legislative frameworks and literature could aid this research. Crucially, however, Russia has neither signed nor ratified the Convention on Cybercrimes, and thus, its legislation has not been harmonised with the Convention unlike the legislation of the Republic of Azerbaijan. The pre-harmonised Chapter of the Criminal Code of Azerbaijan was very similar to the relevant Chapter of the Russian Criminal Code,[24] but, after the harmonisation with the Convention, not only the legislation but also the stance of Azerbaijan against cybercrimes and approach to international cooperation significantly vary from Russia's standpoint. Thus, trying to enhance the capacity of Azerbaijan against cybercrimes based on the Russian expertise and position would not achieve the desired outcome. Moreover, access to the UK libraries, relevant

[23] This is also applicable to the above-mentioned research papers, articles and literature of Azerbaijan. All articles discussed above include a list of bibliography.

[24] Before the harmonisation, Chapter 30 of the Criminal Code of the Republic of Azerbaijan (1999) is titled as 'Crimes in Sphere of the Computer Information' and included almost the same three articles with identical dispositions (Articles 271-273) of the 'Chapter 28. Crimes in the Sphere of Computer Information' of the Criminal Code of the Russian Federation (1997) (See articles 272-274).

literature and information regarding its experience have been more effectively and efficiently assured through being a student at the University of Leeds.

Furthermore, as a Council of Europe member state and as a party to the European Convention on Human Rights (ECHR),[25] the International Covenant on Civil and Political Rights (ICCPR)[26] and the Convention on Cybercrime[27], the UK has a long history and, therefore, high level of expertise and deep theoretical literature regarding ICT development, as well as advanced policy and legal techniques in controlling and preventing cybercrime. Moreover, the National Cyber Security Strategy 2016 - 2021 and more sophisticated current reporting and measuring mechanisms are also advantages in formulating more successful protection[28]. The UK's public and private sector reactions to cybercrimes have also been more dedicated and comprehensive compared to those of Azerbaijan.

To handle cybercrimes and become 'one of the most secure places in the world to do business in cyberspace' by being 'more resilient to cyber-attacks and better able to protect …interests in cyberspace', [29] the UK Government allocated £860 million public funding for 2010 National Cyber Security Programme with the intention to deliver this vision 'in partnership with the private sector and other countries'.[30] A further £1.9 billion of transformational investment allocated to support a comprehensive National Cyber Security Strategy 2016 to 2021 launched by the UK government in 2016. In addition to these strategies, studying the role of programs, institutions and partnerships in the UK has contributed significantly to make relevant recommendations and offer specific solutions for the enhancement of the cybercrime control capacity of Azerbaijan.

---

[25] European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), (ETS No.5), entered into force: 3 September 1953. Signed by the UK in 4/11/1950 and ratified in 8/3/1951.
[26] International Covenant on Civil and Political Rights (ICCPR) UN Doc. A/6316 (1966), entered into force March 23, 1976. Ratified by the UK in 20/05/1976.
[27] Council of Europe, Convention on Cybercrime (2001) ETS No. 185. Signed by the UK in 23/11/2001 and ratified in 25/5/2011.
[28] Cabinet Office, The UK National Cyber Security Strategy 2016 to 2021 (London 2016).
[29] The UK Cyber Security Strategy (2011) (n.9), 39.
[30] Ibid. 9.

It is evident that UK has attained and is achieving several objectives to satisfy the government's goal of making the country a world-leader in cyber security. Thus, valuable lessons have been drawn from UK for Azerbaijan in ways undertaken by no previous researcher. Understanding the trends of anti-cybercrime policies and laws applied by UK has helped to identify the measures which are required to be taken for establishing a more effective and efficient protection for society and the state against cybercrimes in a technologically developing country like Azerbaijan.

1.4 Methodology

Aspects of the research questions require the collection and analysis of a range of different sources. Thus, both documentary analysis and socio-empirical research methods are applied to ensure the completeness of the study and to critically examine the appropriateness of the policy and legal frameworks in the control and prevention of cybercrime. Moreover, the technique of policy transfer is adopted in the last part of this research to propose recommendations for the enhancement of the capacity of Azerbaijan in controlling and preventing cybercrime.

Since the law is instrumental in combating cybercrime and, therefore, has policy and practical impacts, the collaboration between law and social science is both obvious and necessary to design its content and assess its effects.[31] Given this understanding, a socio-legal approach is adopted by this study. It requires the analysis of relevant laws to be directly linked to the analysis of the social situation to which laws apply and to put into the perspective of the social situation by considering the role of the law in the creation, maintenance and change of perspectives and practices.[32] Involvement of sociological analysis in the evaluation of practise-based features of the law can enable the researcher to uncover and

[31] Malcolm M. Feeley, 'Three Voices of Socio-Legal Studies' (2001) 35 *Israel Law Review*, 175-183.
[32] David N. Schiff, 'Socio-Legal Theory: Social Structure and Law' (1976) 39 *Modern Law Review.* 287.

gain insight into the institutional successes and limits of the legal practices in a way that traditional forms of legal studies are unable to do.[33]

The approach of putting the laws in the context of Azerbaijan has been significantly unattended to and, as a result, their implementation has been ineffective and inefficient. In-depth examination of relevant laws and their operational schemes by the introduction of a socio-legal study in this field are conducive to understanding the laws and enhancing the current capacity of Azerbaijan against cybercrimes.

1.4.1 Documentary research

To decide whether any perceived gaps or shortcomings are the result of inadequate legal doctrine or lack of compliance with the doctrine, before any empirical work it is essential to analyse that the doctrine, properly interpreted, is being complied with.[34] Therefore, the appropriateness of the current legal provisions pertaining to cybercrime has been examined, besides the analysis of policy frameworks and the relevant lessons to be drawn from the UK, by selecting and studying the available literature and sources on the main themes examined within this research (which ended on September 27, 2018). Thus, legal documents, official publications, books, journal articles, 'grey' literature (such as reports, working papers, conference proceedings and newspapers),[35] and statistics comprise the bibliographic structure explored in this research. In addition to online databases, the relevant primary and secondary sources were accessed through the University of Leeds library, as well as the National Library of Azerbaijan and the Baku State University Library.

An essential part of the subsequent deductions was obtained through thematic analysis of the relevant codes, laws and official policies pertaining to Azerbaijan. The relevant legal documents were primarily explored through the *State Registry of Legal Acts* (http://www.huquqiaktlar.gov.az), and the *E-Portal of Normative-Legal*

[33] Reza Banakar and Max Travers, *Theory and Method in Socio-Legal Research* (Hart Pub 2005) 15.
[34] Terry Hutchinson, 'Doctrinal research' in Dawn Watkins and Mandy Burton, *Research Methods in Law* (Routledge 2013) 8.
[35] Charles Peter Auger, *Information Sources in Grey Literature* (4th edn, Bowker-Saur, 1998).

Acts (www.e-qanun.az). The related statistics were retrieved through the online database of *the State Statistical Committee of the Republic the Republic of Azerbaijan*.[36] The parliamentary reports, discussions and debates on related issues, draft legislation, as well as relevant projects were accessed through the official website of the National Assembly (*Milli Majlis*) of the Republic of Azerbaijan (http://www.meclis.gov.az/) and the journal of the National Assembly (http://jurnal.meclis.gov.az/). Relevant judicial acts and documents were retrieved through the website of the judicial system of the Republic of Azerbaijan (http://courts.gov.az/). Government publications, law journals, law reviews, articles and other legal information resources related to the UK were accessed through online resource databases such as LexisNexis[37], Westlaw UK[38] and GOV.UK.[39]

The findings of the literature survey have been scattered pervasively throughout the study rather than being summarised in a separate literature review chapter to reflect on the literature contextually.

1.4.2 Fieldwork

In order to be able to scrutinise the legality, effectiveness and efficiency of the responses of Azerbaijan against cybercrimes, preference was given to a qualitative research approach, which is flexible and sensitive to the social context and broadly 'interpretivist' in the sense that its concern is interpretation and understanding of the social world.[40] Moreover, the objectives of this study required the production of 'rounded and contextual understandings on the basis of rich, nuanced and detailed data'[41], which can be ensured by the qualitative research approach since these features constitute its aims.

By contrast, a more deductive approach to the relationship between theory and research would be entailed by quantitative research, which embodies a view of

[36] See for further information https://www.stat.gov.az/source/crimes/.
[37] https://www.lexisnexis.com/uk/legal/.
[38] http://legalresearch.westlaw.co.uk/.
[39] https://www.gov.uk/government/publications
[40] Jennifer Mason, *Qualitative Researching* (2nd edn, London: Sage, 2002) 4.
[41] Ibid.

social reality as an external, objective reality.[42] To avoid the conduct of a limited evaluation of the appropriateness of responses to cybercrime, achievement of more insightful findings is needed, which can be better attained by the qualitative research. While trying to achieve these findings, the unique and creative ways that individuals understand the world can also be respected which motivates qualitative research.[43]

Qualitative research contributes to the understanding of the context in which crime occurs through providing 'rich and detailed data to flesh out the bare skeleton provided by quantitative data'.[44] In comparison to quantitative research, it manifests 'a view of social reality as a constantly shifting emergent property of individuals' creation'[45]. Moreover, as provided by Silverman, the social and cultural construction of the variables may be neglected by dependence on quantitative methods,[46] which might limit the comprehensiveness of this study. Given that clear and systematic details have not been settled by the legal texts in Azerbaijan and relevant laws have been harmonised without reflecting the social setting of the country, the significance of the integration with the social world and 'interpretivist' approach to the research became even more essential to scrutinise the appropriateness of responses to cybercrime.

Another reason for selecting a qualitative rather than a quantitative approach is the lack of reliable statistical cybercrime data due to numerous factors making accurate data collection difficult in Azerbaijan. Access and collection of the statistical data, which is crucial for a quantitative approach, would be highly challenging and problematic because of the insufficiency of the relevant statistics supplied by the official data sources. In addition, it was unrealistic to expect that the necessary statistics could be generated for this study by the researcher himself within the boundaries of time and resources, as well as due to the likely non-cooperation of crucial agencies. Qualitative research, on the other hand, could also help to

[42] Alan Bryman, *Social Research Methods* (Oxford University Press, 2008) 22.
[43] Martin J Packer, *The Science of Qualitative Research* (Cambridge University Press, 2011) 52.
[44] Clive Coleman and Jenny Moynihan, *Understanding Crime Data* (Buckingham: Open University Press, 1996).
[45] Alan Bryman (n. 42) 22.
[46] David Silverman, *Doing Qualitative Research: A Practical Handbook (*London: Sage 2000) 5.

achieve a better analysis of the 'dark figure of crime', the figure for unrecorded crime or undetected offenders, that is to say those not included in official statistics.[47]

It can be concluded that although it has been referred to as a method fostering 'greater subjectivity',[48] adoption of qualitative research approach delivered more opportunities for attaining the aims of this study.

1.4.2.1 Qualitative interviews

To make adequate suggestions for enhancing the responses of the country to cybercrimes, it is crucial to gain insight into socio-legal issues influencing the perspectives and practices of the country 'through understanding the views of the individuals whose lives reflect those issues'.[49] Views and ideas of individuals can be obtained through the application of various qualitative research methods, such as focus groups, observations, in-depth interviews and etc.

In-depth interviewing was the main method of collecting relevant data, as it was challenging to obtain the information regarding the individual experiences and approaches to the appropriateness of responses to cybercrimes, for example, through focus groups. This is because research questions put forward by this study should have not been answered in an environment, which can unduly influence the responses that are generated, especially when considering that some of the questions touched sensitive issues, such as the effectiveness and efficiency of the State in dealing with cybercrimes. Inference within and beyond the group impacts on the output as well, which might become very biased by this technique, as focus groups become influenced by one or two dominant participants.[50]

Considering time limitations assigned for the fieldwork, generation and collection of sufficient amount of relevant data for the purposes of this research could not be

[47] Lesley Noaks and Emma Wincup, *Criminological Research* (London: SAGE, 2004) 11.
[48] Martin J Packer (n. 43).
[49] Irving Seidman, *Interviewing as Qualitative Research* (4th edn, New York: Teachers College Press 2013) 13.
[50] David Wilkinson and Peter Birmingham, *Using Research Instruments: A Guide for Researchers* (Routledge Falmer 2003) 108-109.

assured through the application of observational research, which is likely to be more time-consuming than interviews. Moreover, the opinions of individuals cannot be studied directly by this research technique, which is also limited in terms of studying the problems of the past.[51] Since the responses have been evaluated by scrutinising the measures taken to date, it would be highly inefficient and ineffective to apply this research technique during the fieldwork.

In-depth interviews, on the other hand, have contributed to understanding the experience of people who have relevant information, and who directly or indirectly participate in the country`s information security life, and 'the meaning they make of their experience'.[52] Interviews also obtained insight into identifying the reasons behind success or failure when establishing an effective and efficient cybercrime control and prevention. Understanding the views of the interviewees can be better achieved if interviews are 'open', which also helps to collect rich and detailed answers.[53] So, based on a broad list of issues and questions to be asked during the interviews, semi-structured interviews were conducted, since that approach provides an opportunity for dialogue and exchange between the interviewer and the interviewee.[54] To sum up, the conduct of in-depth, face-to-face, semi-structured interviews for considering the views of experts on the appropriateness of cybercrime control and regulation approach of Azerbaijan and their practices and attitudes towards the anti-cybercrime capacity of the country was more appropriate for the field research in Azerbaijan than any other technique.

The interview guides (see Appendix 1) were designed to cover four main topic areas, which directly reflected the thesis structure. After gathering general biographic and background information about the interviewee, the interview moved to cover the problem of cybercrime in Azerbaijan, followed by policy, criminal law, and procedural law responses to cybercrime. The interviews were structured in a

[51] Leonard Cargan, *Doing Social Research* (Rowman & Littlefield Publishers 2007) 142-143.
[52] Irving Seidman (n. 49).
[53] Alan Bryman (n. 42) 439.
[54] Emma Wincup, *Criminological Research: Understanding Qualitative Methods* (2nd edn, London: Sage 2017) 100.

way to aid the critical examination of the central thesis through eliciting information concerning each of the research questions.

Multiple questions were contained under each of the four headings. The questions were appropriately and deliberately phrased to be as open as possible and to guard against leading the interviewee or getting socially or contextually desirable answers.[55] Given that very limited research and expertise has been undertaken to date in the country, the interview questions were not focused on testing basic knowledge, but rather aimed at gaining insight into relevant perceptions, practices and attitudes.

1.4.2.2 Sampling strategy

To 'discover, understand and gain insight', it was crucial to select a sample from which the most can be learned.[56] This requirement cannot be met by adopting the 'random sampling' strategy which is laborious and time-consuming and might generate biased results.[57] Therefore, 'purposive or purposeful sampling' approach, which identifies the most relevant people who can give the most beneficial contribution, was adopted to accomplish the purpose of this study. According to Patton, 'the logic and power of purposeful sampling lies in selecting information-rich cases (those from which one can learn a great deal about issues of central importance to the purpose of the inquiry) for study in depth'.[58] Application of purposive sampling strategy ensures the yield of the most relevant and insightful data.[59] Therefore, the study tried to involve the interviewees with relevant professional expertise.

Since those concerned with cybercrime control and prevention issues form a distinctly small community in Azerbaijan, the population of participants was relatively narrow, and thus, it was not difficult to identify potential key participants.

---

[55] Ian Crow and Natasha Semmens, *Researching Criminology* (Open University Press, 2006) 98.
[56] Sharan B. Merriam, *Qualitative Research: A Guide to Design and Implementation* (Jossey-Bass 2009) 77.
[57] Mark Dantzker, Ronald Hunter, *Research Methods for Criminology and Criminal Justice,* (3rd edition, Jones& Bartlett Learning, 2012) 112.
[58] Michael Q. Patton, *Qualitative Research and Evaluation Methods* (Sage Publications 2002) 230.
[59] Robert K. Yin, *Qualitative Research from Start to Finish* (The Guilford Press, 2011) 88.

The Action Plan for Azerbaijan 2014-2016, which is a joint initiative of the Council of Europe and the Azerbaijani authorities, identified partners in enhancing the capacity of criminal justice institutions to investigate, prosecute and adjudicate cybercrimes. Among the partners identified by the Action Plan, the Ministry of Justice, the Ministry of Internal Affairs, the State Security Service, the General Prosecutor's Office, the Ministry of Communications and High Technologies, as well as Internet service providers were approached for interviews with their relevant experts. In addition to these institutions, the Office of the President of the Republic of Azerbaijan, the Special Communication and Information Security State Agency, the Academy of the State Security Service, two relevant Committees of the Parliament, and 8 out of 11 district courts in the capital city Baku, were contacted for interviews. Given that the research was not only aimed at eliciting views and practices of government sector employees, some private sector representatives from banking and the information technology industry and commercial IT users within that industry, as well as non-governmental, non-commercial institutions and independent experts, were contacted.

Thirty potential interview participants representing both government and private sector entities were initially contacted via e-mail and phone (via coordination with their employers where applicable). E-mails sent contained brief information about the researcher and the project and supported with a letter obtained from the University of Leeds and the 'Information sheet' (see Appendix 1). To give more information and to clarify the decision of those approached, as well as to arrange a suitable venue and time for conducting interviews, all emails were followed up by telephone conversations. In case any approached participant refused to take part in the interview, an alternative relevant person was approached for an interview.

Given that the environment in Azerbaijan is often hostile to open dialogue on the issues being studied, and the high levels of specialist expertise required in the field of cybercrime are not widespread in the country, only eight participants of those accessed agreed to be formally interviewed. Informal meetings and phone conversations were also held with some of the interviewees selected, however, contributions of only those who have agreed to the formal interview have been accounted for in this study. Given that the aim of this study was not to draw generalisable conclusions based on the interviews alone, although limited, the

contributions made by the interviewees were used to enhance and augment the findings of the documentary research.

Ultimately, the following were the number of interviewees included in this study: Parliament of the Republic of Azerbaijan (1), Ministry of Communications and High Technologies (CERT) (5), Non-governmental, non-commercial institutions (1) and independent experts (1). The Office of the President of the Republic of Azerbaijan, Ministry of Justice, General Prosecutor Office, district courts, as well as information technology and services refused to take part in the study due to lack of relevant experts specialised in the field of cybercrime. The State Security Service refused due to the topic being 'sensitive' and 'secretive'. The Ministry of Internal Affairs did not respond to the request for interviews despite the fact that an official online letter was sent directly to the Minister of Internal Affairs through the online portal of the website of the Ministry asking for permission and support for conducting interviews with relevant police officers. This was also the case with the Special Communication and the Information Security State Agency and the Central Bank of Azerbaijan, as formal requests made for interviews were not replied, although they were initially agreed to be interviewed during the phone conversation.

The private sector companies approached (companies specialized in delivering ICT services and Internet service providers (ISPs)) refused to take part in this study to avoid possible 'risks' and 'conflicts of interest' with state bodies.

The number of interviews performed in each category is given in Table 1.1. Each respondent is referred to throughout this study by the corresponding label.

Table 1.1. Research participants and their categorisation

Category	Label	Number of interviews
Ministry of Communications and High Technologies (CERT) employees	Ministry Official 1, 2, 3, 4, 5	5
Parliament officer	Parliament Officer 1	1
NGO representative	NGO Representative 1	1
Independent expert (lawyer)	Independent expert 1	1

During the interviews, audio recording devices were not used, and the notes taken were transcribed into Microsoft Word. Specific computer software has not been used for analysis on the basis of the low volume of transcript data (16 pages in total). Quantitative analysis was not undertaken given the small sample size. The findings from the interviews and important comments made by the interviewees have been embedded throughout the main body of the study rather than being summarised in a separate standalone chapter or presented as a single set of disconnected comments.

1.4.3 Research Ethics

Ethical scrutiny and approval were sought to conduct the research, which was granted on the 20th of September 2016 by the ESSL, Environment and LUBS (AREA) Faculty Research Ethics Committee of the University of Leeds.

All participants were professionals over the age of 18 years. No participants or individuals from vulnerable groups were involved by this study. There was also no element of deception involved. No expenses were faced by participants (other than the time they spent for the interview), and they were not offered any financial or other inducements to take part in this study. The potential benefits for the participants were described as giving them the opportunity to share their knowledge and to take part indirectly in evaluating and making suggestions to enhance the capacity of the country. This study had no significant personal risks to the participants of a physical, emotional or financial nature.

Scope for any other conflict of interest was not present, given that the research findings were not affecting any ongoing relationship between any of the individuals or organisations involved and the researcher, and the research funder exercised no control over the compilation or publication of research findings. Ethical considerations were mainly concerned informed consent, confidentiality and data protection.

1.4.3.1 Informed Consent

All participants contacted and interviewed for the research were given an explanation of the purpose and nature of the research, what the research involved, its benefits, risks and burdens. An invitational and non-coercive tone was used in the information sheet (see Appendix 1), and participants were enabled to make an effective decision about participation. Based on this information, they were given a choice to decide freely and voluntarily whether to participate or not without giving any justification or explanation and without repercussion for the participant. Participants were also informed that they could decline to answer particular questions during the interviews without negative consequences.

Given that participants were trained and skilled individuals, they could be expected to easily comprehend the nature and goals of this research project and be able to evaluate the effect of taking part in it will have on them. However, complex explanations and terms were not used in the information sheet to avoid any misinterpretation and misunderstanding of the benefits and risks that the participation might bring. Participants were also provided with information regarding the methods applied to handle their data and the duration of data use, storage of data supplied by them and guarantees of the rightful use of data.[60]

For the participants to be able to consider fully the implications of taking part in research and to ask questions and reflect properly, each participant was given a minimum of 2 weeks to decide whether to get involved in the project or not. Individuals agreeing to take part were required to sign an informed consent statement, and after signing the form, participants received a copy of the signed and dated informed consent form. Moreover, to avoid the difficulties in adequately understanding written or verbal information in English, due to the nature of the work, all verbal explanations and written information were translated into Azerbaijani and sent to participants alongside with their English version. Moreover, the interviews were conducted in the native language (Azerbaijani) of the respondents to make sure respondents can fully understand the content.

[60] Lesley Noaks and Emma Wincup (n.47) 50.

1.4.3.2 Confidentiality

The review, opinions and suggestions of the respondents on the appropriateness of responses of the Republic of Azerbaijan to cybercrimes might be considered politically sensitive information. There was a possibility that some statements given by the participants about the governmental policy on fighting cybercrimes (especially the statements regarding the capacity of public institutions, the implementation level of relevant laws, and the effectiveness and efficiency of measures taken by the government) might become critical, so that its disclosure to any third party might put them at risk. Thus, the policy of non-disclosure to third parties and confidentiality of the raw information was ensured at all stages of the research in accordance with the UK Data Protection Act 1998 and data protection principles, except in cases of obtaining information 'about known preparing or committed minor serious or serious crimes' according to Article 307 of the Criminal Code of the Republic of Azerbaijan 1999. Here it is significant to note that the possibility of obtaining information 'about known preparing or committed minor serious or serious crimes' was extremely low since the content of interviews mainly consisted of experts' general views on cybercrime. It is also worth to note that the participants were either government sector representatives or members of information security society, therefore, they could be expected to use their experience to avoid any passing on any information which needs to be disclosed to any third party or which its non-disclosure constitutes a criminal liability. No such information was disclosed during the interviews.

Although the risk of obtaining sensitive information was very low, recognising this possibility, measures were taken to minimise its risks. Firstly, the interviewees were provided with full information and explanation of the purpose, nature and content of the research, its benefits (or lack of benefits), risks and burdens beforehand through the information sheet.

Secondly, the risks of giving sensitive information were reiterated to the participant before the start and during the interviews in cases of any possibilities of disclosing sensitive information.

Thirdly, the final research outputs did not comprise any information leading to or allowing the identification of individual participants.

Moreover, recognising that, the breach of confidentiality and anonymity can put participants at risk, privacy and data protection issues were dealt with utmost care and the data collected have been anonymised and kept confidential.

1.4.3.3 Managing and Safeguarding Data

The interviews have been used only for this research. All the data obtained (the written and electronic documents, signed informed consent forms) regarding the fieldwork research have been managed in accordance with the Policy on Safeguarding Data - Storage, Backup and Encryption[61] and stored with the project's main documents in a secure location (and in a safe computer system) with locks and passwords at the University of Leeds accordingly with the data protection and management policies and protocols of the University. University computer storage, particularly on its 'M' drive, was used for storing the electronic data. Encryption software has been used in cases where it was necessary to use other devices for storing the data. The data was uploaded onto a secure server or desktop as soon as possible and was removed from the portable device by using appropriate data destruction software.

All the information collected about the participant during the research has been and will be kept confidential. The participants' identity has not been and will not be identifiable in any reports or publications and will be anonymised in the final research outputs. The inclusion of the information leading to the identification of the respondent have been avoided, and direct quotes have been entered the research outputs only in an anonymised form. Audio recording devices have not been used during the interviews due to the traditional preferences and to ensure the confidence of the participants, to avoid potential risks and to encourage frank answers. Notes taken were transcribed within three days. After the transcription of

[61] 'Information Security Management Policy on Safeguarding Data – Storage, Backup and Encryption', (*It.leeds.ac.uk,* 2018) see http://it.leeds.ac.uk/info/116/policies/255/policy_on_safeguarding_data-storage_backup_and_encryption

the interview, paper notes of the interview were destroyed. Moreover, the anonymity of transcripts has been ensured, by not including any personal data of the participant. The transcripts and identification data have been stored in separate secure files (protected with passwords).

1.4.4 Policy transfer

Technology can push governments into policy transfer because of the speed with which it forces change. Governments, not knowing how to deal with the issues technological advances create, turn to each other for precedents and ideas.[62] Policy transfer refers to a 'process in which knowledge about policies, administrative arrangements, institutions and ideas in one political setting (past or present) is used in the development of policies, administrative arrangements, institutions and ideas in another political setting'. [63]

After critically evaluating the appropriateness of the policy and legal responses of Azerbaijan in combatting and preventing cybercrimes, and defining and summarising the deficiencies and needs for possible improvements through doctrinal and empirical research, the results have been addressed from the relevant UK perspectives. To make suggestions for enhancing the responses of Azerbaijan, lessons have been drawn from the UK by adopting the voluntary transfer form, which is 'a rational, action-oriented approach to dealing with public policy problems' and does not involve any degrees of coercion.[64]

Due to the differences in national circumstances, political and legal contexts between the two countries, positive and negative lessons have been incorporated through 'emulation'[65] and 'hybridisation'[66] processes. Although 'direct copying of an

---

[62] David P. Dolowitz and David Marsh, 'Who Learns What from Whom, A Review of Policy Transfer Literature' (1996) XLIV *Political Studies*, 349.
[63] David P. Dolowitz and David Marsh, 'Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making' (2000) 13 *Governance*, 5.
[64] Mark Evans, *New Directions in the Study of Policy Transfer* (Routledge 2010) 8.
[65] Emulation refers to the 'adoption, with adjustment for different circumstances, of a program already in effect in another jurisdiction', Richard Rose, 'What is Lesson-Drawing?' (1991) 11 *Journal of Public Policy*, 22.
[66] Hybridization is referred to the combination of elements of programs from two different places. See: Ibid.

idea, policy or programme from another jurisdiction'[67] is involved in the process of emulation, it is also significant to add that, adjustment to different circumstances is allowed by this process which aids to suit varying needs of the adopter.[68] The process of emulation helped to ensure the effectiveness of policy transfer and give the flexibility in proposing ways for overcoming the challenges posed by the differences. Moreover, this process can also allow finding out the gaps and making suggestions to improve the original policy or program.

The process of hybridisation supplied additional flexibility to lesson drawing and increase its chances of success through allowing the combination of the recognisable elements of UK's and Azerbaijan's relevant programmes where incompatibility or absence of necessary elements was encountered. Furthermore, hybridisation is also believed to allow the development of policy, which is 'culturally sensitive to the needs of the recipient'.[69] Consequently, the adoption of policy transfer through the application of emulation and hybridisation processes can allow ideas for more effective and efficient ways to enhance the capacity of institutions in combatting cybercrimes and ensure better protection and promotion of the rights on the Internet.

[67] Trevor Jones and Tim Newburn, *Policy Transfer and Criminal Justice* (Open University Press 2007) 127.
[68] Adam J. Newmark, 'An Integrated Approach to Policy Transfer and Diffusion.' (2002) 19 *Review of Policy Research,* 153.
[69] Mark Evans, *New Directions in the Study of Policy Transfer* (Routledge 2010) 9.

CHAPTER 2: The Problem of Cybercrime in Azerbaijan

2.1 Introduction

The focus of this chapter is on examining the perception and reality of cybercrime in Azerbaijan and identifying the extent of the problem presented by cybercrime to the country. It sets out the discussion by elaborating what is incorporated or omitted by the term 'cybercrime' and clarifying the range of acts which this thesis aims to study and provides the definition and categorisation of cybercrime. The Chapter then moves on to provide background information on the application of ICTs in Azerbaijan and the opportunities and challenges of fighting cybercrime to ensure early understanding of the problem.

Given that understanding the nature and prevalence of threats and vulnerabilities is crucial for raising 'the importance of investing in protection and prevention against cybercrimes',[70] this chapter later examines the scale and impact of cybercrimes in Azerbaijan as well as causes linked to changes in its harmfulness.

The last section of this chapter is concerned with setting standards for the primary measurement criteria to be used for the evaluation of responses throughout the main body of this research.

2.2 Definition and Classification of Cybercrimes

Although computer crime or computer-related crime is a relatively long-established phenomenon, the growth of connectivity and broader ICT use is inherent to this evolution and transformation, and to contemporary cybercrime.[71] The purpose of this study is not to define 'cybercrime' *per se*. Nor does this study focus on determining whether cybercrimes should have a particular status. However, to ensure consistency, it is conducive to be clear about the range of acts comprised by this term. Given the overlap between the international and national approaches on determining the acts constituting cybercrime, a working definition of cybercrime

[70] The UK Cyber Security Strategy (2011) (n. 9) 2.12.
[71] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (United Nations 2013) 5.

and a speculative set of actions that may be embraced by this term must be introduced to establish a basis for consistent analysis throughout the research.

2.2.1 The term 'cybercrime'

Existing definitions and categorisations of 'cybercrime' provided by numerous academic works and publications still differ to a noticeable extent.[72] Although the existence of cybercrimes is widely recognised and agreed, there is a great ambiguity on what they consist of and what is the extent of their harmfulness.[73] The lack of a unanimously agreed definition of this term is due to the differing perception of both observer/protector and victim and is partly a function of computer-related crimes' jurisdictional evolution.[74] 'Cybercrime' has been recognised neither as a legal nor as a forensic term, and a single reference point in international and national law does not exist. The lack of uniformity over the definition of cybercrime also has implications for defining and discussing the challenges presented by cybercrime to law enforcement, as emphasised by the European Parliament.[75] Thus, to avoid ambiguity associated with the term cybercrime, it is essential to clarify what is meant by this term and identify a list of acts, which could constitute cybercrime for this thesis.

---

[72] see for example, Samuel C McQuade, *Understanding and Managing Cybercrime* (Pearson/Allyn and Bacon 2006); Peter Grabosky, 'The Global Dimension of Cybercrime' (2004) 6 Global Crime; David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007); Ian Walden, *Computer Crimes And Digital Investigations* (Oxford University Press 2007); Stefan Fafinski, *Computer Misuse* (Willan Pub 2009); Susan W Brenner, *Cybercrime: Criminal Threats from Cyberspace,(*Praeger 2010*)*; UNODC, *Comprehensive Study on Cybercrime, 2013;* Majid Yar, *Cybercrime And Society* (SAGE Publications 2013); ITU, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (2014); David S. Wall, 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds) *The Oxford Handbook of the Law and Regulation of Technology* (Oxford: Oxford University Press 2017).

[73] David S. Wall, 'Locking up Hackers Could Do More Harm than Good' (*The Conversation, 2018*) http://theconversation.com/locking-up-hackers-could-do-more-harm-than-good-15889.

[74] Sarah Gordon and Richard Ford, 'On the Definition and Classification of Cybercrime' (2006) 2 *Journal in Computer Virology*, 13.

[75] Ben Hayes et al., *The law enforcement challenges of cybercrime: are we really playing catch-up?* (European Union, Brussels, 2015) 12.

So far, a definite categorisation of criminal offences has not been elaborated, and terms used to describe 'cybercrime' are almost as many as cybercrimes.[76] McQuade identified it as a broad term that incorporates the 'use of computers or other electronic devices via information systems such as organisational networks or the Internet to facilitate illegal behaviour'.[77] It is often used interchangeably with 'computer crime', 'Internet crime', 'digital crime', 'crime online', 'IT crime', 'electronic crime', 'virtual crime', 'high-tech crime', 'technology-enabled crime'.[78] Both legally, and technically, these terms imply different meanings, and despite having gradually changed along with the evolution of ICTs and advent of the Internet, each of these terms is limited and deficient in one or another way.

The United Nations Manual on the Prevention and Control of Computer-Related Crime (1994) focused on 'computers' and determined fraud on computer manipulation, computer forgery, damage to or modifications of computer data or programs, unauthorised access to computer systems and service, and unauthorised reproduction of legally protected computer programs as common types of computer crime.[79] It can be inferred that these early formulated offences that bear no connection to a network, but only affect stand-alone computer systems, are also covered by the concept of computer-related crimes and in this sense, are broader than cybercrimes, which are considered to affect only networked computers and Internet.[80]

As Grabosky stated, although involvement of the Internet is considered to be integral to the term 'cyber' and, therefore, to 'cybercrime', it is used more broadly to refer to crimes committed using stand-alone computers as well.[81] For example, the Draft International Convention to Enhance Protection from Cyber Crime and

[76] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2010) 9.
[77] Samuel C McQuade, *Understanding and Managing Cybercrime* (Pearson/Allyn and Bacon 2006) 16.
[78] See n. 72.
[79] United Nations, *UN Manual on the Prevention and Control of Computer Related Crime* (1994) 10-13.
[80] ITU, *Understanding Cybercrime* (2014) 11; see also Douglas Thomas and Brian Loader, *Cybercrime* Law *Enforcement, Security and Surveillance in the Information Age* (Routledge 2000) 3; Majid Yar, *Cybercrime and Society* (SAGE Publications 2013) 9.
[81] Peter N. Grabosky, *Electronic Crime* (Pearson Prentice Hall 2007) 2.

Terrorism (Stanford Draft International Convention*),* provided a broad definition of the term by determining cybercrime as a conduct, with respect to cyber systems - which means 'any computer or network of computers used to relay, transmit, coordinate, or control communications of data or programs'.[82]

Compared to the Stanford Draft International Convention*,* a definition of cybercrime is not contained in the Convention on Cybercrime. However, the term 'cybercrime' is used herein in a broader sense, referring to offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences, and offences related to infringements of copyright and related rights.[83] The term can be argued as being used not only to 'signify the occurrence of harmful behaviour that is somehow related to the misuse of a networked computer system',[84] but also symbolises insecurity and risk offline. Coupled with the approach taken by the Convention, it can, thus, be claimed that the term 'computer-related crimes' is narrower than 'cybercrime' and covered by the latter.

The UK Home Office tried to introduce a more practical and functional approach to defining cybercrime in the Serious and Organised Crime Strategy in 2013 by referring to two distinct, but closely related, criminal activities - cyber-dependent crimes, and cyber-enabled crimes – when using the term 'cybercrimes'.[85] This approach also recognises that cybercrime could start online while ending up offline. The Strategy identifies Cyber-dependent crimes as those that can only be committed using computers, computer networks or other forms of information communication technology (ICT).[86] In the research report published by the City of London Corporation in 2015, the requirement of having the networked information and communications technology (ICT) via the Internet has been attached.[87] Thus,

---

[82] Article 1, Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, *(*Stanford Draft 1999).
[83] Council of Europe, Convention on Cybercrime (2001) ETS No. 185.
[84] David S. Wall, (n.6) 10.
[85] Home Office*,* Serious and Organised Crime Strategy (London: Home Office, 2013) 22.
[86] Ibid.
[87] Michael Levi et al., *The Implications of Economic Cybercrime for Policing* (London: City of London Corporation, 2015) 3.

according to the report, cyber-dependent crimes could not be committed without the Internet.[88] The Home Office identifies Cyber-enabled crimes (such as fraud, the purchasing of illegal drugs and child sexual exploitation) as traditional crimes which 'can be conducted on or offline, but online may take place at an unprecedented scale and speed'.[89] These crimes are not completely dependent on the facilitation of ICT-connected technologies, and therefore, the crime could still take place without those technologies. However, the main rationale behind the concept is that cyber-enabled crimes are those that can be 'carried out at scale for less capital and sometimes with fewer criminal staff than would be needed for similar crimes offline'.[90]

Given that Azerbaijan is a signatory to the Convention on Cybercrime, the approach taken by the Convention has inevitably influenced the national legislation. The criminalisation approach adopted in Azerbaijan, as well as definitions of surrounding concepts, are thoroughly examined in Chapter 4. At this stage, it is crucial to emphasise that the national legislation has not contained any definition of cybercrime. Nor has a working definition of cybercrime been included, which has resulted in ambiguity over the term 'cybercrime', even among those directly involved in cybercrime control and prevention in Azerbaijan. The lack of uniformity on the definition of cybercrime was also noticeable from the answers provided by the interviewees in Azerbaijan.

A comprehensive study cannot be satisfied by researching only the offences included in the Criminal Code (1999), given that it is comparatively limited and narrow in determining the potential set of acts that constitute cybercrimes. Therefore, adoption of the approach taken by the Convention while addressing this issue would be more conducive to achieving the objectives of this study. This approach would also be useful due to the importance of the Convention on the establishment of international cooperation, which is crucial in combatting cybercrimes. To develop successful international cooperation against cybercrimes,

[88] Ibid.
[89] UK Serious and Organised Crime Strategy (2013) (n.85).
[90] Michael Levi et al. (n. 87).

national laws should be harmonised in a way that does not diminish the effectiveness and efficiency of international cooperation by creating problems arising from discrepancies between national laws and regulations.

At this point, it is important to note that this study covers not just the offences covered by the Convention on Cybercrime because the Convention also places some limits in defining the acts constituting cybercrimes. For instance, only the offences related to child pornography have been nominated as 'content-related offences'.[91] This approach diminishes the extent of cooperation among member states in combatting other offences related to adult pornography, racist statements, hate speech, information inciting violence and terrorism, illegal gambling and online games, offensive communications, extortion and other forms of illegal content. Thus, a broader approach is adopted throughout this study to serve its objectives. All the acts and offences that are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace,[92] and those that can be 'carried out at scale for less capital and sometimes with fewer criminal staff than would be needed for similar crimes offline'.[93]

2.2.2 Classification of cybercrime

Due to the underdeveloped and limited features of the Convention and national laws, it is helpful to identify the set of acts which could constitute cybercrime for this research not only in accordance with the approach adopted by the Convention or national legislation but also referring to relevant academic works and publications.[94] Although the development of a single classification for cybercrime is challenging due to the inclusion of a wide range of possible offences under this term, there is a broad consensus as to what is encompassed by this term, and

[91] Title 3, Council of Europe Convention on Cybercrime (2001) ETS No.185.
[92] These acts and offences are referred to as 'true cybercrimes' by David Wall. See David S. Wall, (n.6) 47-48.
[93] UK Serious and Organised Crime Strategy (2013) (n. 85).
[94] See n. 72.

several academic works have maintained a similar approach.[95] Current procedures regarding the categorisation of cybercrimes vary depending on the selection of a sole criterion as a base, for instance, the objects, features or *modus operandi*.

As one of the earliest authors to study cybercrime, David Wall proposed a four-fold cybercrime categorisation. He differentiated between (1) cyber-trespass (violation of a person's cyber boundaries); (2) cyber-deceptions/thefts (stealing a person's money or property); (3) cyber-porn and obscenity (the publication or trading off sexually expressive materials within cyberspace); and (4) cyber-violence (violent impact of cyber activities upon an individual or a social or political grouping, e.g. stalking, hate speech, etc).[96]

Although the typology proposed by Wall is considered as one of the most comprehensive frameworks to analyse and understand the incorporation of technology into various forms of offending,[97] it would be difficult to ensure the completeness of current study by primarily relying on this model, even though both the Criminal Code of Azerbaijan and this typology focus on the end-result of criminal acts. This is because identifying which crimes are new and which are new forms of existing offences is not helped by this typology, and the system does not necessarily take into account technological innovations and advancements, and therefore, some of the newer forms of offences.[98] Consequently, the four-fold categorisation proposed by Wall leads to the overlap with other offences that are considered a crime regardless of the involvement of computers or computer systems in its commission. Separating the traditional crimes committed via ICT can lead to confusion as it might include a wide range of otherwise 'offline' crimes. Moreover, given the rapid transformation of crimes and changing perceptions on what is considered deviant behaviour in cyberspace, it is crucial to work with a typology that is more flexible, yet also simpler in defining and criminalising acts.

---

[95] See for example, Peter Grabosky, 'The Global Dimension of Cybercrime' (2004) 6 *Global Crime*; David Wall, (n. 6);

[96] David S. Wall, 'Cybercrimes and the Internet' in *Crime and the Internet*, edited by David S. Wall. (New York: Routledge 2001) 3-7.

[97] Thomas J. Holt and Adam M. Bossler, 'An Assessment of the Current State of Cybercrime Scholarship' (2013) 35 *Deviant Behavior*, 21

[98] Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates* (Routledge 2015) 6.

Compared to the four-fold categorization, a tripartite or three-stage classification addresses the problem of defining whether the committed cybercrime is a new form of an offence or merely is a previously existing offence carried out in a new way. Alongside several academics, this categorization is also adopted by the US Department of Justice in 1996,[99] and can be summarised in accordance with Wall's categorization in the following way: [100]

1) Crimes against the machine or Computer integrity crimes;

2) Crimes using the machine or Computer-assisted crimes;

3) Crimes in the machine or Computer-content crimes;

All three categories have been embodied by the categorization adopted in the Convention on Cybercrime.[101] Furthermore, the Convention determined the 'offences related to infringements of copyright and related rights' as a separate category, which can be covered by the above categories.

The categorization by the Convention is not based on a single criterion. The criterion for the first category is the object of legal protection, while the classification of computer-assisted offences is based on the *modus operandi*. In this respect, some overlap between categories is caused by the inconsistency of this classification and some terms used for describing criminal acts cover acts that fall within several categories.[102]

Given the advantages of the tripartite categorization, which is also mostly compatible with the approach adopted by the Convention, it would be more suitable to set the range of acts comprised by the term 'cybercrime' based on the tripartite typology. However, the core rationale behind the establishment of the speculative set of acts under each category is different from that adopted by the Convention, which primarily concerns with the national criminal justice context and criminalisation approach.

---

[99] US Department of Justice, *The National Information Infrastructure Protection Act of 1996*, (Legislative Analysis 1996).

[100] Ibid; see also, David S. Wall, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace', (2007) 8 *Police Practice and Research*, 185-186.

[101] See Titles 1, 2, 3 and 4. Council of Europe, Convention on Cybercrime (2001) ETS No.185.

[102] International Telecommunication Union, *Understanding Cybercrime* (2014).

2.2.2.1 Computer integrity crimes

The development of computer networks and the Internet has led to the evolution and proliferation of computer integrity crimes. The objects of these crimes are the confidentiality, integrity and availability of computer systems or computer data. These crimes are committed in the form of unlawful intrusions into computer networks and the disruption or downgrading of computer functionality and network space.[103] Hacking, cracking, data espionage, spying, denial of service, and the planting of malware (viruses, Trojans, computer worms, etc.) can be determined as examples of computer integrity crimes, and these crimes pave the way to more serious forms of further offences.[104] Both the Convention on Cybercrime and the Criminal Code of the Republic of Azerbaijan identify illegal access, illegal interception, data interference, system interference and misuse of devices as crimes.[105] These acts fall within the established speculative set of acts that is comprised by the term 'cybercrime' and therefore, are thoroughly studied in Chapter 4.

2.2.2.2 Computer-assisted crimes

A common feature of computer-assisted crimes is that instead of being a target of the crime, computer technology is integral to the commission of these crimes. In comparison to computer integrity crimes, these acts target various objects by causing personal harms to individuals, breaching the protected intellectual property rights, conducting computer-related forgery or frauds against the economic property.

Computer systems and computer data can be ancillary to almost any criminal offence due to the ubiquity of the computer systems and digital evidence.[106] This feature poses a challenge to computer-assisted crimes by risking this category to

[103] Mike McGuire, Samantha Dowling, 'Cybercrime: A review of the evidence' - Chapter 1: Cyber-dependent crimes (2013) *Home Office Research Report 75*, 4-6.
[104] David Wall, (n. 6) 49.
[105] See: Articles 2-6, Council of Europe, Convention on Cybercrime (2001) ETS No. 185; Article 271-273, Criminal Code of the Republic of Azerbaijan (1999).
[106] Anthony Reyes*, Cyber Crime Investigations* (Syngress Pub 2007) 158.

be extended to include a wide range of almost an infinite number of otherwise 'offline' crimes. Therefore, not all the acts involving computer technology in its commission are included in this study. Acts that could be perpetrated without the use of computer technologies are excluded, except those that can be 'carried out at scale for less capital and sometimes with fewer criminal staff than would be needed for similar crimes offline'.[107]

According to the ITU, computer-related fraud, computer-related forgery, phishing, identity theft and misuse of devices are covered by this category.[108] However, only computer-related forgery and computer-related fraud have been identified as computer-related criminal acts by both the Convention on Cybercrime and the Criminal Code of the Republic of Azerbaijan.[109] Misuse of devices is covered under the category of 'computer-integrity crimes' in the Convention.[110]

For the purposes of this study and in accordance with the established set of acts besides computer-related forgery and computer-related fraud, online intellectual property theft, spam, phishing, as well as computer-related identity theft are covered by this research.

2.2.2.3 Computer content crimes

The development and ease of availability of ICTs, as well as pervasiveness of the Internet, have given rise to content-related offences.[111] The concern of this category is the content that is considered so wrongful as to be illegal and produced, transmitted or stored by computer systems, networks or other electronic

[107] Michael Levi et al. (n.87).
[108] ITU (n. 102), 31.
[109] See: Article 7 and Article 8, Council of Europe Convention on Cybercrime (2001) ETS No. 185; Article 273-1, Criminal Code (1999).
[110] See: Article 6, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[111] Jonathan Clough (n.76), 247.

devices.[112] The commission of these acts may reflect social or individual pathologies.[113]

It has been challenging to reach a consensus on defining the provisions of illegal content due to extensive variations in normative values and legal systems, which directly influence national approaches. More specifically, the potential conflict with freedom of expression has been the main concern during the establishment of the criminalisation approach. Consequently, although other offences related to pornography, racist statements, hate speech, information inciting violence and terrorism, religious offences, illegal gambling and online games, offensive communications, and extortion can all be considered as containing 'illegal' content, depending on the values of a given society, only child pornography has been criminalised by the Convention on Cybercrime.[114] Explanatory Report to the Convention on Cybercrime specified the 'unlawful production or distribution of child pornography by use of computer systems as one of the most dangerous *modi operandi* in recent times'.[115]

In addition to child pornography, acts such as 'Illegal distribution of pornographic materials or objects', 'Incitement to national, racial, social or religious hostility', 'Libel' and 'Insult' have been identified as crimes by the Criminal Code (1999).[116] Besides, 'Public appeals directed against the state', 'Violation or humiliation of the honour and dignity of the head of the state' have also been criminalised.[117] These reflect the value choices of Azerbaijani society.

Although these offences can still be committed without the use of ICT, the use of ICTs and the Internet has increased the scale or reach of these offences and provided vast opportunities and grounds for their commission. Therefore, criminalisation provisions of these offences are also briefly elaborated in Chapter 4 to create the whole picture of national criminalisation context and sensitivities.

---

[112] Robin Mansell, Peng Hwa Ang and Pieter Ballon, *The International Encyclopedia of Digital Communication and Society* (1st edn, John Wiley & Sons 2015) 118.
[113] Cindy J. Smith, Sheldon Zhang and Rosemary Barberet, *Routledge Handbook of International Criminology* (Routledge 2011) 160.
[114] Article 9, Council of Europe, Convention on Cybercrime (2001) ETS No. 185.
[115] Council of Europe, *Explanatory Report to the Convention on Cybercrime* (2001) ETS No. 185,
[116] See: Articles 147, 148, 242, 244-1, 283 of the Criminal Code (1999).
[117] Ibid, Articles 281, 323.

2.3 ICT adoption and application in Azerbaijan

Azerbaijan has brought the development of ICT and the Internet into the centre of attention to reduce its dependency on the oil industry and further develop non-oil sectors since the beginning of the 21st century. The state has accomplished this priority for ICT through enacting various strategies. *The National Information and Communication Technologies Strategy for the Development of the Republic of Azerbaijan* (2003-2012) which was adopted in 2003 sought to assist country`s democratic development and set out the favourable environment for the transition to the information society through the wide application of ICT. The strategy identified and recognised the favourable impact of the ICT use on the overall development of the country, as well as on reducing poverty and solving socio-economic problems of the population.[118]

The process of ensuring sustainable development and improving the country's overall competitiveness is currently accomplished by the National Strategy of the Republic of Azerbaijan on the Development of the Information Society for the years 2014-2020. It was adopted in April 2014 in accordance with the objectives concerning the field of information and communication technologies, defined on the basis of the Development Concept 'Azerbaijan 2020: The Vision of the Future'. To establish modern governance in the country, the expansion of opportunities for using ICT and communication services, the creation of a reliable security system aimed at developing ICTs, the formation of national standards, as well as launching entirely digitised broadcasting across the country, and 100% application of e-government services are highlighted.[119] The *Concept* has been followed by investments in ICT applications and tools in Azerbaijan, such as e-government, e-education, e-commerce, and e-health, which are regarded as engines that trigger growth and development leading to productivity and quality improvements.[120] In 2016, strategic roadmaps were approved for enhancing the country's capacity in

[118] National Information and Communication Technologies Strategy for the Development of the Republic of Azerbaijan (2003-2012), 2003, 8.
[119] Development Concept 'Azerbaijan 2020: The Vision of the Future' (2012), 11.
[120] See for example, e-portals in Azerbaijan: www.e-gov.az www.e-resurs.edu.az - www.e-derslik.edu.az; www.e.telim.edu.az; www.video.edu.az http://e-health.gov.az/

various areas of the economy including telecommunication and information technologies.[121] Also, a special fund – the State Fund for Development of Information Technologies - was established under the Ministry of Communications and High Technologies to stimulate and finance innovation and development, as well as to provide financial support for the expansion of operative scientific researchers.[122]

As a result of pursuing the set targets, Azerbaijan has fulfilled 62% of the ICT development index (2017) which has placed the country in 65th place in the index.[123] Regarding the Networked Readiness Index (2016), Azerbaijan has fulfilled 61% of the maximum criteria, which placed the country in 53rd place in the index.[124] According to these indications, general ICT development in Azerbaijan appears to be above average.

The Internet user penetration has increased from 8% to 80% between 2005 and 2017,[125] and for mobile-broadband penetration and coverage, Azerbaijan is among the leaders in the CIS region.[126] Moreover, the implementation of a broadband Internet development project will make the society and information infrastructure not only capable of presenting more opportunities, but also more vulnerable to the challenges posed by the widespread use of the ICTs in Azerbaijan. This is because the project is aimed at covering the whole territory of the country with a fibre-optic network and ensuring 85% of broadband penetration by the end of 2018.[127] Also, according to the World Bank estimates, the number of secure Internet servers (per 1 million population) was only 13.5 in 2014 and 20.5 in 2016, which makes

[121] *Strategic road maps for the national economy and main economic sectors,* 2016 https://azertag.az/store/files/untitled%20folder/_STRATEJI%20YOL%20XERITESI_.pdf
[122] See for further information, http://ictfund.gov.az/?page_id=1373&lang=en
[123] ITU, *Measuring the Information Society Report 2017* (ITU 2017) 31.
[124] Silja Baller, Soumitra Dutta, and Bruno Lanvin, *The Global Information Technology Report 2016* (World Economic Forum 2016) 16.
[125] 7,799,431 Internet users as of 12/2017, 80.6% penetration rate Source: http://www.internetworldstats.com/stats3.htm, *see also,* Statistics provided by the State Statistical Committee of the Republic of Azerbaijan https://www.stat.gov.az/source/information_society/?lang=en.
[126] ITU, *Measuring the Information Society Report 2017*, 14.
[127] Development Concept 'Azerbaijan 2020: The Vision of the Future' (2012).

Azerbaijan 118th in the ranking.[128] For example, the number of secure Internet servers per million population in the United Kingdom was 1,291.[129] Development of secure internet servers is crucial for securing online transactions and protecting data from unauthorised interception.

It has also been aimed to make all services of Azerbaijan's government agencies online by 2020, to move to the platform of mobile e-government and deploy the services through using mobile devices via mobile applications.[130] Mobile market penetration has increased from 107% in 2013 to over 110% by 2017, as the number of individuals with two or more mobile phones keeps growing, and 100 per cent of the total population is covered by a mobile network signal in the country.[131] Thus, the accessibility of government services can be easily ensured throughout the whole country via mobile devices. At the same time, the digitisation of the vast amount of personal data and ease of accessibility have also increased the vulnerability of collected information against the threats, and therefore stronger protection and security methods and mechanisms are required.

2.4 Opportunities and challenges in fighting cybercrimes

There are specific opportunities and challenges in fighting cybercrimes, which facilitate crimes and create obstacles before the law enforcement in fighting these crimes. The rapid development of ICTs has created not only challenges and new criminal methods but also new opportunities, which expand the capacity of law enforcement in combatting cybercrimes.[132] While specific influences in a specific context are elaborated in subsequent chapters, it is important to provide an analysis of the main features of these challenges and opportunities to ensure early understanding of the phenomenon.

---

[128] Silja Baller, Soumitra Dutta, and Bruno Lanvin (n.124) 62; See also, the World Development Indicators of the World Bank available at https://fred.stlouisfed.org/series/ITNETSECRP6AE.
[129] Ibid.
[130] 'Azerbaijan to accomplish e-government project by 2020', The interview given by the Communications and High Technologies Minister (2014). accessed online at http://www.azernews.az/business/74290.html.
[131] Silja Baller, Soumitra Dutta, and Bruno Lanvin (n.124) 125; see also, Statistics provided by the State Statistical Committee of Azerbaijan https://www.stat.gov.az/source/information_society/?lang=en.
[132] ITU (n.102) 77.

2.4.1 Opportunities

Automated digital forensics and the traceability of online activities can be identified as opportunities in fighting cybercrime in cyberspace.

2.4.1.1 Automated digital forensics

The rising power of computer systems and sophisticated forensic software accelerates the speed of investigations and automates search procedures. These new powerful tools provided by the two-way flow of information not only enable investigations, but also aid the collection of new sources of evidence which can be utilised to secure prosecutions and convictions, and facilitate more efficient cybercrime control and prevention.[133] The importance also lies in the fact that compared to the early days of digital forensics when the pre-occupations mainly were 'hacking' and 'computer fraud', today digital evidence plays a crucial role in the investigation of most of the crimes.[134] Given that evidence and sources necessary for investigating cybercrime can be searched and collected automatically through the application of computer technology and forensic software, the amount of time spent on the investigation can be significantly decreased. Although evidence collection, processing and documentation are among the procedures which can be automated for investigations, current tools still focus on converting data to information, and more human interaction is still needed to analyse and draw conclusions.[135] More importantly, although the use of digital forensics can provide criminal leads and assist in the criminal investigation, it is difficult to apply modern tools, due to their complexity and the lack of properly trained personnel with relevant knowledge and experience.[136]

---

[133] David S. Wall, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' (2007) 8 *Police Practice and Research*, 195-196.
[134] Peter Sommer, 'Forensic Science Standards in Fast-Changing Environments' (2010) 50 *Science & Justice*, 15.
[135] See for further discussion; Eoghan Casey, *Digital Evidence and Computer Crime*, (3rd edn, Academic Press 2011) 39*;* see also, Joshua I. James and Pavel Gladyshev, 'Challenges with Automation in Digital Forensic Investigations', 2013 *Computers and Society*.
[136] See for further discussion: Thomas J. Holt, Adam M. Bossler and Kathryn C Seigfried-Spellar (n. 3), 323-342.

2.4.1.2 Traceability of online activities

Besides becoming a target for criminal activity, information stored on computers or communicated online also provides new means for law enforcement to solve crimes and prevent such activity.[137] Thus, the more ICT use expands and covers everyday processes, the more crimes incorporate some form of digital usage and the more data become available for law enforcement authorities.[138] Virtually every online activity leaves almost permanent traces that can be retained and collected. From the crime control and prevention perspectives, this implies that the more criminal actions involve the use of technology, the more it leaves digital traces and evidence and therefore becomes an integral part of the investigation and prosecution of crimes. This is also applicable to the commission of conventional crimes such as fraud, robbery, theft, or burglary, as well as for forms of organised crime.[139] Thus, the role and importance of computer technology are increasing not only in combatting 'true' cybercrimes but also for the investigation of conventional offline crimes.

Moreover, besides the evidence and sources incorporating criminal elements, a wealth of information regarding the ways the computer and its contents used is generated and stored by computer operating systems and programs. Also, as programs are used, that information, called metadata, becomes broader and more comprehensive.[140] On the one hand, Oimet has identified the traceability of online activities on the Internet as one of the three principal reasons that lower crime rates, 'as motivated offenders might refrain from crime once realising that they can be somehow identified'.[141] On the other hand, as Wall emphasised, the potential for online monitoring and the mining of the various databases of Internet traffic has been established by this feature.[142]

---

[137] Ben Hayes et al., *The law enforcement challenges of cybercrime* (EU, Brussels, 2015) 12.
[138] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar (n. 3), 16.
[139] UNODC (n. 71), 16.
[140] Orin S. Kerr, 'Searches and Seizures in a Digital World', (2005) 119 *Harvard Law Review* 542.
[141] Marc Ouimet, 'Internet and crime trends' in Frank Schmalleger and Michael Pittaro, *Crimes of The Internet* (Prentice Hall 2009)
[142] David S. Wall (n. 133), 196.

2.4.2 Challenges

Fighting cybercrimes incurs serious challenges besides opportunities. While fighting cybercrimes, there inevitably appear specific design challenges such as ease of availability of access, lack of control mechanisms, liability to automate certain processes, high speed of data exchange systems and constant technological development of the Internet and software. This list may be expanded by other design issues that vary from heavy reliance on ICTs, independence of location and presence at the crime scene, the popularity of the Internet and the number of internet users worldwide to information and computer devices, increasing network capacities and resources, anonymous communications and encryption technology.[143]

A further complicated issue relates to legal challenges which exist along with design ones and poses obstacles when dealing with cybercrimes. The main legal challenges of fighting cybercrimes are about ensuring the sufficiency of national criminal laws, harmonising new offences with international instruments, jurisdictional issues, the establishment of adequate instruments for investigating potential crimes, and lack of procedures for digital evidence. These legal challenges are studied in chapters 4 and 5 in the light of legal responses to cybercrimes and appropriateness of these responses, while design challenges are discussed below.[144]

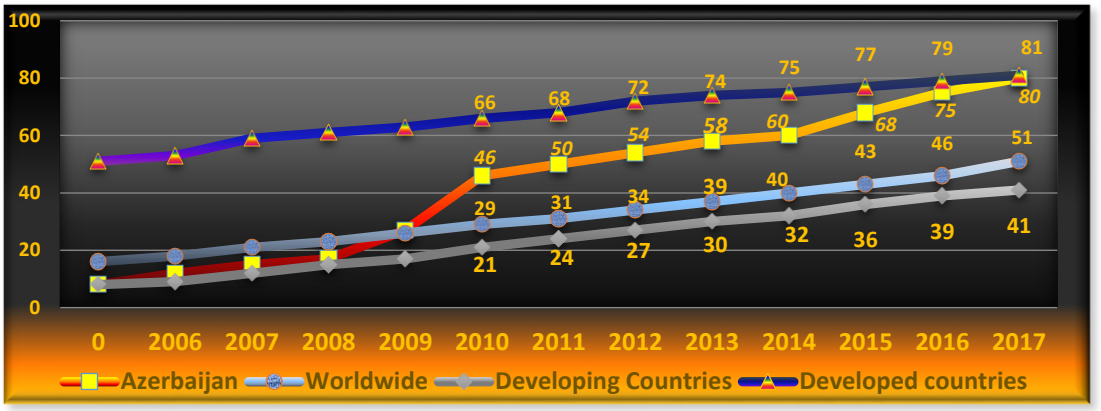
2.4.2.1 Scale of use

An expanded scale of applied innovation and changes makes it problematic to predict and understand the future of cyberspace and respond correspondingly to the sudden emergence of new vulnerabilities and risks.[145] The year 2017 was marked by Internet access by more than 3.9 billion people, comprising 51% of the world population.[146] Although higher levels of internet accessibility have been ensured in the developed countries (more than 82% of the population), the overall

[143] ITU (n. 102), 77-84.
[144] Ibid, 85-88
[145] The UK Cyber Security Strategy (2011) (n. 9).
[146] Internet World Stats, available at http://www.internetworldstats.com/stats.htm.

number of internet users in developed countries is outnumbered by the users in developing countries.[147] Also, the internet penetration rate increased from 8% to 80% between the years of 2005 and 2017 in the Republic of Azerbaijan,[148] which exceeds both the global internet penetration rate and almost twice more than the overall percentage of internet usage in the developing countries (see Figure 2.1)

Figure 2.1: Percentage of internet users between 2005 and 2017



Source: ITU, World Telecommunication/ICT Development Report and database, WEF-The Global Information Technology Reports.

Currently, the development of information and communication technologies and ensuring the transition to an information society is one of the leading priorities of the country for the upcoming years.[149] Thus, it can be suggested that besides enhancing the capabilities of human interaction, the broad application of ICTs and high rate of connectivity will assist the evolution and transformation of crimes in cyberspace. It can also be claimed that the number of suitable targets and motivated offenders increase through the growing proportion of people connected to the networked environment. More importantly, an increasing number of users and the networked environment allows offenders to easily multiply the scale of

[147] More than 2.1 billion (68%) internet users access the Internet from the developing countries. Information regarding the key ICT indicators for developed and developing countries retrieved from http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[148] 7,799,431 Internet users as of 12/2017, 80.6% penetration rate Source: http://www.internetworldstats.com/stats3.htm.

[149] Development Concept 'Azerbaijan 2020: The Vision of the Future' (2012) 20.

offending and consequently, it becomes more challenging to combat these acts and to automate the investigation processes.

While Azerbaijan is a country with a high percentage of internet users, most users have not yet acquired enough computer skills for self-protection in the event of cyber-attacks. As highlighted in the *Freedom on the Net Report*, most users become prone to security threats such as viruses and other malicious programs that could be implanted to monitor their activity by not using licensed software on their computers.[150] These factors reveal that not only the information infrastructure but also the rights and safety of individuals are adversely affected by the threats of cybercrimes.

2.4.2.2 Access to devices and information

Compared to previous decades, today computer technologies have become cheaper and more accessible, and thus, the utilisation of computers has expanded beyond government, research and financial institutions. In addition to this, as the technology is ubiquitous and easier to use compared to the past, it has become more available to both victims and offenders.[151]

Commission of crimes has also become more feasible due to the development of computer hardware, software and widely affordable Internet access. It is essential to add that serious computer crimes can be committed by cheap or second-hand computer technologies, through the assistance of publicly accessible specialist software tools.[152] Moreover, a wide range of information, which can also be facilitated for illegal purposes, is also available to offenders. The networked

[150] Freedom House, *Freedom on the Net 2014 Report*, available online at https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

[151] Jonathan Clough (n. 76), 5.

[152] See for example, software which ensure anonymity and illegal file sharing, such as TOR, I2P, FreeNet, ZeroNet, RetroShare, Syndie, OneSwarm and etc; see also: BlackShades – malicious malware used to control computers remotely; Aircrack-wireless passwords cracking tool; AirSnort - tool for decrypting WEP encryption on a wi-fi network; CloudCracker password cracking tool for cracking WPA protected wi-fi networks.

environment can also serve individuals by allowing them to interact with peers for exchanging their knowledge and experience to further their offending.[153]

The cost of internet access has been decreased as a result of a number of initiatives worldwide. According to *Measuring the Information Society Report 2014,* which provided that the price of an entry-level fixed-broadband plan declined by almost 70 percent globally in the period of 2008-2013: from an average of PPP$ 158 in 2008 to PPP$ 49 in 2013.[154] In 2016 internet access tariff per capita income (monthly) was only 0.3% in Azerbaijan.[155] Lower costs also mean a greater availability and easier access. Accordingly, the possibilities of becoming an offender or a victim have been increased. When it comes to civilian users, victims whose computer skills are limited may not ensure an adequate self-protection and thus, attempts to strike back may 'retaliate' against the wrong computer system.[156] The government, on the other hand, appears to have resorted to taking actions for restricting uncontrolled access to internet services for avoiding criminal abuse over the Internet, which, in turn, violates fundamentals rights and freedoms. Restrictions imposed by law enforcement agencies (LEAs) over the internet access in Azerbaijan are reflected upon in Chapter 3 and Chapter 5.

2.4.2.3 Speed, automation and storage

Central to the nature of the online environment is the ability of any transaction or other processes to be completed in a few seconds. Compared to the transportation or transfer of information in the offline environment, time delay is not a problem in cyberspace. Besides it being an advantage of the Internet, rapid transfer of data imposes serious challenges before the LEAs as it leaves extremely short period for investigation and collection of necessary evidence. Consequently, it becomes crucial for a successful investigation to make the response time correspondingly

---

[153] See for further discussion, George E Higgins and David A Makin, 'Does social learning theory condition the effects of low self-control on college students' software piracy?', (2004) 2 Journal of Economic Crime Management, 1–22.

[154] ITU*, Measuring the Information Society Report* (2014) 114.

[155] Stat.gov.az, 'The State Statistical Committee of the Republic of Azerbaijan' (2016) http://www.stat.gov.az/source/information_society/indexen.php accessed 20 October 2016.

[156] see Susan W. Brenner, 'Cybercrime: rethinking crime control strategies' in Yvonne Jewkes (Edn.) *Crime online*, (Cullompton, Devon: Willan, 2007) 19.

short. This in itself needs adequate legislative instruments allowing authorities to act rapidly and prevent the deletion of necessary data.[157] It is worth to note that there is a considerably big incompliance between the speed of traditional methods practised by LEAs in responding to cybercrimes, which is far too long,[158] and the rate of processes in cyberspace. Discussion on this incompliance in Azerbaijan is provided in Chapter 3 and Chapter 5.

The ability to automate specific processes is another advantage of ICTs allowing multiplication of particular activities by the help of openly and widely accessible software and computer programs. Multiplication also serves for automating criminal activities and scaling up attacks in a range that could not be possible in the physical space.[159] Hence, the possibility of the information exchanges potentiating a crime to be easily automated, replicated and cheaply distributed throughout the network multiplies the scale of criminal activity in cyberspace.[160] Consequently, not only the investigation of these acts becomes difficult for LEAs, but also the prevention of these offences and the protection of victims become challenging due to their multiplied number. The issue of protecting a boosted number of cybercrime attacks and victims due to the automation might become even more serious in Azerbaijan due to the lack of necessary resources.

From the discussion so far, it seems to be clear that the more ICTs integrate into daily life, the more data can be exchanged and stored by using digital technologies and the Internet. Besides, the continually undergoing development of ICTs also increases the storage and processing power, and as a result, a sheer volume of digital information is left before the LEAs to be sifted, sorted and analysed.[161] It poses even a more significant challenge in Azerbaijan where the country lacks both the technological equipment for investigations and sufficient law enforcement staff with the necessary knowledge and expertise in this field.

---

[157] ITU (n. 102), 83.
[158] Marco Gercke, 'The Slow Wake of a Global Approach against Cybercrime', (2006) 7 *Computer Law Review International,* 142.
[159] Phishing attacks, electronic spamming, denial of service (DoS) attacks can be given as examples to this. See for further information: Samuel C McQuade, *Encyclopedia of Cybercrime* (Westport, Conn.: Greenwood Press, 2009).
[160] David S. Wall (n. 6).
[161] Majid Yar, *Cybercrime and Society* (London: SAGE Publications, 2013) 144

2.4.2.4 Borderless nature and global dimensions

Cyberspace is ‘a communication network that is organised transnationally and not through the institutional structures of the state system’.[162] The transnational communication network means that the threats coming from this environment can easily become cross-border and elude or at least complicate state control. Thus, as the instances of cybercrime do not occur within the physical environment, they do not share the same features with the other forms of crime. The physical proximity of the perpetrator and victim to each other becomes unnecessary for the commission of an offence in cyberspace.[163] This feature of cybercrime eliminates the imposition of limits on what criminals can do and physical and temporal constraints on the execution and commission of the crime.[164] The elimination of physical constraints also exerts influence on the scope of cybercriminal activities. Because, as physical constraints do not impose limits on cybercriminals, they become capable of acting transnationally by utilising ‘globally interconnected network in which billions of users rely on common, standardised protocols, operating systems and applications’.[165] A UN study has demonstrated that over half of the responding countries reported that more than 50% of cybercrime acts encountered by police involved a ‘transnational element’.[166] It was claimed that most cybercrime acts reported and investigated by the Azerbaijani LEAs have also involved transnational dimensions.[167]

The application of traditional criminal laws in fighting transnational cybercrimes might not ensure the achievement of the desired outcome. This is because rather than the virtual perspectives, current approaches evolved by criminal laws traditionally focus on physical ones and are devised with territorial jurisdictions in

[162] Ronald J. Deibert and Rafal Rohozinski, ‘Risking Security: Policies and Paradoxes of Cyberspace Security’ (2010) 4 *International Political Sociology* 15-32, 16.
[163] Susan W. Brenner (n. 156), 16.
[164] Milton Mueller (n. 5), 162.
[165] Ibid.
[166] UNODC (n. 71), study cybercrime questionnaire. Q83; Percentage of cybercrime acts involving a transnational dimension was over 70% in responded European countries.
[167] Mehti Mehtiyev, ‘Fighting transnational organized crimes is the priority duty’ (‘Transmilli mütəşəkkil cinayətkarlığa qarşı mübarizə prioritet vəzifədir’), *Respublika qəzeti (newspaper)*, Baku 19.03.2013. also accessible online through http://www.mns.gov.az/az/pages/144-367.html

mind.[168] Therefore, actions taken against these crimes should correspondingly be transnational as improving domestic defence capabilities alone cannot ensure adequate protection. To put it differently, faster and stronger international cooperation is needed among the authorities in all countries affected by cybercrimes.

Convention on Cybercrime requires from the state parties to 'afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings' and 'to designate a contact point 'available on a twenty-four hour, seven-day-a-week basis'.[169] However, most countries, including Azerbaijan, encounter problems arising from discrepancies between legal systems and time issues (multi-layered steps and duration of official procedures).[170] In other words, international dimensions of cybercrimes leave the LEAs with a complex and challenging situation in conducting investigations and collecting digital evidence.

Actions taken in Azerbaijan to ensure international cooperation against cybercrimes are discussed in Chapter 3, 4 and 5.

2.4.2.5 Anonymity and encryption

Alongside the borderless nature of the Internet, anonymity is another feature making precise attribution of wrongdoing challenging and blurring the distinction between adversaries.[171] In most cases, organisations and people may never even realise they are being targeted until long after the damage is done because cybercrime operates mostly unseen.[172] Various tactics, such as using fake emails and spoofed IP addresses, proxy servers, anonymous communication servers, public Internet terminals or open wireless networks, are applied by offenders to

---

[168] Orin Kerr, 'Criminal Law in Virtual Worlds' (2008) University of Chicago Legal Forum, 416; See also Audrey Guinchard, 'Crime in virtual worlds: The limits of criminal law' (2010) 24 (2) *International Review of Law, Computers & Technology*, 175-182.

[169] Article 35, Council of Europe, Convention on Cybercrime (2001) ETS - No 185.

[170] Council of Europe, The Cybercrime Convention Committee (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,* 2014, 61-81.

[171] The UK Cyber Security Strategy (2011) (n. 9).

[172] PricewaterhouseCoopers LLP, *Global Economic Crime Survey,* 2014, 28. See also PricewaterhouseCoopers LLP, *Global Economic Crime Survey,* 2018. https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf.

conceal their identities. Also, an investigation of cybercrimes becomes even more painstaking and time-consuming where the computer data to be 'cracked' before they become legible are protected by openly and widely accessible, easy-to-use software tools and encryption technologies.[173]

Given that determination of the origin of communication and identifying the perpetrator is crucial for criminal investigation,[174] the possibilities of the Internet in ensuring confidentiality and anonymity complicate the investigations and poses serious challenges for law enforcement authorities. Because, as the digital environment enables attacks to be carried out remotely and anonymously, the likelihood of identification, capture, conviction, and punishment of criminals or agents of a nation-state becomes eroded.[175] Consequently, the perpetration of these attacks becomes easier, cheaper and safer for perpetrators.[176] Besides, perpetrators can easily evade prosecution if they reside in countries that will not impose any punishment on them.[177] This can be a reason why certain countries implement legal restrictions such as an authorisation requirement or licensing regimes.[178] To illustrate a similar limitation in Azerbaijan, according to the Rules of Mobile Devices Registration 2011, IMEI numbers of all devices which were brought to the country for personal use shall be registered within 30 (thirty) days period at the latest. However, there is not a legal restriction requiring the identification of users before they start using internet services in Azerbaijan.[179] Given that there are 107 mobile telephone subscribers per 100 population and 100 percent of the total

---

[173] Majid Yar (n. 161) 144. 'Encryption is the conversion of data into unintelligible cipher text that only authorized parties with an encryption key can read it'. For further information, see Michael Cross and Debra Littlejohn Shinder, *Scene of the Cybercrime* (Burlington, MA: Syngress Pub., 2008) 518-524.

[174] According to Article 304 of the Criminal Procedure Code of the Republic of Azerbaijan 2000, if the accused goes into hiding and his whereabouts are unknown the proceedings in the criminal case must be suspended.

[175] Susan W Brenner, *Cybercrime and the Law* (Boston: Northeastern University Press 2012) 2.

[176] National Audit Office, *The UK cyber security strategy: Landscape review, cross government* (House of Commons Papers 2013) 6.

[177] For example, see the legal implications of the origination of "ILOVEYOU" bug. See https://www.washingtonpost.com/archive/politics/2000/08/22/love-bug-virus-case-dropped-in-philippines/2ab9a2d0-e3b8-4fc2-bed6-ed541f230bbc/?noredirect=on&utm_term=.b321e9ef67c7

[178] For further information regarding the authorization practices and procedures of different countries see: http://www.ictregulationtoolkit.org/toolkit/3.6.

[179] Section 6.1. Rules of Mobile Devices Registration 2011, № 212.

population is covered by a mobile network signal in Azerbaijan,[180] identification of perpetrators who involved in criminal acts through mobile phones might ease the situation for LEAs to some extent. At the same time, perpetrators can easily avoid the rules requiring registration of authorisation for use by, for example, by means of unprotected private WI-FI networks, prepaid mobile phones or devices from countries not requiring registration.[181] In addition, implementation of this regulation can compromise user rights.

2.4.2.6 Lack of control mechanisms and resources

Open architecture networking or decentralised network architecture is a critical underlying technical idea embodied behind the Internet's network infrastructure, which makes it resistant to external attempts to govern.[182] Since the facilitation of criminal investigation or combatting crimes from inside the network was not incorporated in the design of the Internet's network infrastructure, it is based on protocols, which were projected in a way that does not require or need central control instruments for its being able to operate. Thus, combatting cybercrimes becomes onerous due to the absence of centralised state control mechanisms. In this sense, traditional investigation instruments established for dealing with crimes offline cannot prove to be sufficient in pursuing cybercrimes, due to the differences between the elements of cyber and physical offences. Investigation and prosecution of cybercrimes necessitate cyber-specific instruments and tools to achieve success. This is also due to the reason that technical solutions are as necessary as relevant legal instruments in dealing with cybercrimes, and these two elements together form the 'capable guardianship', the absence of which leads to the commission of a crime.[183]

---

[180] Soumitra Dutta, Thierry Geiger, Bruno Lanvin*, Global Information Technology Report 2015,* 125.
[181] See for further information, How internet?, 'How to Remain 100% Anonymous on the Internet?' (Security.stackexchange.com, 2015) http://security.stackexchange.com/questions/29196/how-to-remain-100-anonymous-on-the-internet.
[182] For further information regarding the history of the Internet, see Internetsociety.org, 'Brief History of the Internet - Internet Timeline | Internet Society' (2015) http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Origins
[183] Three variables are - a likely offender, a suitable target, and the absence of a capable guardian, coming together in time and space. See Lawrence E. Cohen and Marcus Felson, 'Social Change

All the three factors, indicated by Cohen and Felson, for the commission of a crime, notably the absence of capable protection mechanisms, embed challenges for Azerbaijan in tackling cybercrimes. The significance of investigatory powers and instruments is highlighted by the Explanatory Report to the Convention on Cybercrime.[184] It was recommended that the criminal procedural laws and investigative techniques, as well as safeguards, should also be adapted or developed to keep abreast of the new technological environment and further abuses, as do criminal laws and provisions.[185] Given that Azerbaijan lacks resources and instruments to pursue cybercrimes effectively and efficiently, special attention is needed in researching the ways of possible improvements. This issue is thoroughly addressed in Chapter 3, 4 and 5.

2.5 Nature and Prevalence of Cybercrime in Azerbaijan

An adequate analysis of legal and policy responses to cybercrime must avoid both exaggeration and misinterpretation of the scale of the problem. Having an accurate national picture about the true extent and magnitude of cybercrime is also crucial to inform future actions of controlling and preventing cybercrime. Although regarded as a large, complex, and lengthy task, mapping and measuring cybercrime is the key to inform crime reduction initiatives, enhance local and national responses.[186] In addition, accurate measurements are also needed to identify gaps in response and preventive measures, provide intelligence and risk assessment, facilitate reporting, educate and inform the public, and determine areas for further research.[187]

---

and Crime Rate Trends: A Routine Activity Approach' (1979) 44 American Sociological Review, 589;

[184] Council of Europe*, Explanatory Report to the Convention on Cybercrime* (2001) ETS No. 185 para. 132.

[185] Ibid.

[186] Stefan Fafinski, William H. Dutton and Helen Margetts, 'Mapping and Measuring Cybercrime', (2010) 18 *OII Forum Discussion Paper*, 4.

[187] Ibid.

It has been challenging to identify the most appropriate metrics to judge the threat and impact of cybercrime on national and human security.[188] Mike Hough determined the statistics of recorded crime and clear-up as the staple indicators for measuring the effectiveness in dealing with crime.[189] As one of the main indicators used to highlight the seriousness and impact of crimes, crime statistics are also often accounted when developing criminal justice, and crime prevention policies and strategies, and policy-makers use these statistics in support of the decision-making processes.[190] However, accurate quantification of cybercrimes is challenging as conventional methodologies of data collection have been undermined by the distributed environment of cyberspace.[191] In addition, according to a study conducted by the United Nations Office on Drugs and Crime, in contrast to its value and importance in national level crime prevention, police-recorded cybercrime statistics are not valuable and suitable for cross-national comparisons regarding cybercrime issues due to the variations in underlying offence elements in the respective criminal laws.[192]

The lack of consensus on defining 'cybercrime' and incorporation of the application of computers in crime statistics, the lack of definitive body of knowledge about cybercriminal statistics and the expertise/resources to pursue cybercrime, under-recording and under- and over-reporting of actual offending, as well as media reporting of a distorted picture of cybercrime can be identified among the factors making the accurate quantification challenging.[193] There also exists a punctuated continuum in the interplay between private, corporate governance and wider social risks and a sharp division between larger national security issues and cyber-attacks on banks, businesses and other public or the private sector institutions is

[188] Michael Levi, 'Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues' (2016) 67 *Crime, Law and Social Change*, 3-20.
[189] Mike Hough, 'Thinking about Effectiveness' (1987) 27 *British Justice Criminology Journal*, 70.
[190] Wayne N. Welsh and Philip W. Harris, *Criminal Justice Policy and Planning: Planned Change* (5th edn, Routledge, 2016).
[191] David Wall (n. 6) 17.
[192] See for further information: UNODC (n. 71), 259-262.
[193] See David S. Wall, 'Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime', (2008) 22 International Review of Law Computers and Technology, 45-63; Will Gragido and John Pirc, *Cybercrime and Espionage* (Syngress 2011) 9-10; Stefan Fafinski, William H. Dutton and Helen Margetts (n. 186).

not present.[194] Moreover, in many cases, public and private sectors underestimate the risks posed by challenges because of the covert or complex nature of the threats. As manifested in the Global Economic Crime Survey 2014, many entities lack 'clear insights into whether their networks and the data contained therein have been breached, and they don't know what has been lost — or its value'.[195] Not all victims of cybercrime are inclined to report due to legal and reputational risk concerns,[196] even if they can clarify their losses. For example, commercial victims sometimes prefer not to admit that they have been attacked to conceal their weaknesses from their customers and shareholders.[197]

Noticeably, methodologically sound national surveys measuring cybercrimes are currently unavailable in Azerbaijan. Reasonable evaluation of the extent and impact of cybercrime in Azerbaijan cannot be ensured by relying only on the limited information supplied by the law enforcement authorities. For example, as part of counter-actions against cybercrimes only 12 criminal investigations were conducted by the Ministry of National Security between 2009-2012, and 48 persons were brought to justice.[198] Thus, the scale and impact of online attacks are illuminated in the light of relevant international and security network reports and the information provided by respondents during the fieldwork in Azerbaijan as well as articles, news and reports publicised by the relevant ministries and the primary news outlets.

All the respondents involved in the interviews during the fieldwork in Azerbaijan have stated that in their views the number and potential of cybercrimes targeting the country and citizens have increased. This could also be deduced from the official statistics on cyber incident reports provided by the Computer Emergency Response Centre operating under Special Communication and Information Security State Agency of the Special State Protection Service of the Republic of

[194] Michael Levi (n. 188).
[195] PricewaterhouseCoopers LLP, *Global Economic Crime Survey,* 2014.
[196] ITU, *The ITU National Cybersecurity Strategy Guide* (Geneva, 2012).
[197] Susan W Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, Calif.: Praeger 2010) 171.
[198] Note: information regarding the cybercrime investigations are currently unavailable conducted by the Ministry has not been updated since 2012.

Azerbaijan. According to the statistics, the number of incident cases opened in 2014 was 1582, whereas, in 2016 almost 60% more cases (2704 cases) were reported to the Centre.[199] Also, the Kaspersky Security Bulletin 2014 demonstrated that Azerbaijan was third among the top 20 countries where users faced the most significant risk of online infection.[200] Computers of 49.6% of all unique users of Kaspersky Lab products in the country were targeted by web attacks in 2014, according to the Kaspersky Lab. However, the percentage of the users facing the risk of online infection gradually decreased to 38.8% in 2016[201] and to 34.7% in 2017.[202]

Besides individual citizens, both government and businesses have been widely influenced by cyber-attacks. In 2012, the websites of several Azerbaijani state bodies including the Ministry of Communications and High technologies (rabita.az), the Ministry of Interior (din.gov.az, mia.gov.az), the Constitutional Court (constcourt.gov.az), Azerbaijan's national airline AZAL and television station AzTV, the official news agency Azertag, the Baku city administration, the ruling New Azerbaijan Party (yap.org.az) underwent massive cyber-attacks and some were inaccessible for several hours.[203] In January 2013, the Anonymous hacker group targeted the Special State Protection Service (SSPS) of Azerbaijan and published

[199] See the official website of the Computer Emergency Response Centre https://cert.gov.az/az.
[200] Kaspersky, *Kaspersky Security Bulletin,* 2014, 32-33; Azerbaijan topped this ranking in 2013 where 56.29% of users faced the risk of online infection. see for further information, Kaspersky, *Kaspersky Security Bulletin* 2014, 42.
[201] Kaspersky, *Kaspersky Security Bulletin 2016*, 23.
[202] Kaspersky, *Kaspersky Security Bulletin 2017*, 22.
[203] Kamal Makili-Aliyev and Attiq-ur-Rehman, 'Cyber-Security Objective: Azerbaijan in the Digitalized World' (2013) 11 *SAM Review*, 11-12. see also, 'Mass Cyber-Attack Hits Government Websites' (*AzerNews.az*, 2012) https://www.azernews.az/nation/40349.html; 'Azerbaijani Official Websites Victimized by Cyberattack', (*Radio Free Europe Radio Liberty*, 2012), https://www.rferl.org/a/azerbaijani_websites_hacked/24454171.html; 'Patriotic Hackers' In Armenia and Azerbaijan Escalate Crisis With Cyber Attacks' (*Atlantic Council*, 2012) <https://www.atlanticcouncil.org/blogs/natosource/patriotic-hackers-in-armenia-and-azerbaijan-escalate-crisis-with-cyber-attacks>; 'Iran Cyber Army' Hits Azerbaijan State TV Site' (*Phys.org*, 2012) <https://phys.org/news/2012-02-iran-cyber-army-azerbaijan-state.html>; 'Azerbaijan Airline Websites, hit by Cyber Attack', (*The Daily Star*, 2012) http://www.dailystar.com.lb/News/Middle-East/2012/Feb-24/164417-azerbaijan-airline-websites-tv-hit-bycyber-attack.ashx#axzz2TRrsILKJ.

over 1.7 Gb of documents, allegedly stolen from dmx.gov.az website of the Service (SSPS).[204]

Freedom on the Net 2015 also reported that Azerbaijan encountered hacking attacks from Armenian internet protocol (IP) addresses during politically sensitive dates regarding the unresolved territorial conflict between the two countries.[205] Frequency and scale of cyber-attacks also originating from various Armenian politically motivated groups continued to rise in 2015, 2016 and 2017.[206] However, information regarding Armenian hacker attacks over the Azerbaijani internet users or information infrastructure, especially the information about their investigation has not been widely publicised. This in itself is another indication of the incomplete nature of the information given by state entities regarding cybercrimes. On the one hand, a similar type of relative information can be regarded as sensitive and kept confidential. On the other hand, excluding the true scale and extent of danger from official reports can disguise the local and international vision on cybercrime and thus, weaken the cooperation and prevention measures taken by potential victims.

Businesses have also been encountered with persistent cyber-attacks in Azerbaijan. Kaspersky Lab reported that in 2016, Azerbaijan-based companies

---

[204] *'1.7GB Documents leaked from Special State Protection Service of Azerbaijan. (Cyber War News, 2018).* https://www.cyberwarnews.info/2013/01/20/1-7gb-documents-leaked-from-special-state-protection-service-of-azerbaijan/.

[205] Freedomhouse.org, 'Azerbaijan | Freedom House', 2015 https://freedomhouse.org/report/freedom-net/2014/azerbaijan.

[206] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 65; See for attacks: '"Monte Melkonian Cyber Army" Hacks 47 Azerbaijani Websites' (*armenpress.am,* 2015) http://armenpress.am/eng/news/810768/%E2%80%9Cmonte-melkonian-cyber-army%E2%80%9D-hacks-47-azerbaijani-websites.html; 'Fighting Over Nagorno Karabakh Takes To Cyber Space | Eurasianet' (*Eurasianet.org*, 2016) https://eurasianet.org/fighting-over-nagorno-karabakh-takes-to-cyber-space; 'Armenian Hackers Leak ID Cards, Passports Of 5K Azerbaijani Citizens' (*HackRead,* 2015) https://www.hackread.com/armenian-azerbaijani-cyberwar/; 'CERT Warns Of Cyber Attack By Armenian Hackers', (*AzerNews,* 2015) http://www.azernews.az/azerbaijan/80903.html; 'Information Warfare: Armenia-Azerbaijan Cyber War Intensifies Amid Karabakh Clashes - Karabakh | Armenianow.Com' (*Armenianow.com*, 2016) https://www.armenianow.com/karabakh/71214/armenia_karabakh_azerbaijan_information_warfare; 'Cyber attack hits Azerbaijan International Development Agency website' (*Business Insurance*, 2015) http://www.businessinsurance.com/article/20150220/NEWS09/150229998/cyber-attack-hits-azerbaijan-international-development-agency-website; 'Azerbaijani Hackers Deface NATO-Armenia, Embassy Websites In 40 Countries' (*HackRead*, 2016) https://www.hackread.com/azerbaijani-hackers-defac-nato-armenia-embassy-sites/; see also '*Kaspersky Lab: Azerbaijan could come under increasing cyber-attacks in connection with geopolitical risks'*. (*En.apa.az,* 2016) http://en.apa.az/azerbaijan-economy/infrastructure/kaspersky-lab-nagorno-karabakh-conflict-increases-risk-of-cyber-attack-on-azerbaijan.html.

faced over 2.2 million cyber-attacks, and in total, 11,000 corporative computers underwent cyber-attacks in Baku.[207] Microsoft has warned Azerbaijan about the increasing number of cyber-attacks in 2016 and stated that 1/3 of cyber-attacks directed to Azerbaijan targeted energy, communication, telecommunication, defence industry and construction sectors.[208] Also, B2B International Company claimed that in 2016 each computer connected to the corporate network in Azerbaijan was attacked five times, which is twice more compared to 2015.[209]

The banking sector has been particularly prone to cyber-attacks in Azerbaijan. In 2013 an Iranian group called White Hat Hackers announced that it had already hacked the systems of eight Azerbaijani banks and gained access to the accounts of 53,634 of their clients to a sum of AZN 25 million and that these monies would be transferred to other accounts - of Iranian Royal Bank investors.[210] A news outlet has reported in 2016 that cybercriminal activities targeting Azerbaijani banks have also increased dramatically in comparison with previous years, although most of the attacks were not complicated, organised and powerful enough.[211] The State Security Service revealed one such attack by an international organised cybercrime group, stealing over 3 million AZN from Azerbaijani bank, in 2017.[212]

An article published by an employee of the Ministry of National Security of the Republic of Azerbaijan in 2013 indicated that illegal access, credit/debit card fraud, online money transfer fraud, illegal organization of international communications were dominating cybercrime acts during the past years according to the

---

[207] Kaspersky, *Kaspersky Security Bulletin 2016* (Kaspersky Lab 2016).

[208] 'Microsoft" has warned Azerbaijan' ("Microsoft" şirkəti Azərbaycana xəbərdarlıq edib) (*Report Information Agency,* 2016) https://report.az/i-kt/microsoft-sirketi-azerbaycana-xeberdarliq-edib/.

[209] 'Azerbaijani business faces cyber threat' (*AzerNews,* 2016) https://www.azernews.az/business/99644.html.

[210] The Digital Defenders Partnership (DDP), Insights into Internet freedom in Central Asia: Azerbaijan, (2013) https://www.digitaldefenders.org/azerbaijan/.

[211] 'Can Hackers steal money from Azerbaijani banks? – The number of attacks have been increased'. (*Hakerlər Azərbaycan banklarından pul oğurlaya bilərlərmi? – Hücumlar çoxalıb*) (*Publika.Az*, 2016). http://publika.az/news/tehlil/178593.html.

[212] *Information provided by the Public Relations Department, State Security Service* (2018). *Dtx.gov.az*. Retrieved from http://dtx.gov.az/news188.php; 'State Security Service reveals international cybercrime group stealing 3.7m AZN from Azerbaijani bank' (*Report.az,* 2017), https://report.az/en/incident/state-security-service-reveals-members-of-international-cybercrime-group-stealing-3-7-million-azn-fr/.

statistics.[213] The damage caused by cybercrimes was estimated at more than a half million US dollars,[214] which seems far from being a realistic estimation, especially given the number of attacks that took place in the previous years. In addition to the acts mentioned in the Ministry of National Security article, interviewees identified DoS and DDoS attacks, carding/phishing and other social engineering activities, and online libel among the highly concerning cybercriminal activities that require proportional attention.

It was also mentioned in the Ministry of National Security article that transnational elements were involved by most of the cyber-attacks and citizens from various countries, such as Bulgaria, Latvia, Spain, Russia, Turkey, Nigeria, Israel, Pakistan, and were caught up as a result of criminal investigations. This was also confirmed by the Minister of Communications and Information Technologies at the II Republican scientific conference of multidisciplinary information security devoted to the 150th anniversary of the International Telecommunication Union (ITU), where he stated that 90% of cyber-attacks are made from abroad.[215] However, during the interviews with employees of Electronic Security Service operating under the Ministry of Transport, Communications and Information Technologies in 2017 it was advocated that only 30% of the reported incidents involved transnational element.[216]

The alleged cyber-attacks from different foreign and local sources raise cyber-security concerns and demands a reliable internet and an adequate cybercrime control and prevention. Moreover, Azerbaijan has not only been targeted by cybercriminal activities. It has also been named among the emerging economies from where attack origins have continued to morph.[217]

---

[213] Note: the statistics mentioned by the author is not openly available or accessible.
[214] Mehti Mehtiyev (n. 167).
[215] 'Number of cyber-attacks in Azerbaijan increases annually by 30%'. (*Report News Agency,* 2015). https://report.az/en/ict/the-number-of-cyber-attacks-in-azerbaijan-increases-annually-by-30/.
[216] Interview with Ministry Officials 1, 2, 3, 4 and 5.
[217] 'Europe overtakes US' as the largest perpetrator of global cybercrime' (*Information Age*. 2017). http://www.information-age.com/europe-overtakes-us-largest-perpetrator-global-cybercrime-123466109/.

2.5.1 Root causes of the problem

Given that crime levels are influenced by various factors, it is not realistic to expect the law enforcement authorities to bring cybercrime rates down, when they do not control the root causes of cybercriminal behaviour. The range of factors can be attributed to the increasing scale of cybercriminal activities both targeting and originating from the country.

When considering the legal factors, it needs to be considered that underlying concepts of law and criminal law have been transformed by the complex and rapid changes in crime, which created asymmetries or discrepancies between jurisdictions.[218] Although the regulatory and legal framework for the ICT sphere has been significantly developed in Azerbaijan during the last 10 years, these laws and current capacity of LEAs do not adequately address the underlying social, economic and criminological factors of cybercrimes.[219] Also, the application of the same traditional law-making and social regulation methods 'developed within physical bounds of time and space'[220] might not give the same effect in the cyberspace, as it 'distances its inhabitants from local controls and the physical confines of nationality, sovereignty and governmentality'.[221]

From the technological point of view, along with transforming the nature of value, property and the offences based on property, constant innovations over the past few decades, development of computers and computer systems, as well as evolution of the Internet ensuring the interconnectedness in a worldwide scale have also transformed the crimes.[222] Given the rapid advancement of the ICT sector in Azerbaijan, it can be agreed that besides creating new opportunities for offenders

---

[218] Neil Boister and Robert J. Currie, *Routledge Handbook of Transnational Criminal Law* (Routledge, Taylor & Francis Group 2014) 379.

[219] In addition to the harmonisation of the Criminal Code of the Republic of Azerbaijan with the Convention on Cybercrimes, E-signature and e-document Law (2004), Electronic trade Law (2005), Law on State Secret (2004), Postal communication Law (2004), Telecommunications Law (2005), Law on Access to information (2005), E-commerce Law (2005), Law on Personal data (2010), the Decree on 'Measures in the field of improvement of the activities of the information security' (2012), the Decree on 'E-services' adopted in order to create and develop legislative basis for ensuring the transition to the information society.

[220] Yaman Akdeniz, Clive Walker and David S. Wall, *The Internet, Law and Society* (Longman 2000) 5.

[221] Ibid.

[222] Neil Boister and Robert J Currie (n. 218) 380.

and facilitating the growth of crime, unprecedented use of ICTs also provides ready access for users to an environment where they can easily turn into victims. Moreover, the high rate of application of digital technology is also crucial for conducting investigations and cooperating to combat transnational cybercrime. Therefore, the development of security measures in cyberspace should be installed at an adequate level, and national laws and law enforcement capacity should be amplified correspondingly with the transformation of crimes.

The interviewees have also identified geopolitical risks and bilateral issues, in particular, between Azerbaijan and Armenia, as well as between Azerbaijan and Iran among primary underlying factors associated to cyber-attacks, particularly, on social and critical infrastructure objects.

There are also socio-economic and human factors facilitating cybercrimes and operating as the inner drivers of this problem. As identified by most of the interviewees, low levels of cyber threat awareness and the lack of enlightenment campaigns among the public also increases the number of sucessful cyber-attacks.

Given the high scale use of the internet and electronisation, inadequate legislation and weak law enforcement action, as well as unstable geopolitical and socio-economic conditions and low levels of awareness, it can be suggested that Azerbaijan will come across with both the rising number of victims as well as offenders in the future. The growing realisation of the criminogenic potential of cybercrime and the risks associated should be met with appropriate responses. Forthcoming chapters are particularly focused on scrutinizing the appropriateness of the responses to cybercrime and presenting solutions and making recommendations for improving those responses.

2.6 Setting standards for ‘appropriateness’

In order for the responses to be appropriate in dealing with cybercrimes legality, effectiveness and efficiency of these responses should be ensured at all levels and stages. All the responses studied throughout this research are measured based on these three criteria. Following sub-sections explain these notions and justifies the reason for selecting these three particular values as assessment criteria.

2.6.1 Legality

Legality can be defined as the state or quality of conforming to the laws of a particular jurisdiction. Since the responses of Azerbaijan are studied, the legality of its responses should be measured in accordance with its laws and the international treaties to which Azerbaijan is a party.

The formation, harmonisation and development of a normatively sound legal base must be conducted in accordance with provisions of the Constitution of the Republic of Azerbaijan. According to the Constitution, 'the state guarantees protection of rights and liberties of all people'[223] without any 'restriction due to race, nationality, religion, language, sex, origin, conviction, political and social belonging'[224]. In addition, providing rights and liberties of a person and citizen is the highest priority objective of the state.[225] Besides other fundamental rights and liberties, the Constitution entitles everyone to a range of rights and freedoms the protection and implementation of which are mandatory.[226]

Alongside the constitutional provisions and national legal normative requirements, Azerbaijan has to fulfil its statutory and specific obligations as a Council of Europe member state and as a party to the major international human rights treaties; the International Covenant on Civil and Political Rights (ICCPR)[227] and European Convention of Human Rights and Fundamental Freedoms.[228] To put it differently, the legality of responses requires the conformity with both the national and international laws, standards and principles.

Moreover, as a signatory to the Convention on Cybercrime Azerbaijan should ensure that the establishment, implementation and application of the powers and procedures adopted by Parties to the Convention are 'subject to conditions and safeguards provided for under its domestic law which shall provide for the

[223] Article 26, Constitution of the Republic of Azerbaijan (1995).
[224] Ibid, Article 25.
[225] Ibid, Article 12.
[226] See for example, Ibid. Article 30, Article 32, Article 47, Article 50, Article 54, and Article 55.
[227] International Covenant on Civil and Political Rights (ICCPR) UN Doc. A/6316 (1966); Azerbaijan ratified the ICCPR in 1992.
[228] European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), (ETS No.5), entered into force: 3 September 1953. Signed in 25/1/2001 and ratified in 15/4/2002 by the Republic of Azerbaijan.

adequate protection of human rights and liberties …and which shall incorporate the principle of proportionality'.[229] The Convention establishes principles and requirements for ensuring that positive obligation of protecting individuals and their rights against cybercrime is proportionately met by governments while at the same time fundamental rights and liberties are respected by them when investigating crimes.[230] Moreover, the adoption of complete and effective legislation on cybercrime that meets human rights and the rule of law requirements have also been endorsed as one of the strategic priorities for cooperation against cybercrime.[231]

The international treaties to which Azerbaijan is a party constitute an integral part of the legislative system according to the Constitution.[232] The provisions of international treaties shall apply in case of a possible contradiction between normative legal acts of Azerbaijan and the international treaties to which Azerbaijan is a party.[233] To sum up, while combatting cybercrimes, restrictions imposed by any national action must comply with international law and legal obligations enshrined in the above-mentioned legal instruments.

2.6.2 Effectiveness and efficiency

Enhancing the responses of a country to cybercrime cannot be fulfilled by merely scrutinizing the legality of responses to cybercrimes. The appropriate fight against cybercrimes also needs these responses to be effective and efficient, because progress assessment must be carried out constantly to detect success or failure and adjust the strategy, policies, and laws accordingly.

The notion of effectiveness is defined as 'the degree to which objectives are achieved and the extent to which targeted problems are solved', whilst efficiency means 'achieving maximum productivity with minimum wasted effort or

[229] Article 15, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[230] Council of Europe, *Article 15 - Conditions and Safeguards under the Budapest Convention on Cybercrime* (CyberCrime@IPA 2012).
[231] Council of Europe, *Declaration on Strategic Priorities for Cooperation against Cybercrime in the Eastern Partnership Region* (CyberCrime@EAP project, 2013) 3.
[232] Article 148, Constitution of the Republic of Azerbaijan (1995).
[233] Ibid, Article 151, This rule is applicable in all possible contradictions except in the cases of contradiction with the Constitution of the Republic Azerbaijan and acts accepted via referendum.

expense'.[234] It is worth noting that, various approaches exist about the evaluation of national anti-cybercrime policies and cybersecurity strategies and consequently, metrics applied for measuring the effectiveness and efficiency of these strategies and policies vary.[235] In the case of 'crime-control', 'effective tends to be used to mean 'effective in dealing with crime'.[236] While the test of police efficiency is regarded as 'the absence of crime and disorder, not the visible evidence of police action in dealing with them'.[237]

Online risks cannot be completely averted by a single cybersecurity strategy or policy, and 'there will not be a "one size fits all" policy that is appropriate for all instances'.[238] Thus, the effectiveness of policy and legal responses of Azerbaijan should be measured by assessing the extent to which relevant national laws and enforcement are successful in addressing the threats posed by cybercrimes. Hence, success should be reflected by the structures, institutions, and resources in place and their adequacy in addressing and preventing threats, as well as results and outcomes achieved by the law enforcement. Meeting the human rights and the rule of law requirements are also essential for effective cybercrime legislation.[239] Therefore, the legality of responses can also be accepted as one of the baseline considerations for measuring the effectiveness of public responses.

It is also true that fighting cybercrimes calls for both public and private sector responses and cooperation at the national and international levels. Moreover, not only legal measures are needed for coping with criminal activities in cyberspace, but also technical measures and resources are crucial to control and prevent cybercrimes. Besides, an effective security strategy takes a multi-layered

---

[234] See http://www.oxforddictionaries.com/definition/english/.

[235] See for example: Responses from the Business and Industry Advisory Committee (BIAC), the Civil Society Internet Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC) to 'How should national cybersecurity strategies and policies be evaluated? What metrics should be applied to measure their efficiency?' differs in several ways. See Organisation for Economic Co-operation and Development*, Non-governmental perspectives on a new generation of national cybersecurity strategies* (Paris: OECD Publishing, 2012) 20-22.

[236] Mike Hough (n. 189), 70.

[237] Principle 9, *Sir Robert Peel's Principles of Law Enforcement*, 1829, https://www.durham.police.uk/About-Us/Documents/Peels_Principles_Of_Law_Enforcement.pdf.

[238] See (n. 235) 21.

[239] Council of Europe, *Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region* (CyberCrime@EAP project, 2013) 3.

approach, instead of single technology or solution.[240] It can also be added that education and training of people who are involved in prevention, detection, prosecution and report of cybercrime are required for implementing an effective anti-cybercrime strategy.[241] To sum up, to be effective in dealing with cybercrimes, the effectiveness of all of these elements must be satisfied.

Maintaining efficient regional and international cooperation is a necessary factor for achieving the effectiveness of protection from cybercrime.[242] More importantly, communication and cooperation in national, regional and international level should involve, and be supported, by all stakeholders.[243] As many interdependencies are comprised of public and private sectors in cyberspace, the cybersecurity challenges cannot be surmounted alone by any country, company or individual.[244] Therefore, as it has been stated by the UN General Assembly Resolution 64/211, 'governments, business, organizations and individual owners and users of information technologies must assume responsibility for and take steps to enhance security'.[245]

2.7 Conclusion

This Chapter has focused on examining the problem of cybercrime in Azerbaijan. It started the discussion by elaborating what is incorporated or omitted by the term 'cybercrime' and clarifying the range of acts this thesis aims to study, and provided the working definition and categorisation of cybercrime. Definitions covering the principal points have been adduced by several scholars worldwide. However, these definitions have left gaps. In Azerbaijan, there is still considerable ambiguity about which acts are incorporated or omitted in the term 'cybercrime', and what is the extent of their harmfulness. To serve the objectives of this study, a working definition of cybercrime has been provided. In doing so, a broader approach has

[240] Michael Cross and Debra Littlejohn Shinder, *Scene of the Cybercrime* (Syngress Pub 2008) 508.
[241] Debra Littlejohn Shinder and Ed Tittel, *Scene of the Cybercrime* (Syngress Pub 2002) 37.
[242] Council of Europe (n. 239), 5.
[243] UN General Assembly, Creation of a global culture of cybersecurity and the protection of critical information infrastructures (2004) A/RES/58/199, 2.
[244] ITU (n. 196), 38.
[245] UN General Assembly, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (2009) A/RES/64/211.

been adopted covering all the acts and offences considered as 'true cybercrimes',[246] and those that can be 'carried out at scale for less capital and sometimes with fewer criminal staff than would be needed for similar crimes offline'.[247]

It was identified that general ICT development and application in Azerbaijan appears to be above the global average. However, there is a disproportion between the application of ICTs and the level of ensuring the cybersecurity in the country. Moreover, Azerbaijan has not grasped the opportunities of ICTs successfully in controlling and preventing cybercrime, due to the complexity of modern tools and has faced a range of design and legal challenges which has left the country vulnerable to the growing number of cybercrime.

It has also been revealed that under-reporting and under-counting of cybercrime have blurred the understanding of the current cyber threat landscape and obscured its impact on the country. Nor are there methodologically sound national surveys measuring cybercrimes in the country. Relevant international and security network reports, as well as the interviews have been considered to illuminate the scale and impact of cybercrime on Azerbaijan along with considerably limited and incomplete information provided by the national sources. It was identified that cybercrime is a real and growing threat to the country. Globalisation, complex geopolitical position of the country, possible and ongoing conflicts with neighbouring countries, lack of control and monitoring mechanisms on the information space, increasing dependence on the Internet and digitisation of services, low levels of ICT education and awareness, as well as changing socio-economic conditions have been identified among the root causes linked to the increasing impact and scale of online threats and cybercrime in the country.

In the last part of this chapter legality, effectiveness and efficiency were determined as the appropriate standards against which the responses to cybercrime are evaluated and adjusted throughout the main body of this research, primarily within Chapters 4, 5 and 6.

[246] Which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace. See for further information, David Wall (n. 6) 47-48.
[247] UK Serious and Organised Crime Strategy (2013) (n. 85).

CHAPTER 3: Policy Responses of Azerbaijan to Cybercrime

3.1 Introduction

The previous Chapter provided the definition and categorisation of cybercrime for the purposes of this thesis and analysed the problem of cybercrime in Azerbaijan, its extent and impact on individuals, society and the state, as well as the opportunities and challenges of fighting cybercrime.

Following the second research objective of this thesis, which is to explore and inspect official policy responses of Azerbaijan to cybercrimes, this Chapter explains in outline the measures undertaken to control and prevent cybercrimes. It then draws out and debates the arrangements that can be considered as parts of its anti-cybercrime policy responses, and its translation into national strategy.

It needs to be stressed from the outset that dedicated cybercrime policies and strategy, the importance of which was raised by majority of interview respondents,[248] have not been established in Azerbaijan yet in a distinct form, despite the relevant legislative frameworks have been harmonised with the Convention on Cybercrime. Due to the lack of formal statements, the complexity of cybercrime measures and the expansive mandates and variety of actors involved in their realisation, it is difficult to ascertain and delineate the full scope of a cybercrime policy.[249] The elaboration of the evolution and reach of the relevant strategy and policies, as well as actions undertaken against cybercrimes might assist in interpreting the political stance of the country and create the whole picture of its policy against cybercrimes.

Moreover, although the legal measures are discussed based on the policy perspectives in this chapter, legal responses of the country to cybercrime are also inspected against the standards set for 'appropriateness' in Chapter 4 and 5. Chapter 4 considers relevant constitutional rights, liberties and regulatory laws, as well as the criminalisation approach and substantive criminal laws, while investigatory powers, and jurisdictional issues and international cooperation provisions are scrutinised by Chapter 5.

---

[248] See Interviews with Ministry Official 1, 2, 3, 4, 5, NGO Repr. 1, Independent Expert 1.
[249] Ben Hayes et al. (n. 137) 24.

3.2 National Cybersecurity Context

While ICT use has flourished in Azerbaijan, the same cannot be claimed for ensuring an adequate level of cybersecurity in the country. Based on the interviews[250] and the documentary research, it can be argued that Azerbaijan lacks the capacity to develop national cyber security policies, given that the government has neither established a national-level cyber security coordination format (council, committee, working group, etc.) for cyber security policy coordination, nor a policy unit specialised in national cyber security policy development.

Up to this moment, it is primarily 'information security' which has gradually become a policy priority of Azerbaijan, while the broad application of ICTs for a wide range of purposes in government, business and society is promoted and identified among the priorities of 'the long-term national development strategy of Azerbaijan'.[251] The National Security Concept has identified information security as one of the main directions of national security policies of the country since 2007, which is concerned with the security of 'the State, public and individual information resources, as well as protection of national interests in information sphere'.[252] However, measures undertaken in this regard remain fragmented. For instance, cybercrime has not been listed among the 'threats to national security', possibly because cybercrime would have not posed a significant threat before the adoption of this concept. If this process is compared to that of in other countries, where the Internet has become increasingly central to the economy and society, it is notable that it took those countries a while before they considered cybercrime among national risks of highest priority.[253]

Security of information resources and information infrastructure, on the other hand, has been among the primary objectives of other instruments concerned with information security. In 2012, the Decree on 'Measures in the field of improvement

[250] Interviews with Independent Expert 1 and NGO Representative 1.
[251] See Section 2.3. Chapter 2.
[252] Section 4.3.11, *National Security Concept of the Republic of Azerbaijan*, approved by Instruction No. 2198 of the President of the Republic of Azerbaijan on 23 May 2007.
[253] See for example, UK National Security Strategy (2010), UK National Security Strategy and Strategic Defence and Security Review (2015), National Security Concept of Estonia (2010), National Security Concept of Georgia and etc.

of the activities of the information security' was adopted in Azerbaijan. The Decree aims at ensuring stability and security of information processes, and information resources of state authorities, coordinating the activities of state and non-state actors, and users of the information infrastructure to prevent and analyse threats, assessing and managing cybersecurity risks, and ensuring national preparedness and awareness.[254] However, the Decree does not embody cybercrime related components in particular, but is mainly concerned with the security and stability of information processes, and information infrastructure belonging to state entities. This gap has been reflected in the roles and responsibilities of organisations set up in accordance with the Decree. Simply put, cybercrime-control issues have not been addressed, although it is claimed that the Decree provides 'a new strategic approach to the problem of ensuring cybersecurity'.[255]

The National Strategy on the Development of the Information Society for the years 2014-2020, adopted in 2014, has taken a broader perspective, in the sense that it does cover cybersecurity strategy related elements. The strategy is regarded as an 'officially recognised national cybersecurity strategy',[256] although it is not focused solely on cybersecurity issues and does not embody all necessary components of a comprehensive cybersecurity strategy. As has rightly been demonstrated, this strategy is 'an information society strategy, which encompasses most aspects of a cybersecurity strategy'.[257] Nonetheless, the section concerned with the 'information security'[258] covers elements of a cybersecurity concept. Cybersecurity can be defined as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies' that can be used for the protection of the cyber

[254] Decree of the President of the Republic of Azerbaijan on 'Measures in the field of improvement of the activities of the information security', 2012, № 708.
[255] Yadigar N. Imamverdiyev, (n. 17) 43.
[256] NATO Cooperative Cyber Defence Centre of Excellence, for example, included the strategy among Cyber Security Strategy Documents in its website: https://ccdcoe.org/strategies-policies.html.
[257] Council of Europe, *Cybercrime and cybersecurity strategies in the Eastern Partnership region,* (Cybercrime@EAP 2015) 19.
[258] See The National Strategy on the Development of the Information Society for the years 2014-2020, Section 13.

environment and organisation and user's assets,[259] or in other words, the 'confidentiality, integrity and availability of information in the cyberspace'.[260] Along with other objectives, the strategy also aims at ensuring the security of the country's information space, increasing the trust and confidence in ICT, improving the state policy and the legislative frameworks in this field, and conducting enlightenment and raising awareness among internet users regarding the threats in cyberspace.[261] These objectives in the Strategy are followed by the list of actions to be realised if the ultimate goal is to be achieved.[262] Not surprisingly, it gives the highest priority to the security of 'national information space and critical information infrastructure',[263] but does not directly refer to the necessity for the protection and promotion of human rights and the rule of law when ensuring the information security.

It can be appealed that securing the information space of the country so that individuals are able to exercise their rights and freedoms does not seem to be an important objective of section 13. Ensuring human rights, however, especially individuals' access to information and communication with each other is included among the tasks to be realised to achieve primary objectives determined by the strategy.[264] One of the limitations of the Strategy is related to the ambiguity caused by its focus on measures (whether technical, procedural or institutional). Specifically, the proclaimed objectives and actions concerned with cybersecurity, such as 'improving legal and policy framework in the field of information security', 'developing the system which ensures the security of national information space and critical infrastructure', 'establishing information security culture', 'ensuring international cooperation in the field of information security', cannot be regarded as fully quantitative targets.[265] It, thus, appears to be difficult to measure cyberspace

[259] ITU, *Recommendation ITU-T X.1205 "Overview of Cybersecurity",* (04/2008), clause 3.2.5.
[260] ISO/IEC 27032:2012, *'Information technology – Security techniques – Guidelines for cybersecurity,* (ISO copyright office, Geneva, Switzerland 2012).
[261] The National Strategy on the Development of the Information Society for the years 2014-2020, Section 13.1.
[262] Ibid, Section 13.2.
[263] Ibid.
[264] Ibid, Section 3.
[265] See Ibid, Section 13.2.

progress against the benchmark of projected goals. Hence, it would be useful to adopt 'clear, succinct and achievable'[266] cybersecurity ends that can later be measured to 'tell success from failure'[267] and to further identify those factors hindering regulatory initiatives from being translated into action. Furthermore, the Strategy does not provide guidance for the cases of confrontation with challenges, and leaves it open as to who will take the lead regarding each action, and how the targets should be reached. It might be helpful to develop a more comprehensive action plan for the enforcement of the strategy.

Another important factor is that the strategy does not comprise any action specifically referring to cybercrime-control for the fulfilment of its goals.[268] However, combatting cybercrime is considered by the ITU to be an integral component of a national cybersecurity strategy.[269] In addition to having the responsibility of taking actions in the legal and regulatory areas to improve, clarify, and enforce its laws in terms of cybercrime**,** the state also has a positive obligation of protecting people and their rights against crimes, and bringing offenders to justice.[270]

To conclude, the national strategy cannot be regarded as a comprehensive approach to the problem of ensuring cybersecurity, as it is ambiguous about responses to cybercrime and does not provide clear corresponding directions for addressing its challenges. It is not necessary, however, to combine all relevant measures and activities in a single document to establish a comprehensive approach to a problem, so long as clear and comprehensive directions can be easily found. However, it seems that Azerbaijan has instead resorted to multiple documents and measures in place, underpinned by an approach that might lead to a potential lack of compatibility and inconsistency within these measures. Consequently, the approach results in significant reduction of effectiveness and efficiency of state responses.

---

[266] ITU (n. 196) 21.
[267] David Osborne and Ted Gaebler, *Reinventing Government* (Addison-Wesley Pub 1992) 14.
[268] See the National Strategy on the Development of the Information Society for the years 2014-2020, Section 13.2.
[269] ITU (n. 102), 2.
[270] Article 26 of the Constitution of the Republic of Azerbaijan (1995) specifies that the state guarantees protection of rights and liberties of all people.

Although limited or at least, not fully declared, the commitment of the country to cybersecurity has also been subjected to international studies and measurements. According to the Global Cybersecurity Index (GCI) 2017 Azerbaijan has fulfilled 56% of the criteria, which gave the country the 48th ranking.[271] As a composite index, the GCI included 25 indicators and 157 questions, to measure the cybersecurity commitment of 193 ITU Member States with regard to the five pillars: legal, technical, organisational, capacity building, cooperation.[272] Based on the GCI score Azerbaijan was included in the list of 'maturing' states, that have 'developed complex commitments, and engage in cybersecurity programmes and initiatives'.[273]

Taking account of the results of another study - the National Cyber Security Index (NCSI) – which was conducted to measure countries' preparedness to prevent the fundamental cyber threats and readiness to manage cyber incidents, crimes and large-scale cyber crises - it can be claimed that the cyber security situation in Azerbaijan is more deficient.[274] According to this study, the country has fulfilled only 23% of the cyber security criteria, which placed the country in 81th place among the 109 countries studied.[275] In comparison to the GCI 2017, which included 25 indicators, the NCSI focused on 12 indicators/cyber security capacities under which four aspects have been taken into consideration: legislation in force, existing units, cooperation formats, and outcome of different processes.[276] To satisfy the measurability principle, the NCSI included indicators which can be proven by clearly evidenced materials and thus, only the official web links or/and official documents are accounted for the study. It is, therefore, problematic to establish an accurate picture of cybersecurity capacity of Azerbaijan based on this study, where there is a limited number of potential online sources to study and a tendency of non-cooperation of crucial agencies with researchers, a tendency experienced during this thesis study as well, as explained in Chapter 1. For example, the NCSI

[271] ITU, *Global Cybersecurity Index 2017*, 60.
[272] Ibid, 3-11.
[273] Ibid, 60.
[274] e-Governance Academy Foundation (Estonia), *National Cyber Security Index*, 2018 http://ncsi.ega.ee/.
[275] Ibid.
[276] Ibid.

study was unable to determine whether there is any unit in Azerbaijan specialised in combating cybercrime due to the non-existence of online information on public sources/online websites; thus, the country is regarded as having 'no such capacity' in this regard. The contrary has been identified by this study, although the researcher was refused access to conduct interviews with the employees of the special units established to combat cybercrime under the State Security Service and the Ministry of Internal Affairs of the Republic of Azerbaijan.

Further, there are evaluations, which clearly differ from those provided by the GCI 2017. For instance, the GCI 2017 values the work undertaken in Azerbaijan regarding cyber security strategy as 'medium', while NCSI valued this with '0', providing that the central government has not established the national-level cyber security strategy or other equivalent document.[277] In fact, as previously noted, some elements of cyber security are contained by the National Strategy of the Republic of Azerbaijan on the Development of the Information Society for the years 2014-2020. However, this is not to say that the GCI 2017 survey is completely independent of errors and inaccurate evaluations. For example, Azerbaijan's level of commitment to cybercriminal legislation is regarded as being 'high', whereas, in fact, the country has been significantly lacking cyber-specific procedural laws in dealing with cybercrime cases and digital evidence.[278] Thus, it can be argued that the cybersecurity situation in Azerbaijan is not as positive as that described by the GCI 2017. At the same time, the actual capacity of the country does not seem to be as insufficient as claimed by the NCSI.

In fact, to cope with internet-related threats and vulnerabilities rising from increasing reliance on ICT, Azerbaijan has taken several measures against cybercrime in terms of legal, organisational, cooperation, as well as crime prevention, which are examined later in this thesis. It is crucial to test whether all components of these measures are fully in alignment and compatible with each other to maximise their effectiveness.

---

[277] Kristina Reinsalu et al., *Situation Review: Safety and Security of Cyberspace and E-Democracy in the Eastern Partnership Countries* (e-Governance Academy 2017) 34.
[278] See Chapter 5.

3.3 Legal measures

One of the main roles of a policy is that it can be utilised for identifying various components of the legislative elements needed in a comprehensive approach and key areas that should be addressed by legislation.[279] Being one of the main instruments used for regulatory purposes, laws play an important role in combatting cybercrimes, despite the difficulties of adapting to the nature and challenges of cyberspace.[280] To be more specific, notwithstanding that the law is regarded as being dynamic, flexible, continuously subject to change, and 'in perpetual motion',[281] its dynamics are still slow when compared to the dynamics of cyberspace and criminal conduct in this environment. It can be agreed that legal measures alone cannot address the challenges of cybercrime effectively and efficiently. Nevertheless, legal measures are crucial in responding to cybercrime and required in distinct areas, including criminalisation, jurisdictional coverage, procedural powers, international cooperation, and fixing the responsibility and liability of different stakeholders.[282] While each of these areas is extensively studied by Chapter 4 and 5, it would be useful to briefly elaborate actions to be undertaken in terms of cybercrime legislation, government legal authority and cybercrime capacity in responding to cybercrime in this Chapter from policy perspectives.

According to the National Strategy on the Development of the Information Society for the years 2014-2020 Azerbaijan seeks a dynamic legal framework which is capable of keeping pace with evolving cyber threats.[283] Hence, substantial efforts have been made to enhance the country's capacity to respond to cybercrimes in terms of legal measures. Specific criminal legislation on cybercrime has been

---

[279] Marco Gercke, 'Strategy, Policy, Legislation, Prevention and Enforcement' in Adil Duyan (Edn), *Analyzing Different Dimensions and New Threats in Defence against Terrorism (*104 *NATO Science for Peace and Security - Series E: Human and Societal Dynamics*) (IOS Press, 2012) 15-16.
[280] See Ian Ayres and John Braithwaite*, Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, Oxford, 1992); see also, Lawrence Lessig, *Code and Other Laws of Cyberspace*, (New York: Basic Books, 1999) ch.7; Colin Scott, 'Analysing Regulatory Space: Fragmented Resources and Institutional Design' (2001) *Public La*w, 329.
[281] Sharyn L Roach Anleu, *Law and Social Change* (2nd edn. London: SAGE, 2010) 252.
[282] UNODC, (n. 71), xviii.
[283] The National Strategy on the Development of the Information Society for the years 2014-2020*,* 13.2.

reflected through the Criminal Code (1999), Chapter 30, which has also been harmonised with the Convention on Cybercrime in 2012.[284]

Azerbaijan has taken significant steps to reduce discrepancies between national laws and enable transnational evidence collection through harmonising its laws with international ones. [285] Ratification of the Convention on Cybercrime in 2010 is just one of these steps, but within the context of cybercrime combatting, it can be regarded as the most important one.[286] Implementation of the Convention on Cybercrime, however, imposes both challenges and opportunities. On one hand, as Williams states, 'the offenders can avail themselves of the borderless advantages of the Internet while enforcement agencies are hampered by the need to respect each other's sovereignty'.[287] In this regard, harmonisation of the relevant Criminal Code articles with the Convention of Cybercrime may foster a better protection and prevention mechanism, because cybercrime control requires an international mechanism making it 'marginally easier for the network partners to collaborate'. [288]

On the other hand, to ensure an appropriate response to cybercrimes, the Convention on Cybercrime must be applied and fully implemented by all of the States that have access to cyberspace.[289] In contrast, provisions of accession to the Convention constitute obstacles to nation-states which are not members of the Council and which have not participated in its elaboration. According to the Article 37 of the Convention, these states may only be invited to accede to the Convention by the Committee of Ministers of the Council of Europe 'after consulting with and obtaining the unanimous consent of the Contracting States to the Convention'.[290] This provision is a limitation of the Convention in addressing the challenges of

[284] Law on Amendments to the Criminal Code of the Republic of Azerbaijan, 2012, № 408-IVQD
[285] See Chapter 4, Section 4.3.
[286] Council of Europe Convention on Cybercrime (2001) ratified by the Law dated 30.09.2009, see at http://www.e-qanun.az/framework/18619.
[287] Katherine S. Williams, 'Transnational developments in Internet Law' in Yvonne Jewkes and Majid Yar (Edn.) *Handbook of Internet Crime.* (London: Willan Publishing, 2010) 477.
[288] Milton Mueller (n. 5), 176.
[289] Over ten years after the Convention on Cybercrime adopted, it has been signed by 55 states. see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
[290] Article 37, Council of Europe Convention on Cybercrime (2001) ETS No. 185.

cybercrimes. Because, making a decision based on a "nation-state" for an instrument to be implemented in a borderless space decreases the effectiveness and efficiency of cooperation. Besides, even if the prerequisite of having the Convention applied and fully implemented by all nation-states, the length of the time spent for the implementation may become a hindrance. In addition, the Convention has already started showing signs of a need for updating, given that specific emerging new types of cyber offences are not clearly addressed, although they may be subsumed beneath broader categories.[291] Nor does the Convention mention the new investigation instruments like key-loggers ("Magic Lantern") and identification instruments ("CIPAV") that are already in use in several countries either as permissible or not.[292] Detailed discussion is provided later in Chapter 4 and 5.

It is recommended by the Explanatory Report to the Convention on Cybercrime that 'not only must substantive criminal law keep abreast of … new abuses, but so must criminal procedural law and investigative techniques'.[293] In this regard, it can be highlighted that alongside with penal legislation, the country also possesses fundamental legislative foundations for procedural instruments that enable LEAs (LEAs) to conduct investigations of cybercrime cases, notwithstanding these instruments are not sufficiently cyber-specific and therefore, less efficient in dealing with cybercrime. Another shortcoming is that electronic evidence is not properly regulated, given that national regulations do not provide for clear rules on the collection and use of electronic evidence. Instead, general procedural rules on evidence collection and use alike are applied to handle electronic evidence, which has proven to be difficult and inefficient to apply, as these rules are not sufficiently clear and comprehensive. Thus, LEAs are faced with the risk of being partially deprived of the means for proper investigation and prosecution of serious incidents in cyberspace. An alarming inconsistency between the number of reported cyber incidents to the Computer Emergency Response Team (CERT) and the number of

[291] Ian Brown, Lilian Edwards and Christopher Marsden, 'Information Security and Cybercrime' in L. Edwards, C. Waelde (Edn) *Law and the Internet*, (3rd edn. Oxford: Hart, 2009) 12.
[292] Ibid.
[293] *Explanatory Report to the Council of Europe Convention on Cybercrime* (2001), para. 132.

criminal cases opened by the former Ministry of National Security can also be attributed, but not exclusively, to the lack of appropriate procedural instruments. For example, more than 1500 incidents per year have been reported to the Computer Emergency Response Team (cert.gov.az) since its establishment in 2013, while only 12 criminal cases were opened as part of counter-actions against cybercrime by the former Ministry of National Security throughout 2009-2012.[294] It is, however, important to add that discrepancy between the number of reported cyber-incidents and the criminal cases opened could be due to other possible reasons, including the complex design and nature of cybercrime, the difficulties of cross-border investigation, the lack of awareness and willingness to report as well as the shortage of resources.

Furthermore, following the ratification of the Convention on Cybercrime in 2010, Azerbaijan started to bring its legislative framework in line with the Convention to address the challenges arising from the transnational nature of cybercrime. Harmonisation of the Criminal Code with the Convention has been followed by changes in other corresponding laws and regulations. Bringing national legislation into compliance with the Convention has also assisted Azerbaijan in establishing a legal basis for both public-private cooperation, and international cooperation. However, national context, circumstances, resources and actual capacity of the country have not been sufficiently reformed. As a result, notwithstanding the fact that the relevant legislative criminal law frameworks are being brought into compliance with the Convention, the actual protection against, and prevention of these crimes have become even more challenging. Along with this situation, the existence of various material conditions and the unclear parameters has left the law open to abuse and made the users vulnerable even to the LEAs that are obliged to protect them. These can all be regarded as negative implications of not giving priority to ensuring that the legislation follows the dedicated strategy and policies.

[294] Note: information regarding the cybercrime investigations conducted by the Ministry had not been updated since 2012 and currently, the statistics about cybercrime investigations are not available.

Consequently, it can be asserted that the lack of a dedicated strategy and policies has led to inadequacy of implementation and coordination of legal efforts. This becomes even more apparent when analysing Azerbaijani legislation with reference to the Convention on Cybercrime. It appears that despite a set of relevant provisions being put in place, there remain gaps and weaknesses in the legal responses of Azerbaijan to cybercrime, as well as the challenges of implementation of the Convention provisions. These responses and provisions are studied alongside with details regarding contextual factors and incompatibilities influencing the actual level of implementation throughout Chapters 4 and 5.

3.4 Roles and Capabilities

When establishing a comprehensive approach to responding to cybercrime, it is crucial to recognise that more complex components, such as the distribution of roles and responsibilities are also necessitated by it. In this regard, as an evolving law enforcement matter, cybercrime necessitates the clarification of the roles and responsibilities of a range of actors, determining the specific focuses and aspects of law enforcement responses and the allocation of appropriate resources to do this properly.[295] The next section analyses the roles and capabilities of government institutions, as well as private sector, academia and civil society in responding to cybercrime.

3.4.1 The Government

In Azerbaijan, the Government has a primary authority to provide the development of appropriate strategy, policies and programmes, alongside bearing the responsibility to take actions in the legal/regulatory field to improve, clarify, and enforce national laws in terms of cyber-crime. Thus, the government has legal powers and does allocate roles and responsibilities between stakeholders, notwithstanding it still lacks any comprehensive vision on cybersecurity and cybercrime-control and prevention, which has resulted in ‘disproportionate

[295] Michael Levi et al. (n. 87) 29.

allocation of budget and resources', as especially supported by NGO Representative 1.

Following the adoption of the Decree on 'Measures in the field of improvement of the activities of the information security'[296] to pursue the objectives determined, the State Agency for Special Communications and Information Security, and the Electronic Security Service were established in 2012. The Agency functions under the Special State Protection Service of the Republic of Azerbaijan. It provides organisation, maintenance, security, and development of special state communications for governmental agencies, information and technology systems and networks for special-purpose, flow of interagency electronic documents, state bodies' communications with the Internet network, posting of their information web-resources in the information and resource centre.[297] The Electronic Security Service (cert.az) was established under the Ministry of Communication and Information Technologies of the Republic of Azerbaijan. Its constituency is both public and private sector and engages in coordinating the action of information infrastructure subjects, reporting about existing and potential risks at country level, educating public, private and other institutions in the field of cyber security, and providing methodological assistance to them.[298] Both of these organisations participate in collaborative international efforts against cyber threats by being a full member of the Forum for Incident Response and Security Teams (FIRST),[299] the Anti-Phishing Working Group (APWG)[300] and the TF-CSIRT Trusted Introducer.[301]

These organisations are also the officially recognised agencies responsible for the implementation of the national cybersecurity strategy, policy and roadmap; they do

[296] Decree of the President of the Republic of Azerbaijan on 'Measures in the field of improvement of the activities of the information security', 2012, № 708.
[297] See for further information: http://www.cert.gov.az/en/pages2/about.html.
[298] See for further information: http://www.cert.az/s/u/document/rfc_2350.pdf.
[299] FIRST is the premier organisation and recognised global leader in incident response. See for more information, https://www.first.org/.
[300] APWG is the international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities. See for more information, https://www.antiphishing.org/about-APWG/.
[301] The Trusted Introducer Service was established by the European CERT community in 2000 to address common needs and build a service infrastructure providing vital support for all security and incident response teams. See for further information, https://www.trusted-introducer.org/index.html.

not bear tasks regarding the investigation of cybercrime activities. Nonetheless, Electronic Security Service, for example, has been determined by law as a special administrative body authorised for making decisions on temporarily limiting access to the illegal content on the Internet without a court approval.[302] Limiting access to websites, botnets and dark markets - collaboratively with ISPs - might result in reducing harm, and further prevent the commission of cybercrime. Moreover, these organisations have also been tasked to work closely with the State Security Service and the Ministry of Internal Affairs and pass on reported incidents encompassing the elements of cybercrime to them after being filed. It is, however, important to note that during the interviews with Ministry Official 1, 2, 3, 4, and 5 in March 2017, it was repeatedly stated that the Electronic Security Service had not been allocated 'sufficient human, financial, and technical resources' to meet its legal obligations effectively and efficiently. This could be the reason why NGO Representative 1 claimed that 'there is an urgent need to take serious steps' for enhancing cybercrime control and prevention capacity within the private sector and businesses as well as among the publicity, which is primarily under the constituency of the Electronic Security Service.

Up until 14 December 2015, only the former Ministry of National Security Department of Organised Crime/Cybercrime Division was assigned to combat cybercrime through investigating these offences, regardless of these activities encompassing any national security component.[303] This unit is focused on investigating and fighting computer-related crimes, illegal interception and interference with data, computer-related fraud, child abuse, racism, as well as signs of terrorism in the Internet, embezzlement and fraud related to use of IT and Internet.[304] A limited number of cases has been reported and investigated, keeping in the single digits for recent years.[305] It can be argued that having a special service agency as the only option for reporting and having all types of cybercrime

[302] See Article 13-3.3. Law on Information, Informatisation and Protection of Information, 1998, №460-IQ.
[303] Article 20.2.5. Law on National Security 2004, № 712-IIQ.
[304] Council of Europe, Cybercrime Programme Office*, Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play* (2017) 12.
[305] Ibid.

investigated was affecting victims and leading to underreporting, besides burdening the agency and draining the limited resources.[306] This lack of an effective public reporting mechanism makes it difficult to provide a clear understanding of cybercrime threats and trends or to facilitate proper criminal justice action.[307]

Since 14 December 2015, the Ministry of Internal Affairs has also been tasked with the investigation of cybercrimes.[308] However, provincial cybercrime divisions have not been established under these ministries, which makes it extremely challenging to cope with all cases in an effective and efficient manner by the existing single central divisions in the ministries. What is more, there is a shortage of qualified specialists and sufficient resources,[309] in both ministries, and those dealing with cybercrime are not provided with proper equipment and training. Council of Europe delegation emphasized that more attention should be paid to legal training in the field and investigative officers, with targeted specialisation of professionals.[310] Furthermore, functions performed by both the Ministry of Internal Affairs and the State Security Service (former Ministry of National Security) in fighting against cybercrime overlap. There has also been a challenge in discerning necessary distinctions and restrictions to allocate roles and responsibilities between the state agencies concerned with law enforcement, civil protection, national security and military force in the field of cybercrime in Azerbaijan, a problem also experienced elsewhere.[311] The lines are particularly blurred between the policing function and national security.

Next, a limited degree of capacity and commitment has been observed in Azerbaijan in terms of the prosecution and adjudication of cybercrimes, which also

---

[306] 'What does the empowerment of the Ministry of Internal Affairs with further investigation powers promise?' ('DİN-In Istintaq Səlahiyyətlərinin Genişləndirilməsi Nə Vəd Edir?') (*Azinforum.az*, 2015) http://azinforum.az/din-in-istintaq-s%C9%99lahiyy%C9%99tl%C9%99rinin-genisl%C9%99ndirilm%C9%99si-n%C9%99-v%C9%99d-edir/.

[307] Council of Europe (n. 231), 3.

[308] Article 215-5, Criminal Procedure Code (2000), see also, Section 2, Presidential Decree № 707, 2015, available online http://e-qanun.az/framework/31610.

[309] See. 'Police will fight cybercriminals' (Sputnik.az, 2015) http://sputnik.az/radio/20151216/403058771.html.

[310] See also, Council of Europe, *Progress Report (covering the period of 1 June 2011 – 31 March 2012*) (Directorate General of Human Rights and Rule of Law, 2012) 38.

[311] Ben Hayes et al. (n. 137), 23.

call for specialisation within the criminal justice system.[312] Minimal levels of personnel and organisational cybercrime specialisation were shown by prosecution and courts. At present, no special institutional entity exists within the Prosecution Service for dealing with cybercrime cases, although the Prosecutor General's Office is tasked to exercise supervision over the accurate and uniform execution and application of laws in the country.[313] Nor have the courts in Azerbaijan shown a suitable level of specialisation for cybercrime on both organisational and personnel levels.[314] Some of the main reasons for the low number of cybercrime cases tried before courts can be, thus, the shortage of necessary resources, cybercrime-related training and expertise within the judiciary.

Furthermore, in addition to the lack of specific legal provisions, there is also a serious shortage of knowledge and resources allocated to identify, collect, preserve, prepare, present and evaluate the electronic evidence, as also provided by Independent expert 1 and NGO Representative 1, which puts a question mark over the effectiveness, efficiency and legitimacy of criminal investigation and proceedings.

3.4.2 Private sector, academia and civil society

The role of the industry, private sector, academia and civil society in Azerbaijan's cyber security alongside government sector has been undermined, as also supported by Independent expert 1 and NGO Representative 1. The private sector and businesses, for example, play an important role in Azerbaijan's cyber security, because the internet infrastructure is primarily used and owned by them. Moreover, the critical infrastructure also largely lies in the hands of the private sector. Service providers, especially Internet Service Providers (ISPs) are particularly significant, being effectively the gatekeepers of data on the Internet,[315] because, computer data processed and transferred across the internet are mostly controlled and

[312] UNODC (n. 71), 172.
[313] Article 133, Constitution of the Republic of Azerbaijan (1995).
[314] All 8 courts/judges operating in the capital city contacted for the interview refused due to not previously having any cases adjudicated and therefore, not having any experience about cybercrime cases.
[315] Jonathan Clough (n. 76), 8.

stored by them and other communication or web-service providers. Service providers hold subscriber information, communication content, some connection logs, location information, and billing invoices, all of which can represent critical electronic evidence of an offence.[316] It is, however, notable that the government in Azerbaijan holds a significant control and ownership of the leading ISPs. This situation has resulted in the practice of a closer cooperation between the government authorities and ISPs, since ISPs would tend to avoid the negative impact on their business by refraining to collaborate with the government. At the same time, the lack of strict and transparent rules has made it challenging to ensure a fair and legitimate balance between individual rights and freedoms and the surveillance powers when responding to cybercrime.

As has also been confirmed by NGO Representative 1, involvement of the private industry, civil society organisations and community representatives in the formulation and development of policies pertaining to cybercrime (such as monitoring, investment, counter-measures, harmonisation of terminology and laws) is not widely practiced in Azerbaijan. Thus, the government is unwilling to engage with the community members who possess special knowledge and experience that professionals and bureaucrats are seldom aware of. The Azerbaijan Internet Forum (AIF), for example, which is a non-profit public association formed by independent experts, encompasses a broad range of interests in the development of ICTs in the country, as well as its information security, and has been working towards shaping policy and regulation responsive to the rising potential of the Internet and ICTs.[317] Nonetheless, the government has been unwilling to involve either AIF or other civil society institutions during the development of important cybersecurity and anti-cybercrime related documents.[318] Consequently, various concerns of civil society and private sector and businesses are hardly reflected in the policy and legal documents. Moreover, the civil society organisations, private sector interests and

[316] UNODC (n. 71), xxiii.
[317] See for further information, http://aif.az/.
[318] 'The Regulation of the Electronic Security Center should be prepared through public engagement' (*Aif.az, 2012*) http://aif.az/etm-nin-%C9%99sasnam%C9%99si-ictimaiyy%C9%99tin-istiraki-il%C9%99-hazirlanmalidir/.

businesses are still far from being relevant to policy formation, nor has their capacity been fully tapped.

Academic institutions can also be considered to be potential significant contributors in designing responses to cybercrime. Academics in Azerbaijan, however, have also been passive in terms of policy and capacity enhancement against cybercrime and cybersecurity threats. Efforts placed in knowledge development and sharing through the educational institutions and programs can not be claimed to be significant given that a sufficient degree of knowledge and training materials have not been provided. For its part, academia has not given suitably high priority to cybersecurity studies, and its vision on cybercrime is often blurred. Academic institutions engaged in developing academic foundations of cyberspace, cybersecurity and cybercrime are very limited. The Department of Information Technologies and Information Security, alongside with the departments of Law and Operational Activities in the Academy of the State Security Service research and teach cybersecurity and cybercrime related issues.[319] Moreover, law faculties at Baku State University[320] and Academy of Public Administration under the President of the Republic of Azerbaijan include the studies of cybercrime as part of their criminal law and information law modules.[321] In addition, in 2002, the Institute of Information Technology was established under Information and Telecommunication Scientific Center (operating under the Azerbaijan National Academy of Sciences). The Institute has developed various aspects and approaches to ensure security of web systems, proposed models for detecting information security threats in computer networks, and for information security risk assessment and control, as well as offered some proposals to provide security of information economy in Azerbaijan.[322]

Furthermore, to meet national demands of cybersecurity professionals and workforce development needs, besides founding the Information Technologies University in 2013, Azerbaijan has included the study of high technologies among

[319] See for further information http://dtx.gov.az/en/articles4.php.
[320] See http://law.bsu.edu.az/az/content/cnayt_hququ_v_krmnologya_kafedrasi__312.
[321] See for further information http://dia.gov.az/?e=101&a=244.
[322] See for more information about the Institute: http://ict.az/en/content/250/.

'the first degree priority areas of specialty' for its 'State Program of Azerbaijani Youth Education Abroad for 2007-2015', and 348 students were sent abroad under this program to get higher education in this field.[323]

However, these developments are not broad enough to claim that Azerbaijan has fully accounted for its national cybersecurity context and satisfied its demands for expert skills. So, there are very limited numbers of cyber-security and cybercrime-control related studies, specialised educational programs, research and training centres and units within different institutions. Nor have the national curricula been aligned with the regulatory and industry demands of the country. At the moment, only couple of universities (Baku Higher Oil School, Azerbaijan State Oil and Industry University) and the Academy of the State Security Service provides a bachelor's and master's level programme on information security, which primarily focuses on technical and technological aspects. Yet, there are no cyber-crime focused specific programmes provided by public and private universities on the undergraduate or graduate level. In addition, specific cybersecurity related programs, campaigns or lessons offered at schools in Azerbaijan are also missing.

3.5 Cooperation measures

Alongside a more effective criminal justice response, fighting cybercrime also necessitates effective and efficient cooperation at all levels. Given that many interdependencies are created between the public and private sectors in cyberspace, and cybercrime is often a transnational crime, challenges of fighting it cannot be surmounted alone by any country, agency, company or individual. Thus, Azerbaijan has taken measures in both intra-state and international level to respond to cybercrimes more appropriately.

3.5.1 Intra-state cooperation

After the harmonisation with the Convention on Cybercrime the dialogue between LEAs and internet service providers has been strengthened, procedures and

[323] See: http://xaricdetehsil.edu.gov.az/uploads/Statistika4.pdf.

guidelines have been developed to request for cooperation against cybercrime. Coordination of the work of public and non-public information infrastructure subjects has also been identified among the plans in the National Strategy.[324] However, enhancing the capacity of service providers and involving them in combatting cybercrimes has not been included in the Action Plan 2014-2016, although ISPs are indicated as partners for enhancing the capacity of criminal justice institutions.[325] Roles and responsibilities of ISPs, as well as provisions of cooperation with LEAs against cybercrimes are thoroughly discussed in Chapter 5.

Notwithstanding that the cooperation with private sector, businesses and civil society institutions has been included as one of the mechanisms of realisation of the National Strategy on the Development of the Information Society for the period 2014 – 2020,[326] information security and the cyber-crime control policy direction of Azerbaijan has mainly given priority to state actors and the role of the private sector has been undermined. The governmental organisations[327] involved in safeguarding the society against cybercrimes and ensuring cybersecurity are also responsible for increasing the nationwide preparedness, the level of education and awareness concerning the cybersecurity. Moreover, governance of the Internet infrastructure is also monopolised by the government in Azerbaijan. As demonstrated by the Freedom on the Net 2017 report, the Ministry of Transport, Communication and Information Technologies continues to hold a significant share in a handful of the leading Internet Service Providers.[328] Besides, the government has legal powers to instruct companies and providers to impose limits on internet service and even curtail them under very broadly defined circumstances, including the presence of threats to the state interests, or to people's life, health and

[324] The National Strategy for Information Society Development in Azerbaijan for 2014-2020 (2014), 13.2.8.
[325] Council of Europe, Action Plan for Azerbaijan 2014-2016 (ODGProg/Inf (2014) 2revE).
[326] See Section 15.3.
[327] The State Security Service (http://dtx.gov.az/en/haqqimizda2.php); Ministry of Internal Affairs (http://mia.gov.az/); Computer Emergency Response Team (http://cert.gov.az/); the Electron Security Service (http://www.cert.az/).
[328] In fact, the state-run Delta Telecom, owns the internet backbone and is the main distributor of traffic to other ISPs. It controls Azerbaijan's only Internet Exchange Point (IXP) and charges the same amount for local and international traffic. See for further information, Freedom House, *Freedom on the Net, 2017.*

wellbeing.[329] The state's monopolisation of service providers has influenced the establishment of a competitive environment, which has also stifled innovations, and discouraged private sector investments in the ICT sector to some extent.

The Progress Report prepared by the Council of Europe in 2013 also identified the lack of overall public–private cooperation, training for law enforcement, as well as the lack of contact points for public-private cooperation in ministries and financial service providers and ISPs, as shortcomings that deter the ability to effectively control and prevent cybercrimes in Azerbaijan.[330] Moreover, by prioritising only the enhancement of the capacity of criminal justice institutions to investigate, prosecute and adjudicate cybercrimes in Azerbaijan, the Action Plan for Azerbaijan 2014-2016 underestimated and excluded the role of private sector in tackling cybercrimes. This cannot be regarded as a 'better policy solution', which relies on 'working more creatively with the interplay between private and public regulation'.[331] In addition, the State has refrained from actively involving various actors in efforts to promote self-sufficiency and increase the level of preparedness and awareness of Internet users. Very limited awareness-raising activities have been realised, and the nationwide and social media campaigns have been weak and not sufficiently informed.

3.5.2 International cooperation

Maintaining efficient regional and international cooperation is a necessary component to achieve effective control and prevention of cybercrime.[332] As discussed in Chapter 2, significant share of cybercrime acts encountered by law enforcement authorities involved a 'transnational element'.[333] The country has, thus, taken multiple actions to enhance its capacity to cooperate internationally in the fight against cybercrime.

[329] See Article 13-3.3. Law on Information, Informatisation and Protection of Information 1998.
[330] Council of Europe (n. 310).
[331] Ian Ayres and John Braithwaite (n. 280), 4.
[332] Council of Europe (n. 231), 5.
[333] See Sub-section 2.4, Chapter 2.

First, national laws have been harmonised with the Convention on Cybercrime, which partly ensures that its laws are globally applicable and interoperable, and to some extent allows global cooperation on cybercrime investigations and prosecution.

Next, steps have been taken to ensure immediate assistance for criminal investigations and the collection of electronic evidence, also to comply with the Convention on Cybercrime provision. The Convention requires from the state parties to 'afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings' [334] and 'to designate a contact point 'available on a twenty-four hour, seven-day-a-week basis'.[335] Relevant units had been operating under the Prosecutor General's Office and the Ministry of Justice as the central bodies for delivering legal assistance, transfer of criminal prosecution, and extradition. To comply with the Convention provision, a 24/7 point of contact has been created under the Department of Combating Crimes in Communications and IT Sphere, State Security Service. It is legally authorised to provide specialised assistance, order the expeditious preservation of computer data or traffic data, after getting court decision the seizure of objects containing data and perform or facilitate the execution of procedural documents.[336] However, there are problems arising from discrepancies between legal systems and time issues (multi-layered steps and the duration of the procedure (steps)), which make it difficult to deliver extensive co-operation, and to 'minimise impediments to the smooth and rapid flow of information and evidence internationally'.[337] In other words, international dimensions of cybercrimes has left the LEAs with a complex and challenging situation in conducting investigations and collecting electronic evidence. As a result, 24/7 networks have been underutilised by Azerbaijani LEAs. More information, as well as possible solutions are provided by Chapters 5 and 6.

[334] Article 25, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[335] Ibid, Article 35.
[336] Council of Europe, the Cybercrime Convention Committee (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime* (2014) 110.
[337] Article 21, Council of Europe Convention on Cybercrime (2001) ETS No. 185.

Next, the government has entered bilateral, regional, international cooperation agreements with other countries or international organisations. As regards multilateral arrangements, in addition to the Convention on Cybercrime, the country has signed and ratified the European Convention on Mutual Assistance in Criminal Matters, which sets out rules for the enforcement of letters of request by the authorities of a Party ('requested Party') aiming to procure evidence or to communicate the evidence (records or documents) in criminal proceedings undertaken by the judicial authorities of another Party ('requesting Party').[338] Furthermore, signing the United Nations Convention against Transnational Organised Crime can also be regarded as Azerbaijan's demonstration of its political will 'to answer a global challenge with a global response'.[339] Also, the government is represented regularly in cooperation forums that deal with international cybercrime, such as the plenaries of the Council of Europe Cybercrime Convention Committee.

As regards bilateral arrangements, Azerbaijan has entered partnerships on mutual assistance in criminal matters with Bulgaria, United Arab Emirates, Georgia, China, India, Iran, Kirgizstan, Lithuania, Morocco, Moldova, Uzbekistan and Russia.[340] In addition, official partnerships have been established with Russia, Ukraine, Republic of Latvia, Republic of Slovakia and Japan to share information on cyber threats.[341] However, the country is still at the early stages of the development of multilateral and mutually productive working relationships with other countries. Thus, a sufficient number of channels for informal cooperation has not been developed yet.

Apart from state cooperation, the cooperation with 'foreign' private service including major service providers such as Apple, Facebook, Google, Microsoft, Twitter and Yahoo has been extremely low. More discussion are provided in Chapters 5 and 6.

---

[338] Council of Europe, European Convention on Mutual Assistance in Criminal Matters (1959) CETS No.030. Azerbaijan has signed the Convention since 07/11/2001 and ratified since 04/07/2003.
[339] UN General Assembly, United Nations Convention against Transnational Organized Crime, 2000, Azerbaijan has signed the convention since 12/12/2000, and ratified since 30/10/2003.
[340] The full list and the content of the agreements are available online at, http://www.justice.gov.az/images/toplu-2014.pdf.
[341] Council of Europe (n. 257), 19.

3.6 Cybercrime prevention measures and capacity

Crime prevention, as one of the primary purposes of criminal justice, is regarded as comprising strategies and measures aimed at reducing the risk of crimes and their potential harmful impacts on individuals and society, including fear of crime, through interventions that influence their multiple causes.[342]

Azerbaijan has not established a cybercrime prevention plan with clear priorities and objectives, nor does a general crime prevention plan encompassing such priorities and objectives in a clear way exist, notwithstanding that the Criminal Code has included the prevention of crimes among its 'tasks'[343] and purposes of punishment.[344] The government has not intensively invested in developing cybercrime prevention skills through training and capacity building, or crime prevention programmes and initiatives. In addition, as elaborated in Chapter 2, an understanding of risk posed by cybercrime is still indistinct. The shortage of resources and insufficiency of legislation has made it challenging for the government to ensure close monitoring, and disruption of cybercriminal capability at the earliest opportunity, which can, in turn, assist in preventing an increase in cybercriminal activities and capability in the long term.

However, although not adequately experienced at this stage, Azerbaijani law enforcement authorities engage in training, international conferences and forums devoted to the fight against cybercrime, which can also enhance the capacity in both controlling and preventing cybercrime.[345] Furthermore, LEAs and other governmental institutions, academia and private sector entities have undertaken

---

[342] United Nations Economic and Social Council (UNESC), *United Nations Guidelines for the Prevention of Crime*, *Economic and Social Council resolution* (Council resolution 2002/13 - Annex) para 3.
[343] Article 2, Criminal Code of the Republic of Azerbaijan (1999).
[344] Ibid, Article 41.

[345] See for example, The plenaries of the Council of Europe Cybercrime Convention Committee (TCY plenaries) https://www.coe.int/en/web/cybercrime/t-cy-plenaries; 'Project Co-Ordinator in Baku Organised a Training Course on Basic Digital Forensic | OSCE POLIS' (*Polis.osce.org*, 2015) https://polis.osce.org/node/644; 'OSCE Trains Cybercrime Investigators from Georgia and Azerbaijan | OSCE' (*Osce.org,* 2017) https://www.osce.org/secretariat/307621; 'Regional Conference on Cybercrime Kicks Off in Baku' (*Aztv.az*, 2017) http://www.aztv.az/readnews.php?lang=en&id=4910.

prevention and awareness raising activities to foster a better protection against cyber-attacks, although these measures have not been specifically and directly pertaining to cybercrime prevention alone. Both the Computer Emergency Response Team and Electronic Security Service, for example, are tasked with raising awareness and operate through the Internet and social media platforms to enlighten the society about the threats of cybersecurity, as provided by Independent expert 1, NGO Representative 1, as well as Ministry Official 1, 2, 3, 4, and 5. Furthermore, easily accessible focal points operate under both of these organisations for reporting cyber-incidents and getting preventive advice.[346] The rising number of incidents reported to them can be regarded as a success in their activities, while, at the same time, as an indication of a growing necessity for stronger technical, legal and cooperation measures.[347] Rising threat awareness might not immediately lead to a considerable behaviour change. Nonetheless, neither the Computer Emergency Response Team, nor Electronic Security Service conduct regular evaluations (such as through surveys/questionaries) among internet users to see whether applied awareness raising techniques have been effective, and to make adjustments based on the results.

Service providers also play an important role in cybercrime prevention due to their technical capabilites and direct communication with customers. In general, service providers are in a better position than their customers in ensuring a protection against cyber-attacks, as they can monitor outgoing traffic for and receive reports of spam, worms or Denial of Service attacks, and prevent users' machines from getting infected through limiting their access to infectious sites.[348] In addition, subject to data protection laws, which are elaborated in Chapter 5, service providers can also store user data that can then be accessed and used by LEAs to conduct cybercrime investigations.[349]

---

[346] See for further information: 'Kompüter Insidentlərinə Qarşı Mübarizə Mərkəzi' (*Cert.gov.az,* 2017) http://cert.gov.az/en/pages2/about.html; http://www.cert.az/s/u/document/rfc_2350.pdf/.
[347] For example, the number of incidents reported to CERT in 2015 was around 1500, while this number exceeded 2700 in 2016 and 3500 in 2018.
[348] Ian Brown, Lilian Edwards and Christopher Marsden (n. 291), 19.
[349] UNODC (n. 71) 247.

3.7 Conclusion

This chapter has focused on the analysis of official policy responses of the country to cybercrimes, which constitutes the second research objective of this study. Given that a dedicated strategy and policies have not been developed in Azerbaijan, the Chapter critically analysed the measures undertaken by Azerbaijan to control and prevent cybercrime, which must be derived from its official policies, and translated into an implied national strategy. Besides, the evolution and reach of other relevant strategy and policies have been studied, which have further assisted to interpret the political stance of the country and create the whole picture of its policy against cybercrimes.

It was identified that an adequate level of cybersecurity has not been ensured, as the country struggles to adopt a systematic and comprehensive approach to addressing the problem. The country is missing a comprehensive vision and viewpoint in terms of clearly determining what should be achieved, in what way, who is responsible for which part, and how different elements relate to each other in the fight against cybercrime. There exists a wide range of cybersecurity areas to be developed to support the ICT development in the country. The country, however, also lacks the capacity and resources to develop national cyber security policies, which has resulted in failing to devise a comprehensive strategy and policies. Thus, apart from lacking sufficient level of sectorial capacity, the country has been missing management at strategic level.

Furthermore, it was determined that the lack of a dedicated strategy and policies has led to inadequacy of coordination of legal efforts. Lack of coordination at a strategic and policy levels has also resulted in difficulties in allocating the roles and responsibilities, notwithstanding a state-centric approach has been adopted in protecting citizens from cyber-attacks and cybercrime. This has also caused the misallocation of necessary resources to control and prevent cybercrime and other cybersecurity related threats.

It was also identified that significant variations are present in terms of the levels of organisational and personnel cybercrime specialisation among the government

authorities. Minimal levels of specialisation for cybercrime have been observed by prosecution and adjudication institutions, notwithstanding some levels of organisational and personnel cybercrime specialisation have been ensured to investigate cybercrime cases. In terms of the availability of qualified specialists and sufficient resources within the government authorities dealing with cybersecurity and cybercrime, there is a serious shortage at both investigation, and the prosecution and adjudication levels. Moreover, authorities significantly lack the ability to deal with electronic evidence, which is crucial to ensure the effectiveness and legality of criminal investigation and proceedings.

Next, it was determined that the government has undermined and underestimated the role of the private sector, industry, academia and civil society in Azerbaijan's cyber security alongside with government sector. This has reflected itself in the governments' preference of managing risks and threats posed to the country, by not treating those risks and threats as its strategic priority. Despite some types of measures being taken at both inter-agency and international levels to foster a better cooperation, a strong public-private partnership has not been developed to respond to cybercrimes more appropriately.

Another problem that has been exposed is that multilateral and mutually productive working relationships with other countries, as well as a sufficient number of operational channels for both formal and informal cross-border cooperation have not been developed yet, especially with the private sector.

In the last section of the Chapter, it was found that Azerbaijan does not have a dedicated cybercrime prevention plan. Nevertheless, LEAs and other governmental institutions, academia and private sector entities have undertaken some prevention and awareness-raising activities, although limited and uncoordinated.

CHAPTER 4: Substantive Laws

4.1 Introduction

The previous chapter studied official policy of Azerbaijan on the prevention and combatting of cybercrimes, and analysed the evolution and reach of the policy framework of Azerbaijan and its translation into national programmes. To elaborate and scrutinise further legal responses of the country to cybercrimes, which constitutes the second research objective of this study, this and the next Chapter will overview and evaluate the appropriateness of national legislation and frameworks. The criminalisation approach and substantive criminal laws are analysed in this Chapter, while Chapter 5 scrutinises investigatory powers, jurisdictional issues and international cooperation provisions.

As has been raised in the previous chapter, the overall adequacy of criminal and procedural laws in addressing the issues raised by cybercrime is often questionable due to their inconsistency with the nature of cyberspace and criminal conduct in this environment. One of the features narrowing the role of criminal law in virtual worlds is that the physical component was always the primary focus of criminal law, while virtual realities fostered by virtual worlds have not been the situation in mind over the centuries.[350] Furthermore, addressing the transnational character of cybercrime by applying established laws, which are mainly confined to territorial jurisdictions, becomes problematic as the territorial foundations of law and operational cooperation are complicated by cybercrime.[351] Thus, it can be argued that fighting twenty-first century crimes with an outdated law enforcement model is problematic. Application of the same traditional law-making and social regulation methods developed in accordance with, and to operate within, the physical boundaries of time and space might not often achieve the desired level of enforcement in cyberspace, which 'distances its inhabitants from local controls and the physical confines of nationality, sovereignty and governmentality'.[352] In addition, policy and lawmakers are seldom aware of the societal structure of

[350] Orin Kerr (n. 168), 417. See also Audrey Guinchard, 'Crime in virtual worlds: The limits of criminal law' (2010) 24 (2) *International Review of Law, Computers & Technology*, 175-182.
[351] Ben Hayes et al. (n. 75) 26.
[352] Yaman Akdeniz, Clive Walker and David S. Wall (n. 220).

cyberspace, and therefore their reflections through laws often fail to address the challenges of this new environment.[353]

Another feature leading to the confinement of the role of criminal and procedural laws in virtual worlds is the dynamics of the legislative process. In addition to general traditional offline obstacles involved while implementing laws (lack of relevant laws, differences in local laws and cultures), laws adopted for fighting cybercrimes may take a longer time to enforce than the evolution of technology and ICT itself, and therefore may become 'out of date' even before their full application.[354] The rapid pace of technological changes and constantly evolving cyber threats require exceptional agility to adapt to this dynamic environment, which also means 'a culture change for many departments and being more open, sharing information, working with others and communicating in different ways, including on related cross-government strategies such as those on digital, transparency and ICT'.[355]

Nevertheless, law still possesses an important role in responding to cybercrime. Laws identify acts as crimes, define the tools for addressing them, and distribute the roles and powers between actors in this objective. As a source of authoritative standards, criminal and procedural laws possess major roles in the fight against cybercrime, given that they are the foundation for the main processes of defining, combatting, investigating, prosecuting and punishing serious social wrongs. These legal tools should comprise 'an arsenal of well-defined cybercrime offences for use in prosecuting cybercriminals and procedural rules governing evidence-gathering and investigation'.[356] The absence of these necessary legal tools can make the effective pursuit of cybercriminals practically unattainable for law enforcement authorities. Notably, the key cybercrime concern for law enforcement has been

[353] Subhajit Basu, 'Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis' (2012) 3 *European Journal for Law and Technology*, 13.
[354] Susan W. Brenner (n. 156) 18.
[355] National Audit Office (n. 176) 30.
[356] Susan W Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law', (2001) 8 *E-Law: Murdoch University Electronic Journal of Law,* 8 [online] Available at: https://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html

determined by the European Parliament to be legal rather than merely technological.[357]

A wide range of issues may be addressed by legislation relevant to cybercrime. While criminal law and criminal procedure law are often perceived as being most relevant in dealing with cybercrime, constitutional and regulatory laws are also part of the legal responses and incorporate provisions pertaining to conditions and safeguards to be met to combat and prevent cybercrime. Thus, the analysis of those relevant provisions is also significant to ensure the completeness of this Chapter.

4.2 Conditions and Safeguards

After the collapse of the Soviet Union, Azerbaijan re-established its independence on October 18, 1991. Following independence, it started to implement fundamental reforms and thoroughgoing amendments to its legal system with the aspiration of instituting a democratic system of governance. Having declared itself as a democratic, legal, secular, unitary republic with a new constitution passed in 1995,[358] Azerbaijan went further to adopt legislative acts reflecting both constitutional and international values and principles. However, notwithstanding that the steps taken to develop pluralist political system, democratic institutions and human rights protection mechanisms, the legal system in Azerbaijan still preserves the old traditions, given that the system has been modified based on the Soviet communist legal system. Consequently, adequate implementation of emerging laws and rights has become challenging due to the absence of effective laws and mechanisms.

In Azerbaijan, the Constitution is the basis of legislative system and has the highest legal force in the hierarchy of laws.[359] The Constitution is followed by laws adopted by referendum, which should not contradict the Constitution.[360] Thus, it is worth to consider relevant constitutional provisions as they embody the basic principles of

[357] Ben Hayes et al. (n. 137), 10.
[358] Article 7, Constitution of the Republic of Azerbaijan (1995).
[359] Ibid, Article 147.
[360] Ibid, Article 149.

the legal system and addresses the relations between governmental authorities and civil rights and liberties of individuals. Also, given that constitutional provisions are not specific enough to serve as concrete legal orders and do not provide the clarity required for criminal norms,[361] where necessary, lower tier laws and legal instruments that provide the clarity in understanding the underlying standards and values, are also considered whilst elaborating concerning constitutional provisions.

In addition, while examining the legality of responses to cybercrimes it is also necessary to scrutinise their compatibility with relevant international laws and legal provisions emanating from the international treaties. Because, the international treaties, of which Azerbaijan is a party, are also an integral part of the legislative system,[362] and the provisions of international treaties shall apply in case of a possible contradiction between normative legal acts of Azerbaijan and those international treaties.[363] The adoption of complete and effective laws on cybercrime that meets human rights and the rule of law requirements has also been endorsed by the Council of Europe as one of the strategic priorities for cooperation against cybercrime.[364]

The Constitution determines that the state has a positive obligation to protect individuals against crimes and bring offenders to justice**.** The state guarantees protection of 'rights and liberties of all people'[365] without any 'restriction due to race, nationality, religion, language, sex, origin, conviction, political and social belonging'[366] and providing rights and liberties of a person and citizen is the highest priority objective of the state.[367] Thus, the rights and liberties of individuals must be strictly respected and protected in every action taken by the state in the fight against cybercrime, with the most relevant rights as follows.

The Constitution entitles everyone to the right to live in safety and security, and life, physical and spiritual health, property, living premises are protected from any

[361] Gabriel Hallevy, *A Modern Treatise on the Principle of Legality in Criminal Law* (Springer Berlin 2014) 34-35.
[362] Article 148, Constitution of the Republic of Azerbaijan (1995).
[363] Ibid, Article 151.
[364] Council of Europe (n. 231), 3.
[365] Article 26, Constitution of the Republic of Azerbaijan (1995).
[366] Ibid, Article 25.
[367] Ibid, Article 12.

infringements and acts of violence, except in cases envisaged by law.[368] In addition, pursuant to Article 32 of the Constitution, everyone is entitled to the right to personal immunity, implying that confidentiality of personal and family life is protected, and except cases envisaged by legislation interference in personal life is prohibited.[369] Incorporation of everyone's right to the protection of the law against arbitrary or unlawful interference with privacy, family, home or correspondence also ensures the compliance with international treaties to which Azerbaijan is a signatory.[370] The right to the confidentiality of correspondence, telephone communications, postal, telegraph messages and information sent by other communication means is guaranteed, and it might be restricted only in accordance with law, for preventing crime or ensuring the correctness of facts while conducting the investigation of criminal cases.[371] Next, the right to privacy is protected under Article 156 of the Criminal Code, which determines that illegal distribution of information on private life, consisting of the personal or family secrets of the person, is a crime. The Law on the Right to Access Information 2005 defines the private information or information on family life (hereinafter 'the private life') as 'any facts, opinions, knowledge on events, activities and circumstances directly or indirectly facilitating the identification of the person'.[372]

In addition to restrictions imposed by the Constitution on the right to personal immunity, the Constitutional Law on the Regulation of the Realization of Human Rights and Freedoms 2002 broadens the extent of limitations. According to this Law, the right to personal immunity can also be limited by the interests of national security, for the protection of health or morals, for the protection of the rights and

[368] Article 31, Constitution of the Republic of Azerbaijan (1995). Note: The clarification of 'cases envisaged by law' is not presented by the Constitution.
[369] Ibid, Article 32.1 and 32.2.
[370] See Article 17, International Covenant on Civil and Political Rights (ICCPR) UN Doc. A/6316 (1966); Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (1953) ETS No.5.
[371] Article 32.4, Constitution of the Republic of Azerbaijan (1995).
[372] Article 3, Law on the Right to Access Information 2005.

freedoms of others, for the prevention of disorder or crime, for ensuring public order and public safety or the economic well-being of the country.[373]

The restrictions imposed over the rights should not exceed the scope of restrictions permitted by the ECHR.[374] Compared to the ECHR, the ICCPR does not specify a list of limitations regarding privacy under article 17, but rules out that the right shall not be subjected to 'arbitrary or unlawful interference'.[375] According to the UN Human Rights Committee (HRC) the term 'lawful' incorporates both the compliance with law and with the provisions, aims and objectives of the ICCPR, while the concept of arbitrariness can be extended to require from the imposed limitations to be both 'lawful' and 'reasonable' in the particular circumstances.[376] Consequently, while trying to limit the enjoyment of this right by citizens, the State has to satisfy the requirements of 'reasonableness' in order for its actions to be compliant with international treaties. Otherwise, the responses given by the State could breach its international obligations and therefore unlawful, as international treaties, of which Azerbaijan is a party, are an integral part of the legislative system.[377]

The Constitution also entitles everyone to the freedom of lawfully looking for, obtaining, transmitting, developing and distributing information, and guarantees the freedom of mass media by prohibiting state censorship over mass media, including press.[378] Despite both the ICCPR and ECHR including this right as a part of 'Freedom of expression', which also covers freedom to hold opinions and impart information and ideas without interference,[379] the Constitution arranges these rights separately, yet, the scope of restrictions imposed is compliant with ICCPR and ECHR. So, there is a separate article (Article 47) concerned with the freedom of

---

[373] Article 3, Constitutional Law on the Regulation of the Realization of Human Rights and Freedoms 2002, 404-IIKQ.

[374] See: Article 8.2, European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (1953) ETS No.5.

[375] Article 17, ICCPR 1966.

[376] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988.

[377] Article 148, Constitution of the Republic of Azerbaijan (1995).

[378] Ibid, Article 50.

[379] Article 10, European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (1953) ETS No.5; Article 19, International Covenant on Civil and Political Rights (ICCPR) UN Doc. A/6316 (1966); see also, *Guerra v Italy,* App no.14967/89, [1998] ECHR 7, para 58; *Társaság a Szabadságjogokért (TASZ) v. Hungary* no. 37374/05, [2009] ECHR 618, para 37.

thought and speech. The Constitution prohibits both the forced promulgation or renouncement of thoughts and convictions, and any agitation and propaganda provoking racial, national, religious and social discord and animosity.[380] Notwithstanding that Azerbaijan has neither signed, nor ratified the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, prohibition of this activity is directly reflected by the Criminal Code, Article 283.[381] Criminalisation of this act will be considered in the next subsection.

Although the restrictions over the freedom of information and the freedom of thought and speech have not been signified by the Constitution itself, they can also be subjected to certain restrictions in those same cases, which create the grounds for the imposition of limitations over the right to personal immunity according to the Constitutional Law (2002).[382] In addition to those limitations the freedom of information, alongside with the freedom of thought and speech, can also be to restricted in the interests of ensuring the territorial integrity of the country, the authority and impartiality of the court, as well as for preventing the disclosure of information received confidentially.[383]

Considering the incorporation of terms 'information' and 'personal data' in legal texts covering cybercrime issues, it is useful to elaborate these terms from the national law standpoint especially as none of these terms has been defined by Criminal Code (1999) or Criminal Procedural Code (2000). Therefore, relevant regulatory laws are studied for the clarification of their meaning. According to the Law on Freedom of Information 1998, 'information' means 'news about events, processes, facts and persons appearing in the nature, society and state regardless of the presentation form'.[384] Depending on the form of access, the Law on Freedom

[380] Article 47, Constitution of the Republic of Azerbaijan (1995).
[381] See Article 283, Criminal Code (1999); See for the chart of signatures and ratifications of Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003) ETS No.189 *(*Status as of 01/09/2018)
[382] Article 3, Constitutional Law on the Regulation of the Realization of Human Rights and Freedoms 2002, 404-IIKQ.
[383] Ibid.
[384] Ibid, Article 1.

of Information 1998 classifies information into two groups: 'publicly accessible' (open) and 'with limited access'.[385] Information regarding the 'state, professional (lawyer, notary, doctor), service, bank, commercial, investigation and court secrets, information on personal and family life of individuals, terrorist acts' are included under the 'limited access' information group,[386] while the 'publicly accessible' (open) information is defined by the Law on the Right to Access Information 2005 as 'the information to which the access is not limited due to the law'.[387] This Law specifies that the information to which the access is limited in accordance with law is divided into 'secret' and 'confidential' information: state secret is classified as 'secret', while 'state, professional (lawyer, notary, doctor), commercial, investigation and court secrets' is nominated as being 'confidential'. Before the amendments made in 2010 on the Law on the Right to Access Information 2005, 'personal data' was also included under the category of 'confidential' information, while now, personal data itself is divided into two groups: 'confidential' and 'open'.[388]

The term 'personal data' is defined by the Law on Personal Data 2010 as 'any information directly or indirectly leading to the identification of a person'.[389] This definition is parallel to the one provided by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, which was signed and ratified by Azerbaijan in 2010.[390] Nevertheless, neither the Law on Personal Data, nor the Convention (1981) provide detailed clarification of personal data, so, which particular data is incorporated or omitted by this definition is equivocal. The information regarding 'the name, surname and the father's name of an individual is 'open' personal data', and therefore, ensuring the confidentiality of 'open' information is not required.[391] Furthermore, the Law (2010) does not provide clear provisions on the collection, processing and protection of personal data.

[385] Ibid, Article 8.
[386] Ibid, Article 10.
[387] Article 34, Law on the Right to Access Information 2005.
[388] Ibid, see also: Article 5, Law on Personal Data 2010.
[389] Article 3, Law on Personal Data 2010.
[390] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) ETS No.108. Signed and ratified by Azerbaijan in 03/05/2010.
[391] Ibid, Article 5.3.

Instead, it puts forward requirements to be met while establishing data resources and data systems on personal data by referring to the notions such as 'the compliance with the main human and civil rights and freedoms' as well as 'the rule of law', and 'principles of balancing voluntary participation with obligation', which are challenging to apply.[392] The Convention (1981), however, identifies special categories of data and makes it clear that personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, or relating to criminal convictions should not be processed automatically unless domestic law provides appropriate safeguards.[393] What is more, the provisions set forth by the Law (2010) for protection of personal data are also ambiguous. The Law, in general, specifies that protection and security of personal data should be provided by the owners and operators,[394] and personal data published without the consent of an individual must be removed from commonly used information systems following a written demand from the individual concerned, a court, or the executive branch.[395] However, provisions on physical protection of personal data and protection of its integrity, as well as limitation of access to it, and registry of the equipment and software used are missing.

Next, everyone is entitled to the freedom of conscience and religion, and thus, can freely express and spread religious beliefs, so long as they are not violating public order and public morals, or using those beliefs and convictions as an excuse for infringements of the law.[396] In addition to public morals, the honour and dignity of individuals are also guaranteed with the state protection and besides, according to the Constitution, everyone has the right to defend his/her honour and dignity, which cannot be subjected to any humiliation.[397] Neither the Constitution, nor the Criminal Code and other laws specify 'honour' and 'dignity'. The Supreme Court of the Republic of Azerbaijan has defined 'honour' as the value given to an individual

[392] Article 4, Law on Personal Data 2010.
[393] Article 6, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) ETS No.108.
[394] Article 5.5, Law on Personal Data 2010.
[395] Ibid, Article 5.7,
[396] Article 48, Constitution of the Republic of Azerbaijan (1995).
[397] Ibid, Article 46.

based on his attitude to moral, spiritual qualities, to other people, to the state and to the community, and 'dignity' means a person's perception of his / her moral and intellectual qualities, position and influence in society, and self-esteem.[398]

The Constitution also ensures the right to enjoy intellectual property signifying that copyright, patent rights and other rights for intellectual property are under the protection of law.[399] Besides the Civil Code (2000), the standards, range of IP laws[400] are enacted mainly by the Law on Enforcement of the Intellectual Property Rights and Fight against Piracy 2012. Moreover, Azerbaijan is a member of the World Intellectual Property Organization (WIPO) and has become a contracting party to all of the treaties that article 10 (Offences related to infringements of copyright and related rights) of the Convention on Cybercrime concerned, except the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).[401]

Intellectual property rights are defined as 'the rights to works, performances, phonograms, programs of broadcasting organizations, topographies of integrated circuit, databases, folklore expressions (traditional cultural expressions), inventions, utility models, industrial designs, trademarks and geographical indications'.[402] The Law determines that illegal utilization of copyrights and other related rights (including the pirated copies) entails civil, administrative and criminal liability in accordance with the legislation of the Republic of Azerbaijan.[403]

Consequently, Azerbaijan shall ensure that criminalization provisions, which will be analysed in the next section, are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties.

---

[398] Section 3, Resolution of the Plenum of the Supreme Court of the Republic of Azerbaijan 'On the judicial practice on considering complaints in private criminal prosecutions' (Feb. 21, 2014 No 03).
[399] Article 30, Constitution of the Republic of Azerbaijan (1995).
[400] See for example, Law on Patents 2009, № 312-IQ; Law on Trademarks and Geographical Indications 2010, № 504-IQ; Law on Copyright and Related Rights 1996, № 115-IQ; Law on Legal Protection of Compilations of Data 2013.
[401] See for the full list of WIPO-administered treaties, which Azerbaijan is a contracting party: http://www.wipo.int/treaties/en/ShowResults.jsp?country_id=11C.
[402] Article 1, Law on Enforcement of the Intellectual Property Rights and Fight against Piracy 2012, № 365-IVQ.
[403] Ibid, Article 16.

4.3 Substantive criminal law provisions

Having considered conditions and safeguards provided for under the domestic laws as well as underlying values and standards to be protected in combatting cybercrimes, this section reflects upon criminalisation of specific offences and specific criminal norms, as well as general provisions and principles of the criminal statute shaping the criminalisation approach.

Criminal legislation of Azerbaijan is entirely codified under the Criminal Code (1999). It has a central role to play in introducing legal objects to be safeguarded from cybercrime and in extending protection of traditional legal interests against new forms of interference and attacks. The Code is comprised of two parts: 1) the general part and 2) the special part.

The General part deals with the norms establishing the principles and general provisions of criminal law, such as tasks and principles of the criminal statute, concept and classification of crimes, features of criminal responsibility of persons and juveniles as well as concept, purpose, types and imposition of punishment. Provisions on specific offences are laid out in the Special part, which determines the necessary elements of a crime and establishes the types and scope of sanctions for their commission.

Before embarking upon a discussion on specific offences, it is conducive to illustrate selective general provisions and principles of the criminal statute to establish a complete view and grounds for scrutinizing the criminalisation of particular offences and its components. The general provisions and principles will be analysed comparatively with the provisions and principles determined by the previous criminal statute of Azerbaijan (Criminal Code of Azerbaijan SSR 1960), while the specific cybercrime offences will be studied comparatively with the pre-harmonised version of the current Criminal Code (1999) and in the light of the Council of Europe Convention on Cybercrime (2001) provisions.

4.3.1 General principles and provisions of the criminal statute

Reforms and amendments of the legal system after independence included the adoption of a new criminal code by the Parliament on September 30, 1999, which came into force on September 1, 2000.[404] The Code is 'based on the Constitution of the Azerbaijan Republic and generally accepted principles and norms of international law'.[405] It replaced the previous Criminal Code of Azerbaijan SSR 1960, which was based on the principles of Soviet criminal law and aimed at protecting 'the socialist political and economic system, along with the socialist legal order'.[406] The purpose of the current Criminal Code (1999) is different from those determined by the Criminal Code (1960). It spells out its tasks in Article 2 as 'maintaining peace and security of mankind, protecting the rights and freedoms of person and citizen, property, economic activity, public order and safety, the environment, the constitutional system of the Azerbaijan Republic against criminal encroachment, as well as the prevention of crimes'.[407] In addition to other innovations, the current Code explicitly determines five basic principles of criminal statute and criminal responsibility: legality, equality before the law, culpability, justice and humanism.[408] Determination of these principles in the Code can also be regarded as an intent to depart from those exercised by the previous Criminal Code of Azerbaijan SSR 1960, which was focusing on 'protecting the social, political and economic system of the USSR …and the socialist rule of law from criminal encroachments'. [409]

The criminal legislation adopts and assumes the principle of *nullum crimen sine lege* (no crime without law), which requires that a person may only be found guilty of a crime if the conduct constituting a criminal offence is described by law.[410] The formal definition of a crime is specified by the Code 1999 as 'a socially dangerous act (action or inaction), committed with guilt and prohibited by the present Code

[404] See the Law on Approval, Entry into force of the Criminal Code and the Legal Regulation Issues Connected With it 1999, № 787-IQ.
[405] Article 1.2, Criminal Code (1999).
[406] Richard J Terrill, *World Criminal Justice Systems* (Routledge; 9th edition. 2015) 421.
[407] Article 2.1, Criminal Code (1999).
[408] Ibid, Article 4.
[409] Article 1, Criminal Code of the Azerbaijan SSR 1960.
[410] Article 1, Criminal Code (1999).

under the threat of punishment'.[411] So, the criminalisation of an act requires the incorporation of four compulsory elements, comprising social danger, illegality, punishability, and culpability.

Social danger expresses the social nature of a crime and is an objective (material) feature, which harms or creates a threat of harm to the socially important values and interests regardless of the perception and will of a legislator.[412] The objective developments of the society widely affect the recognition of the social danger of certain conducts, while the evaluation of the social danger of the act is performed at the legislative and executive levels.[413] Therefore, it is necessary to have deep insight and knowledge of the nature of these values and interests to entail justification of the norm in the statute and therefore serve their protection more effectively.[414]

The Criminal Code (1999) puts forward socially important values and interests in a different way due to the changed political, socio-economic and socio-cultural situation. A consolidated list of objects of penal protection is provided by Article 2, which includes peace and security of humanity, the rights and freedoms of person and citizen, property, economic activity, social order and public safety, the environment, the constitutional system of the Azerbaijan Republic.[415] It can be argued that Article 2 represents a hierarchy of the values and interests provided by penal protection: [416] (1) humanity, (2) personality, (3) society, and (4) State, which is also reflected in the construction of the Special part of the Criminal Code (1999). Thus, the current criminal legislation has taken a more liberal individualist stance. Based on the answers provided during the interviews, however, it was found that in practice the government still prioritises the protection of state interests over interests of individuals in the fight, in particular, against cybercrime. This priority

[411] Ibid, Article 14.
[412] Firudin Samandarov, *Criminal law: General Part (Cinayət hüququ: Ümumi hissə)* (Baku: Hüquq ədəbiyyatı, 2002) 215.
[413] Iryna Marchuk, *The Fundamental Concept of Crime in International Criminal Law: A Comparative Law Analysis* (Heidelberg: Springer, 2014) 52.
[414] Isfandiyar Aghayev, *Corpus delicti: its concepts, elements, significance* (Moscow, 2008) 64.
[415] Article 2.1., Criminal Code 1999.
[416] Isfandiyar Aghayev*, Criminal Law: The General Part* (Leipziger Universitätsverlag, 2015) 72.

might also be due to the assumption, as was supported by Parliament Officer 1 and NGO Representative 1, that cybercrime does not pose too much of a danger to the public, and it is primarily the government sector that is vulnerable to cybercrime. Analysis of institutional and technical measures undertaken in Azerbaijan against cybercrime in the previous chapter also helps to back up the argument that the government does not put the individual at the centre of protection in the fight against cybercrime, and therefore the Soviet socialist way of approaching a problem is still operative.

Compared to the previous Criminal Code 1960, the current Code 1999 includes 'harm' as a signifying element of the 'social danger'. Article 14 clarifies that an act that neither causes harm, nor creates the threat of causing harm to the person, society or the State should not be admitted as a crime, because by the virtue of their insignificance those acts are not considered to represent a social or public danger.[417] Thus, the formal presence of 'harm' or 'harmful result' has been included as a necessary element for the majority of crimes determined by the current Criminal Code. Depending on the object protected, socially dangerous acts can inflict harm on (1) participants of social/public relations or subjects, (2) activities of these subjects and (3) values and items related to the social/public relations.[418]

If an act is not socially or publicly perceived as harmful and, therefore, dangerous, it should not be regarded as a crime. This test is also applicable to the criminalisation of cybercrime. In Azerbaijan, the lack of public perception of social danger posed by cybercrime has led to under-reporting and underestimation of cyber incidents/offences at different levels. As a result, those not directly associated with cybercrime or cyber-incident handling have a very limited vision of how and why certain conducts pertaining to cybercrime should be criminalised unless there is a wide public outcry.[419]

Once illegality is applied, the principle of legality determined by the Criminal Code manifests the concept of unlawfulness in the Article 5 by implying that the

[417] Article 14, Criminal Code (1999); see for comparison Article 7, Criminal Code 1960.
[418] Firudin Samandarov (n. 412), 216.
[419] See Chapter 2, Section 2.4.

criminality of a deed, its punishability and other legal consequences shall be determined by the Code alone and the application of criminal law by analogy is not allowed.[420] The Code further specifies that only the commission of an act (in the form of action or inaction) containing all the indicia of the constituent elements of a crime provided for by the Code can be a ground for criminal liability.[421] An act that is not penalised by law cannot be acknowledged as a crime, even though it poses a social danger. Thus, the fulfilment of the value of legality of criminal law responses to cybercrimes is strictly dependent on the norms determined by the Criminal Code.

Next, punishability can be defined as the threat of negative penal consequences for a criminal action. Although the Criminal Code (1999) has set up types of punishments and other penal measures, not all cases of commission of socially dangerous acts are subject to criminal punishments. This is due to the reason that the Criminal Code (1999) also determines certain grounds where the punishment is not attributed for a socially dangerous act (for example, due to the active repentance, reconciliation with the victim, changed situation, or expiration of statutes of limitation).[422] Therefore, punishability should not be equated with the imposition of punishment, as it conveys mere ability to impose criminal responsibility once the breach has occurred.[423]

Given that different types of wrongdoing (including criminal and administrative) can harm the same interests, it is useful to highlight features differentiating crimes from other wrongdoing, which makes the imposition of criminal punishment justifiable. This differentiation will further help to examine the justifiability of criminalisation and therefore imposition of criminal punishments for cyber offences. The signs allowing the differentiation can be summarised as follows:

[420] Article 5. Criminal Code (1999).
[421] Ibid, Article 3.
[422] See Articles 72-75, Criminal Code (1999).
[423] Ardsley Kosachenko (Edn.), *Criminal law: General Part* (4th edn, Moscow: Norma Publisher, 2009) 170-171.

"- *Object* - Crimes encroach those socially important fundamental values and interests, the breach of which can only be appropriately regulated by the criminal statute;

- *Nature of illegality* – Crime is a criminally-illegal act, acknowledged directly and only by the criminal statute;

- *Nature of results* – Commission of a crime accompanied by the most severe measures of the law enforcement, while other offences cause the realization of less severe measures;

- *Nature and scale of social danger* – crimes exhibit greater social harm, than other offences. Since violence usually accompanies criminal deeds, guilt exhibited by offenders is more serious."[424]

The nature and scale of social danger also constitute the grounds for categorising crimes. The four categories of crime and maximum punishments imposed are:[425]

1) Crimes not representing great social danger	Up to 2 years of imprisonment
2) Minor crimes	Up to 7 years of imprisonment
3) Grave crimes	Up to 12 years of imprisonment
4) Especially grave crime	12+ years or life imprisonment

According to the classification provided by the Criminal Code, cybercrimes, as identified by the relevant special part articles of the Code, which will be discussed later in this Chapter, are regarded either 'crimes not representing great social danger' or 'minor crimes', depending on the type, consequences and punishments imposed.

The Criminal Code lists the purposes for punishment that include the restoration of social justice, reformation of the convicted person, and the prevention of the commission of a new crime.[426] Thus, it is important to bear in mind that aside from

[424] Isfandiyar Aghayev (n. 414), 45-46.
[425] Article 15, Criminal Code (1999).
[426] Ibid, Article 41.

being ‘effective, proportionate and dissuasive’,[427] sanctions should also serve these ultimate purposes.

Culpability is another necessary element for an act to be specified as a crime. It involves the mental/subjective attitude of a person to his socially dangerous action and its consequences penalised by law.[428] If the guilt has not been established, a person cannot be imposed to criminal responsibility.[429]

The Criminal Code (1999) determines that guilt is manifested intentionally or through negligence.[430] Intention itself is also expressed in two forms: direct or indirect. A crime is commissioned with direct intention if the person understood that his action (inaction) is socially dangerous, and had foreseen and desired its socially dangerous consequences.[431] For indirect intention, a person must knowingly allow socially dangerous consequences to take place in order for the act to be regarded as being commissioned with indirect intention.[432] Next, a crime is committed negligently if the person foresees the possibility of the onset of socially dangerous consequences of his conduct, but thoughtlessly expects those consequences to be prevented, or if he fails to foresee the possibility of occurrence of socially harmful consequences of his acts, although he could and should have done so (gross negligence).[433] It is important to note that all of the crimes reflected under the relevant Criminal Code Chapter dealing with cybercrimes require the incorporation of intentional commission as a *mens rea*. The rationale of the intentionality requirement resides in the ease of doing things on computer systems, as well as ease of changing or deleting computer data due to its intangible and rather volatile nature.[434]

Criminal responsibility is influenced by two further factors: age and mental capacity. For a person to be subjected to criminal liability, he/she should be a mentally

[427] Article 13, Council of Europe Convention on Cybercrime (2001) ETS 185.
[428] See, Article 7 of the Criminal Code (1999).
[429] Ibid, Article 7.2.
[430] Ibid, Article 24.
[431] Ibid, Article 25.1.
[432] Ibid, Article 25.2.
[433] See Article 26 for the clarification of each forms.
[434] Paul De Hert, Gloria González Fuster and Bert-Jaap Koops, ‘Fighting Cybercrime in the Two Europes.’ (2006) 77 *Revue internationale de droit pénal*, 508.

capable person who has reached the statutory age of responsibility envisaged by the Code.[435] In general, the age of 16 is a prerequisite for being subjected to criminal responsibility, however there are several exceptions made to this rule. Individuals who, before the commission of a crime, have reached the age of 14 years can be subjected to criminal liability for specified crimes that are shortlisted by the Criminal Code (1999), which does not include any act that can be considered to be 'cybercrime', as defined in this thesis in Chapter 2.[436] Given that, for example, the majority of hackers start their 'careers' during adolescence, around 13-14 years of age,[437] it can be suggested that, a revision is needed for the amplification of the list of crimes provided by Article 20.2 of the Criminal Code. Fixing the minimum age of criminal responsibility at too high an age level, in particular for cybercrime, can be also problematic from the perspective of combating cybercrime, as young people are increasingly involved in online delinquency and being drawn into cyber-criminality.[438]

4.3.1.1 Attempt and aiding or abetting

The Criminal Code of the Republic of Azerbaijan provides for criminalisation of attempt and aiding or abetting the commission of crimes. Pursuant to Article 32, the abettor is a person who has abetted another person in committing a crime by persuasion, deal, threat, or by any other methods. The subjective element of the actions of abettor is characterised by his/her direct intention in involving in a crime.[439] Criminal liability is attached for acts of aiding where the person assists in the commission of a crime by advice, instructions, information, or providing means, tools, or by removal of obstacles for the commission of a crime, or, promises to conceal the criminal, as well as means and instruments used for committing a

[435] Ibid, Article 19, Criminal Code (1999).
[436] For a list of crimes leading to a criminal responsibility in cases committed before the age of 14, see Article 20.2 of the Criminal Code (1999).
[437] Raoul Chiesa, Stefania Ducci and Silvio Ciappi, *Profiling Hackers* (Boca Raton: Auerbach Publications, 2009) 122, see also: Randall Young, Lixuan Zhang and Victor R. Prybutok, 'Hacking into the Minds of Hackers', (2007) 24 *Information Systems Management*, 281-287.
[438] See for further discussion, Elvin Balajanov, 'Setting the Minimum Age of Criminal Responsibility for Cybercrime' (2017) 32 *International Review of Law, Computers & Technology*, 5-6.
[439] See Article 25.1 of the Criminal Code.

crime, traces of the crime, the objects procured through the crime, and promise to acquire or sell such items.[440] Article 33 of the Criminal Code stipulates that the abettor and the person who have aided shall be subject to criminal liability, except for the case when they were concurrently the co-perpetrators of the crime. Consequently, the Criminal Code (1999) has established as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any crimes discussed in this Chapter and incorporated in the Convention on Cybercrime.[441]

The Convention on Cybercrime further requires that the attempt be criminalised with respect to offences established in accordance with Articles 3 (Illegal Interference), 4 (Data Interference), 5 (System Interference), 7 (Computer-related forgery), 8 (Computer-related fraud), 9(1)(a) (producing child pornography for the purpose of its distribution through a computer system); and 9(1)(c) (distributing or transmitting child pornography through a computer system).[442] This requirement is fully met by the Criminal Code. Article 27 provides that criminal liability for attempted crime, which is a deliberate action designed to perpetrate a crime but was not completed due to the reasons beyond the person's control, is determined under the relevant article of this Code, which provides for liability for completed crimes, by giving reference to Article 29 (Attempt to commit a crime).

4.3.1.2 Corporate liability

The current legal trend to recognise corporate liability has also been followed by Azerbaijan. In 2012 pursuant to the Law on Amendments to the Criminal Code of the Republic of Azerbaijan, the basis and conditions for application of penal measures to legal entities were fixed in the Criminal Code.[443] At present, similar to the conditions determined by the Convention on Cybercrime, four conditions must be met in Azerbaijan for criminal responsibility to attach:

[440] Ibid, Article 32.5.
[441] See Article 11.1 Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[442] Ibid, Article 11.2.
[443] Law on Amendments to the Criminal Code of the Republic of Azerbaijan 2012, № 408-IVQD.

"1) The criminal offence must have been committed for the benefit or in the interests of the legal person;

2) The offence must have been committed only by a natural person who has a certain position within the legal entity;

3) The person must act on the basis of one of these power:

- a power of representation of the legal person;

- an authority to take decisions on behalf of the legal person;

- an authority to monitor the work of the legal person.

4) Only, one of the crimes specified in Article 99-4.6 of the Criminal Code must have been committed."[444]

Hence, besides other offences explicitly determined in Article 99-4.6, pursuant to above conditions, penal measures are applied to legal persons for the commission of the following offences, that are studied in this Chapter: Turnover of child-pornography (Article 171-1); Illegal dissemination of pornographic materials or items (Article 242); Illegal access to computer system (Article 271); Illegal interception of computer data (Article 272); Illegal interference (Article 273); Misuse of devices (Article 273-1); Forgery of computer data (Article 273-2); Public appeals directed against the state (Article 281); Incitement to national, racial, social or religious hostility (Article 283); Forgery, illegal preparation, sale or use of forged official documents, state awards, stamps, seals, and letter-head (Article 320); Violation or humiliation of the honour and dignity of the state - the President of the Republic of Azerbaijan (Article 323).

The Criminal Code does not attach liability to legal entities for the commission of offences related to infringements of copyright and related rights. However, Article 99-4.2 clarifies that corporate liability does not exclude individual responsibility.

To sum up, the applicable provisions regarding the liability of legal entities determined by the Criminal Code are very closely modelled on the corresponding provisions in the Convention on Cybercrime. The main difference between the two is the exclusion of copyright and related rights' infringements from the list of offences specified by Article 99-4.6 of the Criminal Code, which attach criminal liability to legal persons.

[444] See Article 99-4 of the Criminal Code (1999) for the full list.

4.3.2 Analysis of cybercrime offences

A dedicated chapter regarding the 'Crimes in the Sphere of Computer Information' had been contained in the pre-harmonised version of the Criminal Code (1999). It specified 'illegal access to computer information', 'creation, use, and dissemination of harmful computer programmes', 'Infringement of the rules of operation of the computer, computer system or network by a person with the right to access' as crimes.[445] In order to harmonise the Criminal Code (1999) with the Cybercrime Convention, the Chapter (30) devoted to 'crimes in the Sphere of Computer Information' was amended in 2012.[446] The new version of the Chapter, entitled 'Cybercrimes', provides legal solutions for 'illegal access', 'illegal acquisition', 'data interference', 'system interference', 'misuse of devices' and 'internet forgery'.[447] In addition, the circulation of child pornography has also been criminalised since 2012.[448] Detailed analysis and comparison of specific offences and their elements determined by both versions (pre-harmonised and harmonised) will be provided later in this sub-heading.

Criminal offences that are incorporated in the concept of 'cybercrime' are included in the Criminal Code without determining a strict definition for that term. On the one hand, it can be argued that only the acts or offences described in Chapter 30 can be considered as cybercrimes according to the Criminal Code. On the other hand, it is noticeable that the application of computer technologies can be involved in the commission of more than 15 crimes directly and 25 crimes indirectly which are not included in Chapter 30.[449] These crimes have been allocated to different chapters

[445] See the previous version of the Criminal Code (1999), Articles 271-273, accessible via http://e-qanun.az/code/11#.
[446] Law on Amendments to the Criminal Code of the Republic of Azerbaijan 2012, № 408-IVQD.
[447] Articles 271-273-2, Criminal Code (1999).
[448] See Ibid, Article 171-1, See also, Law on Amendments to the Criminal Code of the Republic of Azerbaijan 2012, № 408-IVQD.
[449] See for example, Article 155 - Infringement of secret correspondence, telephone conversations, mail, telegraph or other messages; Article 165 - Infringement of author's or adjacent rights; Article 166. Infringement voting and patent rights; Article 197 - Illegal use of a trade mark; Article 198 - Obviously false advertising; Article 171-1 - Turnover of child pornography; Article 189 - Implementation of telephone conversations by illegal use of a telephone line; Article 202 - Illegal reception or disclosure of a data; Article 242 - Illegal distribution of pornographic materials or objects; Article 244-1: Organization of gambling and places for gambling; Article 281 - Public

of the Criminal Code, due to the variation between the objects and values to be safeguarded by the criminal sanctions. This is because the criminal offences identified by the Criminal Code are mainly classified due to the objects and values to be protected under criminal punishment. Chapter 30 – 'Cybercrimes' - of the Criminal Code is included in the 10th section which is titled as 'the Crimes against Public Security and Public Order'. This Chapter determines only the offences against the confidentiality, integrity and availability of computer data and systems, and computer-related offences as cybercrimes. Consequently, some of the content-related offences and offences related to infringements of copyright and related rights are excluded from the Chapter. Therefore, offences concerning the turnover of child pornography have been covered elsewhere in the Code by the 'Crimes against Minors and Family Relations' Chapter,[450] while the offences related to infringements of copyright and related rights' are contained in 'Crimes against Constitutional Rights and Freedoms of the Person and the Citizen'[451] and 'Crime in Sphere of Economic Activities'[452] Chapters.

A deeper and clearer insight into the objects, values and interests to be protected by the Criminal Code can be provided through examining the meanings of the underlying concepts, which relevant criminal acts embody. As mentioned before, 'computer system', 'computer program', 'computer data' and 'computer information' are the concepts commonly used for describing the elements of cybercrimes. Compared to the criminalisation approach adopted, elements of the definition of surrounding concepts to the term 'cybercrime' in the Criminal Code are meant to be predominantly similar to the Convention on Cybercrime due to the harmonisation required by ratification. So, 'computer system' is defined as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program,

---

appeals directed against the state; Article 283 - Excitation of national, racial or religious hostility; Article 284 - Disclosure of the state secret; Article 313 - Service forgery. Criminal Code (1999).

[450] Chapter 22, Article 171-1, Criminal Code (1999).

[451] Ibid, Chapter 21, Article 165 - Infringement of author's or adjacent rights; Article 166 - Infringement voting and patent rights.

[452] Ibid, Chapter 24, Article 197 - Illegal use of a trade mark.

performs automatic processing of data'.[453] 'Computer data' is used to represent 'any representation of facts, information, programs or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function'. [454] However, neither the Convention on Cybercrime nor the Criminal Code has defined the term 'computer program' directly.[455] Also, other slight differences are present that can result in discrepancies. For example, the Criminal Code has defined neither the 'service provider', nor the 'traffic data', notwithstanding the Convention on Cybercrime does.[456] Instead, Law on Telecommunication 2005 defines the terms 'traffic' and 'telecommunication service provider', which are too broad and substantially different from the definitions provided by the Convention. [457]

While analysing primary source legislation, it is essential to identify differences between the elements of cybercrime offences articulated in the Criminal Code (1999) and the Convention on Cybercrime. In addition, the offences will be studied comparatively with the pre-harmonised version of the current Criminal Code Chapter to provide further elucidation. Thus, each offence will be studied in accordance with the following structure:

i. Description of a crime and its elements;
ii. Sanctions;
iii. Comparison with the pre-harmonised Criminal Code Chapter (30);
iv. Compatibility with the Convention on Cybercrime provisions.

It also needs to be clarified that apart from the offences directly reflected in Chapter 30 of the Criminal Code, the acts falling within the coverage of the established 'working definition of cybercrime and a speculative set of actions that may be

[453] Ibid. Article 271, Criminal Code (1999). See also; Article 1, Council of Europe, Convention on Cybercrime, 2001.
[454] Ibid.
[455] It is the Article 1.0.5 of the Law on Enforcement of the Intellectual Property Rights and Fight against Piracy 2012, which defines the term 'computer program' as 'words, codes, schemes and a set of instructions in any other form in a machine-readable form that enable a computer to achieve certain goals or results'.
[456] Article 1, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[457] Article 1, Law on Telecommunication 2005, № 927-IIQ.

embraced by this term'[458] are also analysed in this section. Thus, in addition to the computer integrity crimes (illegal access, illegal interception, data interference, system interference and misuse of devices), computer-assisted crimes (computer-related forgery and computer-related fraud, computer-related identity theft, online intellectual property theft) are also covered in this section. Moreover, as described in Chapter 2, there are certain content-related offences criminalised in Azerbaijan,[459] the scale and reach of which have been increased due to the expanding use of ICTs and the Internet, and vast opportunities and grounds provided by cyberspace for their commission. To this end, 'Illegal distribution of pornographic materials or objects', 'Incitement to national, racial, social or religious hostility', 'Libel' and 'Insult', as well as 'Public appeals directed against the state', 'Violation or humiliation of the honour and dignity of the head of the state' are also briefly studied within the substantive criminal law perspective.

4.3.2.1 Computer integrity crimes

I. Illegal access

i. With a view to the harmonisation with the Convention on Cybercrime, Article 271.1 of the Criminal Code specifies the crime of illegal access to the computer system as intentional illegal accessing the whole or any part of a computer system without right, by infringing security measures, or with the intent of obtaining computer data or other personal intent.[460] This Article makes express provisions for two different offences: illegal access to a computer system or any part thereof with violation of security measures, and illegal access to a computer system or any part thereof with a purpose of abstraction of computer information stored therein or with any other personal intent.

The security (confidentiality, integrity and availability) of computer systems and computer data is threatened by this criminal act, and as a basic offence, illegal access does not necessarily involve immediate material adverse impact or effects

[458] See Chapter 2. Section 2.2.
[459] See Articles 147, 148, 198, 242, 244-1, 281, 283 of the Criminal Code (1999).
[460] Ibid, Article 271, Criminal Code (1999).

on systems or data. The Criminal Code provides for the criminalisation of illegal access to either the whole or part of the computer system or to computer data.

The guilty act is represented by accessing the whole or any part of a computer system without right, irrespective of the type and method of connection and communication, by infringing security measures, which can be interpreted as a basic hacking offence, or with the intent to obtain computer data or other personal intent. It can also be argued that the intentional failure to log out from a computer system, or illegally remaining in the whole or part of a computer system can also be incorporated in the concept of illegal access. This is because the offender still acquires access without authorisation for being able to remain in the system.[461]

A narrower approach attaching additional qualifying circumstances has been adopted by the Criminal Code with regard to the illegal access to a computer system or any part thereof in violation of security measures. This act can be commissioned by merely logging on to a computer system belonging to another without permission. Thus, once the access was authorised, the Code does not account for the purpose for which the computer was accessed. However, mere unauthorised access to a computer system should be followed by 'infringement of security measures' for it to be specified as a crime. In other words, illegally accessing only those computer systems which are protected by security measures has been criminalised and therefore, access to non-protected systems does not lead to criminal liability. While, the element of bypassing security measures is not required for the criminalisation if it is not only mere access, but also there is an intent of obtaining computer data.[462] It does not matter whether access resulted in any damage in either case for an act to be acknowledged as a crime.

It can be suggested that the rationale behind narrowing the scope by including 'infringement of security measures' as a necessary element based on the assumption that if a security measure is not installed on a computer system, then

[461] ITU (n. 102), 195.
[462] Firudin Samandarov, *Commentary on the Criminal Code of the Republic of Azerbaijan, Second part (Azərbaycan Respublikası Cinayət Məcəlləsinin kommentariyası, İkinci hissə) (*Baku, Hüquq Yayın Evi, 2016) 876.

mere access without permission is not unacceptable. Because it is '…a computer system that permits free and open access by the public, such access is 'with the right'…', and consequently, there should be no criminalisation.[463] Thus, if a person 'merely accesses' a non-protected computer system which is situated in another country, regardless of whether it has been criminalised or not on that country, a person cannot be subjected to criminal responsibility due to the dual criminality approach adopted by the Criminal Code. Article 12 of the Criminal Code specifies that for the implementation of the criminal law concerning the persons who have committed a crime beyond the border of the Republic of Azerbaijan an action shall be regarded as a crime both in Azerbaijan and in the state where the act was committed.[464]

Article 271.1 also criminalises all acts involving unlawful access to a computer system or network with the purpose of obtaining computer data, or any other personal intentions. If a perpetrator intends to obtain computer data and thereby accesses, no matter whether infringing security measures or not, then he is held criminally liable. Then again, it might be challenging to subject the perpetrator to criminal responsibility in cases where security measures are not installed in a computer and there is not a trace of information obtained, as the intention would be hard to evidence without such a trace. Moreover, if the case involves the illegal acquisition of non-public computer data, it must be classified as 'Illegal acquisition of computer data', which is criminalised under Article 272.

The perpetrator of illegal access can be any mentally capable person without a right (whether legislative, administrative, executive, judicial, contractual or consensual) to access, who has reached the age of 16. A person without right is represented as a person, who is not a legal user, or his right to use is prohibited by law, or he is accessing without obtaining permission for use from the legal owner or authorised person.[465] Therefore, individuals, whose temporary or permanent official job is related to computer programming, checking security vulnerabilities, ensuring

[463] Council of Europe*, Explanatory Report to the Convention on Cybercrime (*2001), para. 47.
[464] Article 12, Criminal Code (1999).
[465] Firudin Samandarov (n. 462)*,* 874.

the normal work of computer systems, as well as system administrators, are not criminally liable if they act on a legal basis.

The mental element is clearly defined in the Criminal Code and is represented only in the form of direct intention. A person must understand and foresee that he is accessing without right and infringing security measures and desiring to do so. As the act does not necessitate the infliction of a socially dangerous result for being classified as a crime, there is not a possibility of illegally accessing with indirect intention.

ii. The applicable penalty for the criminal offence of illegal access to a computer system is either a fine up to two thousand AZN[466] or a deprivation of liberty for a term of up to two years with deprivation of the right to occupy certain positions or engage in certain activities for a period of up to two years, in the absence of aggravating circumstances.[467] From the Convention on Cybercrime perspective, it can be argued that since the infliction of damage is not a prerequisite for 'illegal access to a computer system', this punishment can be accepted as 'effective' and 'dissuasive'. However, its 'proportionality' is questionable, as there is not a material nature of damage that can assist in assessing the proportionality of counter-action in this case. From the perspective of the purposes of punishments determined by the Criminal Code, the punishment might provide for the restoration of social justice, and the prevention of the commission of a new crime, however, it can be argued that two years' imprisonment, in this case, seems excessive in reforming a convicted person. It has been argued that individuals involved in illegal access could be readily convinced to use their skills for good, rather than for criminal purposes.[468]

Two sets of aggravating circumstances are introduced for the requirement of aggravated penalties for crimes of illegal access to computer systems/data. Common aggravating circumstances, that are also contained in all articles of the 'Cybercrime' Chapter 30 (except in 'computer related forgery'), include: a) repeated

[466] The manat (code: AZN) is the currency of Azerbaijan. 1 AZN is currently equal to 0.42 GBP.
[467] Article 271.1, Criminal Code (1999).
[468] David S. Wall (n. 73).

commission;[469] b) commission by a group of persons or a group of persons by preliminary concert, by an organised group, or by a criminal community (criminal organisation);[470] c) commission by a person through misusing an official position. The commission of illegal access to the computer system with the presence of this set of aggravating circumstances shall be punishable by deprivation of liberty for a term of up to four years.[471] The second set of aggravated penalties is introduced for the commission of an act against computer system of 'infrastructure facility of public importance or any part thereof'.[472] The notion of 'infrastructure facility of public importance' was introduced to the Code after the harmonisation with the Convention, which establishes the grounds for the imposition of strictest punishment in case of being illegally accessed. Consequently, the most severe punishment applied for illegal access in the presence of this aggravating circumstance is a deprivation of liberty for a term of up to *six* years with deprivation of the right to occupy certain positions or engage in certain activities for a period of up to three years.[473] This punishment seems to be lenient in responding to cyber-attacks that can cause serious loss or disruption to the important information systems.

iii. The pre-harmonised Criminal Code stipulated liability for illegal access to legally protected information. The revised version focuses on protecting the whole or any part of a computer system against any access without a right committed by breaching security measures. Moreover, the revised version has also clarified the motive of illegal accessing, which can be the intent of obtaining computer data or other personal intent.

---

[469] Repetitiveness is manifested in the repeated (twice or more) comission of the same offence that is criminilized under the same article. See article 16, Criminal Code (1999).
[470] Which is a joint participation of two or more perpetrators. For further information see Article 34, Criminal Code (1999).
[471] See Article 271.2 of the previous version of the Criminal Code (1999).
[472] According to Article 271.3 of the Criminal Code (1999) 'Infrastructure facility of public importance' includes government institutions, enterprises, organizations, as well as non-governmental organizations (public unions and funds), credit organizations, insurance companies, investment funds of much importance for the state and society.
[473] Ibid, Article 271.3.

Another major difference is that definitions of 'computer system', 'computer data' and 'infrastructure object of public importance' have been introduced in the current version, which had not been previously defined in relevant Criminal Code articles.

iv. The text adopted by Article 271.1 of the Criminal Code is predominantly similar to those provisions contained in Article 2 of the Convention, subject to the exclusion of the element of committing act 'in relation to a computer system that is connected to another computer system'.[474] Exclusion of this element represents a wider approach that provides for the criminalisation of both physically accessing a stand-alone computer without any use of another computer and illegal access to networked computer systems.

II. Illegal interception/misappropriation of computer data

i. The harmonised version of the Criminal Code provides legal responses for illegal interception of computer data. Article 272.1 defines illegal interception of computer data as intentional acquisition without right, made by technical means, of non-public computer data transmitted to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.
It is important to highlight from the outset that the term, 'non-public', qualifies the nature of the data transmitted. Therefore, the primary object protected by this prohibition is the integrity of 'data' and 'electromagnetic emissions…carrying such computer data',[475] rather than the 'confidentiality of private communications'.[476] Therefore, it can be claimed that the parties who wish to communicate confidentially are not protected under the auspices of this Article 272.1 if the data communicated is publicly accessible information, which is defined by the Law on the Right to Access Information 2005 as 'the information to which the access is not

[474] See Article 2, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[475] Note: Illegal interception of electromagnetic emission is also specified as a crime due to the possibility of reconstruction of data from those emissions.
[476] Ian Walden, *Computer Crimes and Digital Investigations* (Oxford: Oxford University Press, 2007) 184.

limited due to the law'.[477] In order for the data to be considered as 'non-public', it should incorporate information regarding 'state, professional (lawyer, notary, doctor), service, bank, commercial, investigation and court secrets, information on personal and family life of individuals, or terrorist acts'.[478] Consequently, illegal interception of public computer data is excluded from the scope of criminalisation of this article. It can be argued that the concept of the Cybercrime Convention was not fully understood regarding the criminalisation of illegal interception.

However, illegal interception of public computer data can lead to criminal responsibility under Article 271.1 (Illegal access) as it criminalises illegal access to computer data as well. Although Chapter 30 of the Criminal Code does not explicitly criminalise the breach of confidentiality of communications, these acts are punishable under Article 155, which treats the violation of 'the secrecy of correspondence… or other messages of individuals' as a crime. In addition, Article 156 of the Criminal Code criminalises the violation of the confidentiality of personal data, dissemination of data about a person's personal and family life, and unlawful gathering of data.

Applicability of Article 272.1 is limited to interception, which is realised through 'technical means'. As a necessary element of the illegal interception offence, which serves as a restrictive condition for avoiding over-criminalisation, technical measures may include the use of a computer system, electronic eavesdropping, tapping or recording devices.[479]

In order for an offence to be determined as illegal interception under Article 272.1, it must also be committed 'intentionally' like all other offences defined by Chapter 30 of the Criminal Code. This act can only be committed in the form of direct wilfulness. As the act does not necessitate the presence of a socially dangerous

[477] Article 34, Law on the Right to Access Information 2005.
[478] Article 10, Law on Freedom of Information 1998.
[479] According to the Explanatory Report to the Convention on Cybercrime (2001), para. 53. 'Interception by "technical means" relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes.

result for being classified as a crime, there is not a possibility of illegally intercepting computer data with indirect wilfulness, which would seek for a person who knowingly allows socially dangerous consequences to take place in order for the act to be acknowledged as being commissioned. A person must understand and foresee that he is intercepting computer data and electromagnetic emissions without right and through the application of technical measures, and desires to do so.

The subject of this crime can be any mentally capable person 'without a right' to intercept computer data or electromagnetic emissions carrying such computer data, who has reached the age of 16 before committing this act. The Criminal Code does not provide the elaboration of actions that are regarded as committed 'without right'. The set of examples for interceptions that are carried out with right provided by Explanatory Report to the Convention on Cybercrime can guide against over-criminalisation. It identifies that the act is justified, for example, if the intercepting person has the right to do so; if he acts on the instructions or by authorisation of the participants of the transmission; or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities.[480]

ii. The applicable penalty for the criminal offence of Illegal interception of a computer data and two sets of aggravating circumstances that are introduced with the requirement of aggravated penalties for crimes of illegal interception are identical to the aggravating circumstances and penalties determined by Article 271 (illegal access).[481] It can be claimed that imposing identical punishments to these two distinct offences raises the question of effectiveness, proportionality and dissuasiveness of sanctions imposed. This is due to the reason that the main concern of 'illegal interception' is non-public computer data, while 'illegal access' protects the security (confidentiality, integrity and availability) of the computer system and public computer data stored in this computer system.

[480] *Explanatory Report to the Convention on Cybercrime* (2001) ETS No. 185, para. 58.
[481] See sub-section 4.3.2.1.

iii. The pre-harmonised version of the Criminal Code did not provide legal solutions for the criminal offence of illegal interception of a computer data.

iv. The notable disparity between the Azerbaijani position and the position of Convention on Cybercrime is that the Convention's provision aims at protecting the right of privacy of data communication and the term 'non-public' qualifies the nature of the transmission (communication) process.[482] By contrast, according to the Criminal Code, the term qualifies the nature of the data transmitted, which changes the object of protection and leaves the integrity and confidentiality of private communications open to abuse.

III. Illegal interference

i. Although the Criminal Code includes provisions dealing with the destruction of physical property in separate Articles,[483] those provisions are not extended to interference with computer data and systems possibly because of 'the intangible and rather volatile nature of computer data'.[484] Thus, illegal interference with computer data and computer system has been criminalised separately under Article 273 of the Criminal Code.

Separate provisions, under the same article, contain data interference and system interference. According to Article 273.1, when committed intentionally by a person without right, the act of damaging, deletion, deterioration, alteration or suppression of computer data, which results in significant damage, leads to criminal liability. Next, Article 273.2 provides that if a person without right intentionally hinders the functioning of a computer system on a serious scale through inputting, transmitting,

[482] See Article 3, Council of Europe Convention on Cybercrime (2001); see also *Explanatory Report to the Convention on Cybercrime* (2001) ETS No. 185, para 54.
[483] See for example, Article 186. Deliberate destruction or damage of property; Article 187. 'Destruction or damage of property on imprudence', The Criminal Code (1999).
[484] Ulrich Sieber, 'Mastering Complexity in the Global Cyberspace: The Harmonisation of Computer-related Criminal Law' in Delmas-Marty, Mireille, Mark Pieth, and Ulrich Sieber, *Les Chemins De L'harmonisation Pénale/ Harmonising Criminal Law* (Paris, France: Société de législation comparée, 2008) 127-202

damaging, deleting, deteriorating, altering or suppressing computer data, he/she is criminally responsible and therefore must be subjected to criminal punishment.[485]

Data integrity is protected in a broad sense by Article 273.1, which is concerned not only with damaging but also with deletion, deterioration, alteration or suppression of computer data. The integrity, availability and the proper functioning or use of stored computer data is the interest sought to be protected under this criminalisation provisions. The Code also attaches the harm/damage requirement as a necessary element, and it must be 'significant' in size for an act to be recognised as data interference. By 'significant harm', the Code means material damage at a rate of at least a thousand AZN or damaging the interests of the state, society or individuals on a significant scale.[486]

The normal functioning of the computer system is the main concern of the 'computer system interference'. Article 273.2 has also taken a narrower basis for criminalisation, by attaching the provisions of 'inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data' to system interference. Moreover, this criminal offence must be committed in a way which 'seriously hinders' the normal functioning of the system. Serious hindering of the work of the computer system is clarified by Article 273.2 to mean disruption of normal functioning of a computer system where neither the owner nor the user can use the system or exchange data with other computer systems.

Notably, legislators refrained from making specific references to Denial of Service (DoS), which involve sending malformed queries to a computer system or more e-mails to e-mail servers than the system can receive and handle,[487] or to Distributed Denial of Service (DDOS) attacks, which are conducted in a 'distributed' way by multiple systems simultaneously engaged in attack through usually entailing the help of so-called "botnets".[488] Botnets are established to remotely control a significant number of computers by infecting them with malicious software that can

[485] Article 273.1. Criminal Code (1999).
[486] See the 'Note' section, Article 273, The Criminal Code (1999).
[487] Council of Europe, Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #5 DDOS attacks* (9th Plenary of the T-CY, 2013).
[488] Robin Mansell, Peng Hwa Ang and Pieter Ballon (n. 112), 120.

be activated without the computer users' knowledge in order to launch a large-scale cyber-attack with the capacity to cause a major impact.[489] The criminalisation framework set out by Article 273 is broad enough to address both Denial of Service (DoS) attacks and Distributed Denial of Service (DDOS) attacks. Also, guidance notes on DDOS attacks and botnets issued by the Council of Europe Cybercrime Convention Committee can be used to facilitate the effective utilisation and implementation of the Convention, in line with the recent policy, legal and technological developments.[490]

Based on the text provided by Article 273.2, it can be claimed that computer system interference must be committed only through the manipulation of data to fall within the provision. Therefore, interference by other means, such as 'cutting the electricity supply',[491] or 'through a computer device that can initiate fire and damage the whole system'[492] should not be interpreted as being covered by Article 273.2. It is, therefore, possible that if significant damage is done as a result of acts, interference through any other measures that are also able to corrupt computer systems can be prosecuted under Article 186, which deals with deliberate destruction or damage of property, or Article 187, which is concerned with destruction or damage of property through reckless imprudence. This is due to the reason that falling within the scope of protection provided by Articles 186 or 187 leads to an overlap between those Articles and Article 273, whereas if those acts cannot be prosecuted under any Criminal Code Article then there is potential for attackers targeting computer systems being able to evade or escape criminal

[489] Section 5, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (NIS Directive).

[490] Council of Europe, Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #5 DDOS attacks* (Adopted by the 9th Plenary of the T-CY (4-5 June 2013)); Council of Europe, Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #2 Provisions of the Budapest Convention covering botnets* (Adopted by the 9th Plenary of the T-CY (4-5 June 2013))

[491] Article 7, The Commonwealth, Model Law on Computer and Computer Related Crime (LMM (02)17) (Oct. 2002).

[492] see: Max Smolaks, 'Data Center Fire Kills Internet In Azerbaijan', (*DatacenterDynamics,* 2015) http://www.datacenterdynamics.com/power-cooling/data-center-fire-kills-internet-in-azerbaijan/95227.fullarticle; 'MNS traces in the fire at Delta Telecom' ('Delta Telecom-dakı Yanğında MTN izi') (*Xəbərlər.az*, 2015) http://xeberler.az/new/details/delta-telecom-daki-yanginda-mtn-izi--13770.htm.

prosecution. Therefore, it is essential to provide a clearer line between relevant Criminal Code articles to avoid any possibility of overlap. One solution might be referring to Article 186 or 187 if damage arises not through the manipulation of data. Otherwise, Article 273.2 should be applied.

With regard to the electromagnetic interference to a computer system, however, it can be argued that the use of high-energy electromagnetic pulses (EMPs) to attack and manipulate, for example, clocks and therefore, time synchronization for consistent and accurate interaction between the networks, or to overload computer circuitry, which may cause serious disruption on computer systems, can be penalised under Article 273.[493]

Although elements, such as 'significant harm' and 'serious hindering of the functioning of a computer system' are explicitly defined, the Article does not provide the clarifications of different acts covered. In this sense, the Explanatory Report to the Convention on Cybercrimes can be helpful to illustrate the meaning of the acts. According to the Explanatory Report, 'damaging' and 'deteriorating' can be understood as a negative alteration (modification) of the integrity or the information content of data and programmes, while 'deletion' of data means the destruction and making them unrecognisable.[494] Moving a file to the recycle bin, for example, might not come within the confines of this provision, since the file is not deleted or erased from the hard disk, and can be easily restored.[495] Even a file deleted from the recycle bin can be recovered by using a variety of special software tools, such as Recuva, TotalRecovery, and CDRoller. Thus, such deletion might not necessarily result in significant damage or hinder the normal functioning of a computer system on a serious scale, and if this is the case, the application of

[493] Power plants, for example, are highly sophisticated, very high-speed machines, and improper shut down, which is reasonably possible with EMP attacks, can damage or destroy any of the many critical components and can even cause a catastrophic failure. See: John S. Foster, Jr., Earl Gjelde, William R. Graham, Robert J. Hermann, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (Washington, D.C.: EMP Commission, 2008) 43; see also Sumit Ghosh and Elliot Turrini, *Cybercrimes: A Multidisciplinary Analysis* (Springer Berlin 2014) 392; Gráinne Kirwan and Andrew Power, *Psychology of Cyber Crime* (IGI Global 2014) 192.
[494] *Explanatory Report to the Convention on Cybercrime* (2001), para. 61.
[495] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn. Academic Press 2011) 254.

the criminalisation provision could become impotent. In general, it will be challenging to substantiate this view with provisions of Article 273 of the Criminal Code, unless the clarification of acts is provided. 'Suppressing' computer data is explained to cover any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored.[496] 'Inputting' the computer data can be realised by using physical input interfaces to transfer information to the system (such as through USB ports, hard disk drive (HDD), or peripheral devices), whereas the remote input of data is also entailed for 'transmitting' data.[497] Given that malicious codes, such as viruses and Trojan horses, modify the data, their input is also criminalised under Article 273 of the Criminal Code.

Similar to other offences determined by Chapter 30 of the Criminal Code, Article 273 requires the offender to carry out offences intentionally. So, intent to interfere with computer data and system should be proven. However, the mental elements of illegal interference with computer data and computer systems exhibit slight differences from each other. System interference can be committed only with direct intention, as the offender has to comprehend that he/she acts without right and hinders the functioning of a computer system on a serious scale, and foresee and desires the harm to occur. However, data interference can be committed both in the forms of direct and indirect wilfulness. This is due to the reason that regardless of the presence of the desire to cause significant harm, if a person knowingly allows significant harm to take place by interfering with computer data, then the act can be regarded as being commissioned. This approach has created a broader basis of criminalisation, which is a reasonable extension in the light of the fact that computer data are intangible and volatile, and therefore, more vulnerable to be easily changed or deleted accidentally than physical objects.[498]

---

[496] see *Explanatory Report to the Convention on Cybercrime* (2001), para. 61.

[497] ITU (n. 102), 203; see also, Firudin Samandarov (n. 462), 882. Besides covering the use of wireless or cable networks, Bluetooth, infrared, this approach assists to criminalise the transmission of data via the Internet channels as well.

[498] Paul De Hert, Gloria González Fuster and Bert-Jaap Koops (n. 434), 508.

The acts of computer data and computer system interference must be carried out 'without right' by a person who has reached the statutory minimum age of 16 before committing these acts. Activities necessary for designing networks or common operational or commercial practices are not considered those 'without right'.[499] Therefore, if authorised by its owner or operator, for example, computer reprogramming or reconfiguration of operating systems, checking security vulnerabilities that result in significant harm cannot be admitted as a crime according to Article 273.[500]

ii. The applicable penalty for the criminal offence of illegal interference of computer data and systems, and the two sets of aggravating circumstances, which are introduced with the requirement of aggravated penalties for crimes of illegal interference, are identical to aggravating circumstances and the strictest penalties determined for the previous two Articles discussed above.[501] Imposition of identical punishments for acts differing from each other by the inclusion of harm as a necessary element can be considered neither proportionate nor dissuasive.

iii. The pre-harmonised version of the Criminal Code protected the integrity and availability of only computer data, while the current Code provides legal solutions for ensuring the normal functioning of the computer system as well. The strictest applicable penalty for the criminal offence of illegal interference of computer data was a deprivation of liberty for a term of up to one year, in the absence of aggravating circumstances. Only one set of aggravating circumstances with the requirement of aggravated penalties for crimes of illegal interference was introduced: a) commission by a group of persons or a group of persons by preliminary concert, b) commission by a person through misusing an official position or by a person with the right to access the computers, their systems or networks. c) by causing serious damage. The commission of illegal interference

[499] Council of Europe*, Explanatory Report to the Convention on Cybercrime* (2001), para. 68.
[500] See for further information, Ibid, para. 62 and 68.
[501] See Article 271 and Article 272. Criminal Code (1999).

with the presence of this set of aggravating circumstances was punishable by deprivation of liberty for a term of up to three years.[502]

iv. The provisions of criminalisation of illegal computer data and system interference determined by the Code are predominantly identical to those specified by the Convention on Cybercrime.[503] In accordance with Article 42 and Article 4, paragraph 2, of the Convention, Azerbaijan reserved the right to require that the conduct described in Article 4, paragraph 1 of the Convention result in significant harm.

IV. Misuse of devices

i. Commission of the criminal acts discussed above requires high levels of technical sophistication and expertise. Due to the rapidly growing need for software and hardware tools for the realisation of malicious acts, 'dark markets' for those tools started to develop.[504] Consequently, besides viruses, worms and Trojans, the market now provides with exploit codes for capitalising software vulnerabilities, packing programs for complicating malware analysis, and kits that assist non-technical criminals in building their malware.[505]

To suppress the distribution of computer misuse tools and protect the confidentiality, integrity and availability of computer systems and data, an independent criminal offence is established by the Criminal Code, which acknowledges the intentional commission of specific illegal acts related to the misuse of computer tools as a crime. According to Article 273-1, it is a crime to possess, produce, sell, procure for use, import, distribute or otherwise make available computing devices, programmes, passwords, access codes, or similar data for committing crimes stipulated for in the Articles 271-273 of the Code.

---

[502] Article 271, Criminal Code (1999), The pre-harmonised version of the Code is available at http://e-qanun.az/code/11#

[503] See Article 3 and 4 of the Convention on Cybercrime (2001).

[504] Lillian Ablon and Martin Libicki, 'Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data', (2015) 82 Defense Counsel Journal, 143-152.

[505] Science & Technology Committee, *Malware and cyber crime* (House of Commons London: The Stationery Office Limited 2011) Ev w8, http://www.publications.parliament.uk/pa/cm201012/cmselect/cmsctech/1537/1537vw.pdf

However, for these acts to be specified as ‘turnover of facilities and tools produced for cybercrimes’, there are certain requirements to be satisfied determined by Article 273-1.

In this way, the misuse of two types of computer tools, software and devices and passwords and codes, which enable access to computer systems and data have been criminalised under three sets of acts by Article 273-1:

1) production, sale, possession, procurement for use, import, distribution or otherwise making available of computer devices or programmes, the main purpose of which is making or adaptation for committing crimes stipulated for in the Articles 271-273 of the Code;[506]
2) production, procurement for use, possession of computer passwords, access codes, or similar data by which the whole or any part of a computer system is capable of being accessed;[507]
3) sale, distribution, or otherwise making available of computer passwords, access codes, or similar data by which the whole or any part of a computer system is capable of being accessed;[508]

The first two sets of acts need to be followed by the infliction of a ‘significant harm’ in order to be treated as a crime, while the third set of acts can be committed without the formal presence of any material damage. This is due to the reason that the sale, distribution, or otherwise making available of computer passwords, access codes, or similar data for committing an offence is considered dangerous for the public, even without the presence of any significant harm.[509]

The Code has not provided clarification of the meanings of acts covered under Article 273-1 related to computer misuse tools (such as 'producing', 'procuring for use', 'possessing', 'selling', 'importing', 'distributing', or 'making available'). Only the meanings of ‘distribution’ and ‘making available’ have been explained by the Explanatory Report to the Convention on Cybercrime. ‘Distribution’ refers to the

[506] Article 273-1.1 Criminal Code (1999).
[507] Ibid.
[508] Ibid.
[509] See also, Reservations and Declarations for Treaty No.185 - Convention on Cybercrime, Azerbaijan.http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=fFbBOuRj.

active act of forwarding data to others, while 'making available' means the placing online devices for the use of others.[510]

The criminalisation approach adopted by this Article is narrow, as it requires the computer tools to be misused only for committing the offences established in Articles 271 through 273. In addition, the purpose of the tool is another significant characteristic of the offence, especially attached as a requirement by Article 273.1.1. It is mainly concerned with the turnover of computer devices or programmes, 'the main purpose of which is making or adaptation for committing crimes stipulated for in the Articles 271-273 of the Code'. The inclusion of a 'specific intent' for the purposes of an offence has a role in preventing over-criminalisation of unknowing possession, or possession with legitimate intent.[511] At the same time, dual-use devices are excluded due to the limitation imposed by this narrow approach.[512] Thus, misusing computer tools, for example, for the production, distribution, or possession of (child) pornography, for espionage, for inciting racial, national, religious hatred, or for supporting and financing terrorism does not create grounds for criminal liability under this Article, despite all of these acts being crimes elsewhere under the Criminal Code.

Notwithstanding the misuse of computer tools for the commission of these acts can be interpreted as 'preparation' for and 'attempt' of a criminal offence,[513] it would be extremely difficult to prove the objective of misusing tools in such criminal proceedings.[514]

Article 273-1 requires the offender to carry out the offences intentionally, as all other crimes stipulated for in Chapter 30. However, besides the general intent, the specific intent must be present for the offence, which requires the purpose of committing the offences established in Articles 271 through 273. Thus, the element of intent in relation to any of the acts listed in Article 273 must be proven.

---

[510] See *Explanatory Report to the Convention on Cybercrime* (2001), para. 72.
[511] Ibid. para. 76.
[512] Ibid. para. 73.
[513] See for further information, Article 28; Article 29, Criminal Code (1999); However, it should be stressed out that, according to Article 28, criminal liability shall ensue for preparations to commit only grave or especially grave crime.
[514] *Explanatory Report to the Convention on Cybercrime* (2001), para. 73.

ii. Compared to the offences previously discussed, only one set of aggravating circumstances is introduced with the requirement of aggravated penalties for crimes of misuse of computer tools. However, aggravating circumstances and the strictest penalties determined by this Article are identical to those determined by the previous three Articles elaborated. The imposition of equally severe punishments regardless of the presence of harm element is also present in this article.

iii. The pre-harmonised version of the Criminal Code also contained provisions criminalising the creation, use, and dissemination of malicious computer programs. However, only the creation, use, and dissemination of malicious computer programs that serve for the introduction of changes to existing programmes, and knowingly leads to the unsanctioned destruction, blocking, modification, or copying of information, the disruption of the work of computers, computer systems, or their networks were criminalised under Article 272. Only aggravating circumstance with the requirement of aggravated penalty for crimes of misuse of programs was causing grave consequences through negligence, which was punishable by deprivation of liberty for a term of two to five years. The absence of this aggravating circumstance resulted in a deprivation of liberty for a maximum period of two years.

iv. Azerbaijan made two reservations when adopting the provisions about the misuse of devices determined by the Convention on Cybercrime.[515] Both reservations are concerned with acts, which are not considered dangerous crimes for the public. It was declared that given acts would be subjected to criminal charge only at the event of incurrence of significant harm. Otherwise, the provisions of criminalisation of misuse of tools determined by the Code are predominantly identical to those specified by Article 6 of the Convention on Cybercrime.

[515] See for the full list of reservations and declarations for Council of Europe Convention on Cybercrime (2001) http://www.coe.int/en/web/conventions/full-list//conventions/treaty/185/declarations?p_auth=5cnvNMaf

V. Conclusion

The revised version of the Criminal Code (1999) provides appropriate legal solutions for the majority of computer integrity crimes established in accordance with Articles 2 through 7 of the Council of Europe Convention on Cybercrime. The provisions of criminalisation of computer integrity crimes determined by the Code are, thus, largely identical to those specified by the Convention. The major disparity between the Code and the Convention appears to be the criminalization provisions of the Code on illegal interception, as the object of protection is not the privacy of communication given that the term 'non-public' does not qualify the nature of the transmission (communication) process, but the nature of the data transmitted.

The legislator has expanded the object of protection by including broader criminalization provisions compared to the previous version of the Code. In addition, the revised version of the Code has also clarified the motives of different computer integrity crimes to some extent and introduced definitions of 'computer system', 'computer data' and 'infrastructure object of public importance'.

Regarding sanctions, it can be argued that the approach adopted throughout the Code is inappropriate as it determines identical punishments for distinct offences with different elements, which raises the question of effectiveness, proportionality and dissuasiveness of sanctions imposed.

4.3.2.2. Computer-assisted crimes

I. Computer related forgery

i. In the second and third chapters of this thesis, it was stated that Azerbaijan, is a country that promotes the e-governance, has established a legal background for the use of digital documents to simplify the documentation procedure and increase the efficiency of government services.[516] According to the Law on Electronic Signature and Electronic Documents 2005, e-signature and e-documents can be

[516] See Chapter 2, Section 2.3.; Chapter 3, Section 3.2.

used in ‘all fields of activity where corresponding means are applied’.[517] The Law further encourages the application of electronic documents for official and unofficial correspondences, exchange of documents and information causing legal responsibility and liabilities.[518] Given that the digitisation rapidly changes the situation by moving the documentation processes from the offline environment to cyberspace, this trend is likely to be accompanied with a shift from the traditional forgery of tangible documents as well. Thus, it can be predicted that following the rapid digitisation processes, the number of computer related forgery cases, which involves intentional acts of generating or altering of stored data so that they acquire a different evidentiary value in the course of legal transactions without the consent of the owner,[519] will increase. Multiplication of the number of forgery cases in the online environment can also be expected due to the ease of use and accessibility of specialised computer applications and programs.

Computer-related forgery is criminalised under Article 273-2, which determines that when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data with the intent that it be used or acted upon as if it is authentic computer data, which results in disruption of the authenticity of original computer data shall be subjected to criminal liability. In comparison to the forgery of official documents, computer-related forgery has a broader scope focusing on the protection of security and reliability of ‘computer data’ and incorporates ‘any representation of facts, information, programs or concepts’,[520] irrespective of whether the data is official or unofficial, or directly readable or intangible.

The Code does not specify the acts covered by Article 273-2 regarding the computer-related forgery (such as input, alteration, deletion, or suppression of computer data). Clarifications of these acts provided by the Explanatory Report to the Convention on Cybercrime might be used for further interpretation, since Azerbaijan has made no reservations regarding the provisions of computer-related

[517] Article 2, Law on Electronic Signature and Electronic Documents (2005), 602-IIQ; According to the Development Concept ‘Azerbaijan – 2020: The Vision of the Future’ (2012), 100% application of e-government services is in the spotlight.
[518] Ibid.
[519] *Explanatory Report to the Convention on Cybercrime* (2001), para. 81.
[520] Article 271, Criminal Code (1999).

forgery determined by the Convention on Cybercrime. According to the Explanatory Report, unauthorised 'input' means the making of a false document, while subsequent alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond to the falsification of a genuine document.[521] So, the falsification of a genuine document by illegally inputting correct or incorrect data is the common element of these acts.[522]

It is also noticeable that computer-related forgery, as provided by the Code, can result in criminal liability only if the input, alteration, deletion, or suppression of computer data has resulted in inauthentic computer data. In other words, criminal liability is not attached unless the harmful result - disruption of the authenticity of original computer data - is established. Besides, the element of intent in relation to any of the acts discussed above must be proven. In practice it might be challenging to prove the true intention behind the act, given that computer-related forgery can be committed only with direct intention, which requires the offender to comprehend that the person has acted without right and intended to use the data as if they were authentic, as well as foreseen and desired harmful results.

Further, in order for an act to be prosecuted under Article 273-2, it must be committed by a person without right. More precisely, the subject of this act is any mentally capable person who does not have a right to input, alter, suppress or delete the concerning computer data.

ii. Article 273-2 specifies that the acts of computer-related forgery shall be punished either by a fine or by imprisonment for the term of up to 2 years with deprivation of the right to hold certain positions or engage in certain types of activities for a term of up to 3 years.

Compared to the previously discussed articles, no set of aggravating circumstances with the requirement of aggravated penalties for crimes of computer

[521] *Explanatory Report to the Convention on Cybercrim*e (2001), para 83.

[522] Lorenzo Picotti, Ivan Salvadori, *National legislation implementing the Convention on Cybercrime - Comparative analysis and good practices (*Council of Europe, Project on Cybercrime, Discussion Paper*,* 2008) 25.

related forgery is introduced by Article 273-2. On the one hand, even though aggravating factors are not explicitly implied by the Article, the presence of aggravating factors in criminal cases allows courts to impose a stricter penalty provided for the crime.[523] A 'deprivation of liberty for the term of up to 2 years' period' is the strictest punishment set for the crime of computer-related forgery. Although, the crime of computer-related forgery is also focused on the security and integrity of 'computer data', like the majority of other offences included in Chapter 30, the maximum period of deprivation of liberty determined for this crime in the presence of aggravating circumstances appears lenient compared to the penalties allotted to other cybercrime offences with same aggravating factors.[524]

It is also true that the severity of sanctions introduced for 'computer-related forgery' is equal to that set for Article 320, which criminalises the forgery, illegal preparation, sale or use of forged official documents.[525] However, it is important to consider the scale and quantity of vulnerable objects that can be easily multiplied by a single offender in the online environment with a range that could not be otherwise possible in the physical space.[526] Therefore, providing equally severe criminal sanctions in both cases regardless of their seriousness raises the 'effectiveness' and 'proportionality' questions.

iii. Certain interests are subject to protection against falsification and forgery under Article 320 of the Criminal Code, which had criminalised the forgery of official documents before the harmonisation.[527] However, it is not clear from the disposition of the Article 320, whether the notion of 'document' can be extended to cover digital documents, signatures and data, whereas, the Criminal Procedure Code considers the 'document' as 'paper, electronic and other materials bearing information in the form of letters, numbers, graphics or other signs'.[528] Thus, if applied by analogy, the 'documents' protected under Article 320 can cover digitised

[523] See Article 61.2 of the Criminal Code (1999) for the full list of aggravating circumstances.
[524] See Ibid. Article 273.3.
[525] The strictest punishment is deprivation of a liberty for the term of up to two years in both cases.
[526] See Section 2.4, Chapter 2 for more discussion.
[527] See Article 320, Criminal Code (1999).
[528] See Article 135, Criminal Procedure Code (2000).

versions of documents as well. Notwithstanding, a parallel offence to the forgery of documents has been created by adding new cyber-specific forgery provisions to Chapter 30 of the Criminal Code. Although legislators' discussions about the necessity of including it as a separate offence are not available, its inclusion can be accepted as an acknowledgement of insufficiency of protection of certain legal interests 'against new forms of interference and attacks'.[529]

iv. The provisions of criminalisation of computer-related forgery determined by Article 273-2 are mostly compatible with those provided by the Convention on Cybercrime (Article 7). However, the term, 'for legal purposes', which also refers to legal transactions and documents that are legally relevant,[530] is not included in Article 273-1. A broader criminalisation approach has been adopted by Azerbaijan, which does not tighten the scope of its protection by only covering the security and reliability of electronic data, 'which may have consequences for legal relations'.[531]

II. Computer-related fraud

i. As an assimilative offence tailoring traditional fraud offences to cyberspace, the offence of computer-related fraud is often not criminalised separately but is rather a legal construct, with the elements of ICTs being integrated into the core charges of fraud.[532] Unlike computer-related forgery, which has been created as a parallel offence to traditional forgery, a parallel cyber-specific fraud offence has, thus, not been introduced in Azerbaijan.

Article 8 of the Convention on Cybercrime describes 'computer-related fraud' as an 'intentional causing of a loss of property to another person by [interfering with computer data and or a computer system] with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or another person'. This

[529] *Explanatory Report to the Convention on Cybercrime* (2001), para. 80.
[530] Ibid, para. 84.
[531] Ibid, para. 81.
[532] United Nations Office on Drugs and Crime (UNODC), *Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies* (UNODC, Vienna, Austria, 2014) 84.

Article is aimed at criminalising any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property.[533]

It can be suggested that the 'computer-related fraud', introduced by the Convention on Cybercrime,[534] might be considered to fall within the scope of traditional fraud provisions determined by the Criminal Code (1999) and can be prosecuted under a combination of general 'fraud (swindle)' (Article 178) and 'illegal interference' (Article 273) provisions. This is due to the reason that the Convention on Cybercrime criminalises computer fraud manipulations if those manipulations have caused a direct economic or possessory loss of another person's property and the offender's intention behind the manipulations was procuring an unlawful economic gain for himself or for another person.[535] In turn, Article 178 of the Criminal Code specifies 'fraud' as an act of 'maintaining a property or property rights belonging to another person by deceit or breach of trust/confidence'. Consequently, computer fraud manipulations or any 'input, alteration, deletion or suppression of computer data [or] …any interference with the functioning of a computer system'[536] resulting in a 'loss of property' with the intention of procuring an unlawful economic gain will combine the provisions of two offences (Article 178 – Fraud, and Article 273 - Illegal interference).

The criminalisation of this offence is important, because fraud is the second most commonly occurring crime in Azerbaijan, and the annual number of recorded fraud cases has almost quadrupled throughout the last ten years (2007-2017).[537] Also, as discussed in Chapter 2, carding/phishing and other social engineering activities, have been identified by the interviewees among the highly concerning cybercriminal activities that require proportional attention.[538] Since statistical data providing what proportion of it is computer-related fraud is not currently available, it

[533] *Explanatory Report to the Convention on Cybercrime* (2001), para. 86.
[534] Article 8, Convention on Cybercrime (2001).
[535] It has also been clarified by the Explanatory Report that the term 'loss of property' is a broad notion, which incorporates loss of money, tangibles and intangibles with an economic value.
[536] Article 8, Convention on Cybercrime (2001).
[537] According to the crime statistics provided by the State Statistical Committee, in 2007, the annual number of recorded fraud cases was 1223, while 4887 fraud cases were recorded in 2017 (and 4373 in 2016). Available online at https://www.stat.gov.az/source/crimes/;statistics for 2017 available at http://www.mia.gov.az/index.php?/az/content/29958/.
[538] See Chapter 2.4.

is difficult to spot a clear correlation between the rapidly rising numbers of fraud cases and increasing numbers of Internet users during the past 10 years in Azerbaijan. However, between 1999 and 2005 the annual number of recorded fraud cases decreased, whereas, interestingly, starting from 2005 until 2017 the number of both fraud cases and the percentage of the Internet users almost quintupled.[539] Thus, the existence of a correlation between these two variables seems a tenable assumption.

ii. Given the escalating risk and the number of recorded fraud, phishing and other related offences committed through techniques of social engineering during the previous ten years, the rationale for setting stricter penalties could provide a good deterrent in the fight against fraud, which also involves cyber-specific elements. Indeed, compared to sanctions imposed over other offences included in Chapter 30 (Cybercrimes) of the Criminal Code, perpetrators of computer-related fraud are subjected to stricter penalties due to the accumulation of sanctions provided by the combination of two offences (fraud and illegal interference).

iii. The pre-harmonised Criminal Code did not contain provisions on cyber-specific fraud. However, an act of computer-related fraud determined by the Convention on Cybercrime might combine the provisions of 'Fraud' (Article 178) and 'Illegal access to computer information' (Article 271).

iv. Compared to the previously elaborated offences mirroring the provisions of relevant Articles introduced by the Convention on Cybercrime, computer-related fraud provisions stipulated by Article 8 of the Convention are not contained in a separate Article under Chapter 30. However, measures and provisions as may be necessary to establish computer-related fraud as a criminal offence have been adopted under national law, and the traditional elements of fraud are still valid to deal with computer-related fraud.

[539] The number of fraud cases increased from 933 to 4887; and the percentage of Internet users rose from 16 to 78% between 2005-2017. See Figure 2.1. Percentage of internet users between 2005 and 2017.

III. Identity theft

Rapid digitization and global-connectivity have led the increasing significance and wide use of identity-related information in the economy and social interaction during the last decade. Although identity 'theft' existed well before the Internet, its growth has accelerated in the Internet era.[540] The more the areas of daily and social life move into online environment, the more identity-related information is processed and stored in databases and thus, become a potential target for offenders.[541] In addition, besides traditional categories of identity-related data targeted by offenders, such as passport information, driving licences, birth certificates, financial account information and credit card numbers, new categories of identity-related information have been added to the list as a consequence of the digitisation, such as account information and passwords, e-mail addresses and IP-addresses.[542]

It is worth recalling that the internet penetration rate in Azerbaijan has already exceeded 78% and the government is working towards ensuring 100% accessibility of all governmental services through online channels. The importance of identity in the online world grows even further due to this development, and so is the fact that even more identity-related information becomes vulnerable to identity theft.

A generally accepted definition of the term 'identity theft' is absent. There is no single definition of identity theft; with the terms 'identity crime', 'identity fraud' and 'identity theft' often being used interchangeably.[543] The Cybercrime Convention Committee describes identity theft as commonly involving criminal acts of fraudulently obtaining and using another person's identity information.[544] As a precursor to identity fraud, identity theft describes the stage at which criminals

[540] Bert-Jaap Koops et al., 'A Typology of Identity-Related Crime' (2009) 12 *Information, Communication & Society*, 1.
[541] Marco Gercke, 'Legal Approaches to Criminalise Identity Theft' in UNODC, *Handbook on Identity- related Crime* (United Nations, 2011) 12.
[542] Ibid, 13-15.
[543] Kristin M. Finklea, *Identity theft: Trends and issues* (CRS Report for congress, DIANE Publishing, 2010) 2.
[544] Cybercrime Convention Committee (T-CY), T-CY Guidance Note #4 Identity theft and phishing in relation to fraud (Adopted by the 9th Plenary of the T-CY (June 2013)) 3.

obtain personal information from victims.[545] It can both facilitate and be facilitated by other crimes.[546] It may be committed by the aid of psychological means (social engineering) and through technological means (trashing, phishing, pharming, smishing, vishing, a man in the middle attacks), and the intervention of botnets and surveillance software.[547] Identity theft may also assist the commission of further crimes such as bank fraud, document fraud, or immigration fraud.[548]

The Criminal Code has not introduced a single definition of identity theft or a separate cyber-offence of the unlawful use of identity-related data. Since a single-provision approach to the criminalisation of this wrongdoing is not provided, it is conducive to review the approach adopted by Azerbaijan through considering three phases of the condemned behaviour: obtaining through transfer; possessing; and using the identity-related information for criminal purposes.[549] The full criminalisation of identity theft requires the coverage of all three phases.[550]

As previously stated, the commission of identity theft necessitates the obtaining of identity-related information. Therefore, it can be suggested that criminalisation of the 'transfer' of the means of identification with the intent to commit an offence covers the acts related to phase 1 in a very broad way.[551] The Criminal Code contains a number of provisions which criminalise identity-theft acts in this phase, such as 'Illegal access' (Article 271), 'Illegal interception' (Article 272), 'Illegal interference' (Article 273) and 'Computer-related forgery' (Article 273-2). However, these provisions do not cover all possible acts in this phase.

The criminalisation of possession of the identity-related information in order to use them for criminal purposes again reflects a broad approach regarding the range of

[545] David S. Wall, 'Policing identity crimes' (2013) 23 *Policing and Society*, 439.
[546] Kristin M. Finklea (n. 543).
[547] See for further information David S. Wall (n. 545). See also, Nicole Van der Meulen, and Bert-Jaap Koops, 'The Challenge of Identity Theft in Multi-Level Governance' in Rianne Letschert, Jan van Dijk, *The New Faces of Victimhood* (Springer 2011), 159-190.
[548] Kristin M. Finklea (n. 543).
[549] Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #4 Identity theft and phishing in relation to fraud* (Adopted by the 9th Plenary of the T-CY (June 2013)) 4.
[550] See for further information, Marco Gercke, *Project on cybercrime: Internet-related identity theft* (Discussion paper Economic Crime Division Directorate General of Human Rights and Legal Affairs, 2007) 20-29.
[551] Ibid, 21.

acts criminalised. However, provisions regarding the mental element that is the intention of possessing information for using them later for criminal purposes can be considered as a confining element. In other words, if that intention is not present, then the provisions of criminalisation do not fully apply.

The provisions provided by Chapter 30 of the Code, therefore, can hardly cover most acts in this phase, except the provisions of Article 273-1 (Misuse of Devices). This is due to the reason that the offences contained in Chapter 30 do not attach the intention of using obtained data later for other criminal purposes. While, 'misuse of device' can be applied in a limited way for the acts of this phase, because Article 273-1 attaches the specific intent that it be used for committing any of the offences established in Article 271 through 273. More precisely, possession of computer passwords, access codes, or similar data must be coupled with the intent of committing only the offences of Article 271-273. Therefore, sale, procurement for use or distribution of identity-related information for any other purposes cannot be covered by Article 273-1. In addition, the provisions of 'misuse of devices' are applied only to that identity-related information which is in the form of passwords and access codes.

The third phase is characterised by the use of identity-related information to commit further criminal offences. For example, 'Forgery of official documents' (Article 320), 'Computer-related forgery' (Article 273-2), 'Illegal acquisition and disclosure of a commercial or bank secret' (Article 202), as well as 'Fraud' (178) and 'Theft' (Article 177) can be committed by the perpetrator through the application of identity-related information. In addition, the application of digitised identity-related information for the commission of theft can be considered as an aggravating circumstance according to Article 177.2.3-1, which determines that application of electronic data devices and information technologies for theft is punishable with a deprivation of liberty for a term of up to seven years.[552]

[552] See also, the Decision of the Plenum of the Constitutional Court of the Republic of Azerbaijan) on Interpretation of Article 177.2.3-1 of the Criminal Code of the Republic of Azerbaijan (22 June 2015), online available at http://www.constcourt.gov.az/decisions/334. The Court made a decision that the theft committed through the use of a payment (bank) card shall also be interpreted as

To conclude, although the Criminal Code does protect certain legal interests which can be attacked through the misuse of identity-related information, identity theft, is not criminalised as a separate offence. Notwithstanding that different articles of the Criminal Code might apply to some identity theft offences, the problem should be revisited with the aim of providing specific legal solutions for the offence of identity theft. Prosecuting these offences under the Criminal Code might prove difficult, in particular, in the face of technological advancement and because of imperfect knowledge about how technology would impact on crime when these laws were enacted.[553] Specific provisions focused on protecting identity-related information, which could be committed independently of other computer-related offences, should be adopted to achieve more coordinated and integrated responses against cybercrime.

IV. Offences related to infringements of copyright and related rights

i. The onset of digitisation and the Internet, the spread of broadband and social networking has marked a turning point in reproduction and distribution of digitised content, infringements of intellectual property right, in particular of copyright and other adjacent rights, have become the most commonly committed offences on the Internet.[554] The situation in Azerbaijan regarding the protection of IP rights both online and offline cannot be regarded as being satisfactory, as intellectual property related to copyright and trademarks are widely exploited by counterfeiters.[555] According to the International Property Rights Index 2017, Azerbaijan was in 115th place among 127 countries for the overall 'protection of intellectual property rights', while for 'copyright protection' the country was ranked 96th (among 105

commission of a crime qualified under Article 177.2.3-1, since this card reflect the information about the individual and his/her bank account details and therefore, the card must be considered as an 'electronic data carrier'.

[553] Bert-Jaap Koops et al. (n. 540), 1-24.

[554] *Explanatory Report to the Convention on Cybercrime* (ETS No. 185) 2001, para. 68; See also, Ruth Towse, 'The Quest for Evidence on the Economic Effects of Copyright Law' (2013) 37 *Cambridge Journal of Economics,* 1187-1202.

[555] See for example: 'Azerbaijan IP Investigation | Copyright Patent Infringement' (*IP Investigator*, 2016) http://www.iprightsinvestigators.com/azerbaijan-ip-investigation.php.

countries).[556] In addition, the BSA Global Software Survey 2016 indicated that software piracy rate remains high in Azerbaijan, claiming that 84 percent of software was installed without proper licensing.[557] The Copyright Agency of the Republic of Azerbaijan also confirmed the presence of high levels of piracy in the country by stating that currently, the piracy level at the book publishing market makes up 28 per cent, while the figure on audio and video products is 65 per cent, and in the software market is 75 per cent.[558] Thus, copyright violations, as well as online piracy remains rampant in Azerbaijan.

Azerbaijan was one of the first post-Soviet countries, which established a legal framework for ensuring the protection of copyright and adjacent rights by adopting the Law on Copyright and Related Rights in 1996.[559] Moreover, it is a member of the World Intellectual Property Organization (WIPO) and has become a contracting party to all of the treaties that article 10 (Offences related to infringements of copyright and related rights) of the Convention on Cybercrime concerned, except the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).[560] Since Azerbaijan is not yet a member of the World Trade Organisation, bringing in line the country's IP laws together with their enforcement mechanisms with the requirements of the TRIPS Agreement is also the prerequisite for becoming a member of the WTO.[561]

Adoption of the Law on Copyright and Related Rights in 1996 was further followed by the criminalisation of infringement of protected copyright and other related rights.[562] The protection of intellectual property rights from criminal encroachments comes under the realm of the traditional criminal laws of copyright and related rights. So, no separate cyber-specific provisions are set forth by the Criminal Code

[556] Property Rights Alliance, *International Property Rights Index 2017*, see for the country profile https://internationalpropertyrightsindex.org/country/azerbaijan.
[557] The Software Aliance, *The Compliance Gap: BSA Global Software Survey 2016,* http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_InBrief_A4.pdf.
[558] How Copyright Infringements are Punished in Azerbaijan' ('Azərbaycanda piratçılıq edənlər necə cəzalandırılır.') (*Copag.gov.az*, 2018) http://copag.gov.az/copag/az/content/news/972.
[559] Law on Copyright and Related Rights 1996, № 115-IQ.
[560] See for the full list of WIPO-administered treaties, which Azerbaijan is a contracting party: http://www.wipo.int/treaties/en/ShowResults.jsp?country_id=11C.
[561] See 'WTO | Accession Status: Azerbaijan', (Wto.org, 2016) https://www.wto.org/english/thewto_e/acc_e/a1_azerbaidjan_e.htm.
[562] Law on Copyright and Related Rights 1996, № 115-IQ.

to this end. Article 165 of the Criminal Code provides that when significant damage is caused by the illegal use of objects of copyright or related rights, that is the publication of other person's scientific, literary, art or other piece by misappropriation of authorship, or misappropriation of copyright in other ways, the illegal reproduction or distribution of such property shall be punishable by fine or by corrective labour for up to 480 hours. In this way, protection of copyright and related rights has been criminalised as general offences rather than cyber-specific crimes. However, the provisions of Article 165 can be interpreted to cover online infringements as well.

The acts to be criminalised are specified by Article 165. The Law on Copyright and Related Rights 1996 provides that 'publication' means the circulation of copies of a work or phonogram with the consent of the author of work or phonogram producer for meeting the needs of public, and further stipulates that providing an opportunity to use work and phonogram via electronic-information system tools shall also be considered publication.[563] Thus, it can be agreed that publication without the consent of the author can be acknowledged as 'illegal', and the Criminal Code (1999) does not limit criminalisation to acts committed only by means of a computer system. The Law (1996) also clarifies that distribution of works and related rights objects' is understood as making the original or copies of a work or an object of related rights available to the public by sale or other transfer of ownership.

Article 165 of the Criminal Code is linked to the protection of copyright and adjacent right, and pursuant to the Law on Copyright and Related Rights 1996 copyright extends to both disclosed and undisclosed scientific, literary and artistic works existing in objective form and are results of creative activity irrespective of purpose, value and content, also expression form and method.[564] The subject matter of related rights are performances, phonograms, and broadcast programs.[565] However, ideas, processes, methods or mathematical concepts do not fall under the protection of Article 165, due to the reason that copyright

[563] Ibid, Article 4.
[564] Ibid, Article 6.
[565] Ibid.

protection is granted only to the form of expression of a work pursuant to the Law on Copyright and Related Rights 1996.[566] In addition to offences related to infringements of copyright and related rights, the Criminal Code also criminalises 'infringement of the exclusive right to use Topographies of Integrated Circuits' (Article 165-1),[567] 'violation of requirements on use of folklore expressions' (Article 165-2),[568] as well as the 'illegal use of compilations of data' (Article 165-3).[569]

For all copyright offences, criminal sanctions only come into play where the infringement resulted in damage on a 'large scale'. Notwithstanding that Article 165 does not clarify what is meant by this level, pursuant to Article 165-1,165-2 and 165-3, damage is considered to be 'large scale' if it is caused at a rate of at least one thousand AZN. Considering the high rates of piracy and low levels of actual protection of copyright and related rights in Azerbaijan, there is a need to study whether the condition of a 'large' scale damage as a prerequisite for criminal sanctions is at all necessary. For instance, the damage should be caused at a rate of at least five hundred AZN for a criminal responsibility to attach for the commission any of the offences against property established in Articles 177 through 189 of the Criminal Code. A revision would also be important to foster better cooperation against copyright infringements internationally, particularly with the countries applying criminal sanctions with no or lower threshold condition. However, this limitation does reflect both the Convention on Cybercrime and the TRIPS Agreement, which requires criminal sanctions only for acts committed 'on a commercial scale'.[570]

---

[566] Ibid, Article 6.3.

[567] Topographies of Integrated Circuits is defined by Article 1 of the Law on Legal Protection of Topographies of Integrated Circuits 2002 as a spatial geometric arrangement, reflected by a layer of elements and inter-elementary connections of an integrated circuit.

[568] Requirements on use of folklore expressions are determined by the Law on Legal Protection of Azerbaijani Folklore Expressions 2003, No. 460-IIQ, which defines the 'violation' as untraditional and uncommon use of folklore expressions with commercial purpose. See Article 1, for the definition of 'folklore expressions'.

[569] Compilations of data means objective form of presentation of the works, data and other materials obtained by electronic or other means arranged in a systematic or methodical way according to Article 1 of the Law on Legal Protection of Compilations of Data 2004, № 755-IIQ.

[570] See Article 10, European Convention on Cybercrime (2001); see also, Article 61, WTO Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994 (TRIPS Agreement).

ii. Commission of acts criminalised under the provisions of Article 165, 165-1, 165-2 and 165-3 shall be punished by a fine or correctional work for a term of up to 480 hours. If the same crimes are committed repeatedly, or by a group's conspiracy, it shall cause a higher fine or imprisonment for a term of up to three years.

Markedly, these sanctions are considerably more lenient than sanctions imposed for the commission of crimes against property stipulated in Chapter 23 ('Crimes against Property') of the Criminal Code. In fact, pursuant to the Criminal Code, inflicting large-scale damage against property is an aggravating condition and shall cause imprisonment for a term of up to seven years.[571] Hence, unlike provisions of 'Misappropriation or embezzlement' (Article 179.2.4.) or 'Fraud' (Article 178.2.4.), sanctions determined for infringements of copyright or related rights can hardly constitute a deterrent in this field, even if effectively applied in practice. In addition, the presence of such a disparity in sentencing between crimes against property and crimes against intellectual property can send out the wrong messages that intellectual property rights, which are generally perceived as instruments for development,[572] is less significant than the physical one.

iii. iv. The Criminal Code provides for criminalisation of infringement of copyright and related acts, but revisions or amendments of relevant provisions have not followed the harmonisation. However, the provisions of criminalisation of copyright and other related rights under Article 165 are mostly compatible with those provided by the Convention on Cybercrime (Article 10), subject to slight ambiguity. More precisely, an element of 'wilfulness' is not explicitly attached to the provisions of criminalisation determined by Article 165, as well as by Articles 165-1, 165-2, 165-3, which is acknowledged as a prerequisite for the criminalisation of infringements of copyright and related rights pursuant to Article 10 of the

[571] See for example, 'Misappropriation or embezzlement' (Article 179.2.4.), 'Fraud' (Article 178.2.4.), Theft (Article 177.2.4.) of the Criminal Code (1999).

[572] See for further discussion, Hiroyuki Odagiri, *Intellectual Property Rights, Development, and Catch Up* (Oxford: Oxford University Press, 2012); Ruth Towse, 'The Quest for Evidence on the Economic Effects of Copyright Law', (2013), *Cambridge Journal of Economics,* 37, 1187-1202; Lewis S. Davis and M. Fuat Sener, 'Intellectual Property Rights, Institutional Quality And Economic Growth' (2012) *SSRN Electronic Journal*; Keith Maskus, 'The New Globalisation Of Intellectual Property Rights: What's New This Time?' (2014) 54 *Australian Economic History Review*, 262-284.

Convention. Moreover, Convention on Cybercrime, provisions are intended to provide for criminal sanctions against infringements committed through means of a computer system. The Criminal Code has adopted a broader approach, which covers both offline and online infringements.

4.3.2.3 Content-related offences

As the Internet encourages the production and exchange of information (including images), its proliferation has been accompanied by the production and exchange of content regarded as 'immoral'.[573] Due to the extensive variations in normative values reflected in national legal systems, it has been challenging to reach an international consensus on defining the provisions about illegal content. Furthermore, the potential conflict with freedom of expression has been the main concern for any assertion of a criminalisation approach.

Nevertheless, the degree of criminalisation of content-related offences in Azerbaijan differs significantly from that of other countries despite its own strong constitutional protection of freedom of speech. Notwithstanding the absence of a clear evidence of any concrete harm caused to others, a wide range of content-related offences exist in Azerbaijan. This is not to entirely discount the legality of responses in Azerbaijan, since the harm principle might also fail 'to constrain the scope of criminalisation, and … to take individuals seriously'.[574] Although, the harm principle does indeed sound sensible, its practical use might become challenging with regard to the scope of criminalisation of the content-related offences.

The 'margin of appreciation' doctrine developed by the European Court of Human Rights is noteworthy in this regard, in the sense that it allows leeway to countries in determining the boundaries of acceptable expression in line with their own cultures and legal traditions.[575] It means that Azerbaijan has also been granted some discretion, in taking administrative legislative or judicial action in the area of a

[573] UNODC, *The Globalisation of Crime. A Transnational Organized Crime Threat Assessment* (UN Publications 2010) 212.
[574] Hamish Stewart, 'The Limits of the Harm Principle' (2009) 4 *Criminal Law and Philosophy*, 26.
[575] See for example, *Handyside v United Kingdom,* 5493/72 [1976] ECHR 5; *Dudgeon v UK, 7525/76*, [1981] 4 EHRR 149; *Evans v UK,* 6339/05, [2007] ECHR 264.

Convention right. However, as pointed out in *Schalk & Kopf v Austria* (2010), the scope of the margin of appreciation varies given the circumstances, the subject matter and its background.[576] It is also acknowledged by the UN that there are diverse national approaches to the criminalisation of internet and social media content can be accommodated by international human rights law, within certain boundaries.[577] Criminal prohibitions on child pornography; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; incitement to terrorism; and propaganda for war, has been regarded by the UN as permissible.[578] Criminal offences relating to defamation, obscene material, and insult, however, should face a higher threshold, even within the margin of appreciation, to demonstrate that the measures conform to the principle of proportionality, are appropriate to achieve their protective function, as well as the least intrusive instrument measures proportionate to the interest to be protected.[579]

A distinct legal framework regulating the online content provision does not exist in Azerbaijan. Although no peculiarity is presented by content-related offences other than the application of ICTs and networks, this research will critically analyse the provisions regarding offences related to pornography alongside other content-related offences that have been prominent in the light of increasing use and ease of availability of ICTs in Azerbaijan.

II. Offences related to pornography

i. Given that pornography has traditionally been a mainstay of the internet, the largest proportion of materials containing pornography, including child

[576] *Schalk & Kopf v Austria*, 30141/04, [2011] 2 FCR650.
[577] UNODC (n. 71), 116.
[578] Ibid.
[579] United Nations Human Rights Committee, 2011. *General Comment No. 34. Article 19: Freedoms of opinion and expression.* CCPR/C/GC/34, 12 September 2011. para. 34; see also *General Comment No. 27*, para.14; *Marques v Angola,* U.N. Doc. CCPR/C/83/D/1128/2002; *Coleman v Australia*, U.N. Doc. CCPR/C/87/D/1157/2003.

pornography, is now transmitted electronically, through bilateral and multilateral exchanges.[580]

The legal status of pornography in Azerbaijan is ambiguous to some extent. Despite the fact that the illegal dissemination of pornographic materials, or illegal preparation, distribution of those materials for advertisement purposes, as well as illegal trading with pornographic publications, films or videos, images and other things, have been criminalised,[581] the legal definition of 'pornography' has not been provided by the Criminal Code. The Law on Mass Media 1999 specified pornographic materials as meaning 'art, photography, painting, information and other materials, the basic contents of which one is a coarse and unworthy description of anatomic and physiological details of sexual relations'.[582]

Although the proposed element of pornography that the material contains 'coarse and unworthy description' limits the scope of criminalisation, the stance adopted by Azerbaijan is not fully consistent with the ECHR provisions on freedom of expression. It can be argued that the exercise of the freedom of expression may be subject to restrictions for 'the protection of health or morals',[583] which is the main legitimate aim of criminalising the dissemination of pornographic materials in Azerbaijan.[584] However, as the European Court of Human Rights stated in *Handyside v United Kingdom*, the right 'is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society''.[585]

Another problematic element is that the Criminal Code prohibits only the 'illegal' dissemination, preparation for advertisement or trading with pornographic

[580] UNODC, *The Globalisation of Crime. A Transnational Organized Crime Threat Assessment*. (United Nations Publications 2010) 212.
[581] Article 242, Criminal Code (1999).
[582] Article 3, Law on Mass Media 1999.
[583] Article 10.2, Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), ETS 5.
[584] The Criminal Code contains Article 242 under the Chapter that concerns with public morality.
[585] *Handyside v United Kingdom,* 5493/72 [1976] ECHR 5, para. 49; see also, *Otto Preminger Institut v Austria*, 13470/87, [1994] 19 EHRR 34.

materials, which implies that some such activities can sometimes be legal but fails to clearly define what amounts to 'legal dissemination, preparation or trading'. It can be claimed that any pornography websites or platforms used in Azerbaijan could be outlawed.

Article 242 of the Criminal Code punishes the illegal dissemination but not mere possession of pornographic materials or items. This 'legal moralistic'[586] stance has also been supported by the academic literature in Azerbaijan. It is claimed that the dangerousness of the dissemination of pornographic materials lies in its negative impact on 'the normal development of adolescents, potential of resulting in further occurrence of rape, violent sexual actions and sexually immoral behaviour'.[587] However, the statement has not been supported with further empirical evidence. Generally, it is difficult to defend the idea that the distribution of pornography harms society to the extent that provides sufficient condition for state intervention through criminal law. The absence of clear evidence of concrete harm caused by making the pornography freely available has resulted in a unanimity around general opposition to censorship by the supporters of the liberal position.[588]

Notwithstanding that, the Code contained provisions regarding the criminalisation of the offences related to pornographic material, in 2012 a new offence focusing on child pornography was added to the Code.[589] This offence criminalises the 'turnover of child-pornography', by covering the acts of distributing, transmitting, advertising, selling, giving, offering, making available, as well as producing, procuring and possessing with the aim of its distribution or advertisement.[590] As provided by Akdeniz, a clear and succinct definition of what constitutes child

[586] 'Legal moralism' is the view that certain behaviours that conflict with society's collective moral judgments can be prohibited through law even if the conduct does not result in harm to others. See Patrick Devlin, *The Enforcement of Morals* (Oxford: Oxford University Press 1965) 10.
[587] Rafig Guliyev and Mahammad Imanov, *Criminal Law: The Special Part* (*Cinayət hüququ: Xüsusi hissə*) (Baku Digesta, 2001) 501.
[588] See for example, Bernard Williams (Edn.) *Obscenity and Film Censorship*, (Cambridge: Cambridge University Press, 1981). Dworkin, R. 'Do We Have a Right to Pornography?', in *A Matter of Principle*, (Cambridge, MA: Harvard University Press,1985); Helen Fenwick, *Civil Liberties and Human Rights* (Routledge-Cavendish; 4th edition, 2007); Gordon J Hawkins and Franklin E Zimring, *Pornography in a Free Society* (Cambridge: Cambridge University Press, 2011).
[589] See Law on Amendments to the Criminal Code of the Republic of Azerbaijan 2012, 408-IVQD.
[590] Article 171-1, Criminal Code (1999).

pornography is critical in ensuring that offenders are brought to justice.[591] Fortunately, compared to Article 242, a definition of child pornography has been provided by Article 171-1, which is mainly compatible with that introduced by the Convention on Cybercrime, subject to slight differences. According to Article 171-1, for the purposes of Article 171, the term 'child pornography' means any pornographic materials or things that depict a minor or a person appearing to be a minor engaged in a real or simulated sexually explicit conduct, or sexual organs of minors, as well as realistic images representing a minor engaged in sexually explicit conduct. Possibly, the legislator has aimed at protecting the children from sexual abuse and exploitation by including the term 'realistic images representing a minor', which has broadened the scope of the offences. Also, text and audio depiction of child-pornography is also covered under this definition. Moreover, not only a real engagement but also fictitious engagement of a minor in sexually explicit conduct is fallen under the scope of protection.

The definition of the term 'minor' is specified by the Code as a person under the age of eighteen, which is identical to the definition provided by the Convention on Cybercrime. In accordance with Article 1 of the UN Convention on the Rights of the Child, the Convention defines the term 'minor' in relation to child pornography as any person under the age of 18 years.[592] The Convention also determines that a member state may require a lower age-limit based on their national laws, but this limit cannot be less than 16 years.[593]

Article 171-1 of the Code is not only focused on criminalising various aspects of the electronic production, possession and distribution of child pornography, notwithstanding the article was added to the Code to bring the relevant provisions in compliance with the Convention. In other words, instead of criminalising only the computer-related production, distribution or possession of child pornography, a broader approach is adopted by the Code, which covers both online and offline turnover of child-pornography materials. It can, therefore, be argued that this

[591] Yaman Akdeniz, *Internet child pornography and the law: national and international responses* (Routledge, 2016).
[592] Article 9.3, Convention on Cybercrime (2001).
[593] Ibid.

approach may result in an overlap between the provisions of Article 242, which criminalises the illegal dissemination of pornographic materials or items, and Article 171-1 (turnover of child-pornography).

The clarification of acts to be covered under the provisions of child-pornography turnovers, such as 'distribution', 'transmission', 'advertisement', 'selling', 'giving', 'offering', 'making available', as well as 'production', 'procurement' and 'possession', have not been provided by Article 171-1. As a result, the Explanatory Report to the Convention on Cybercrimes might be useful in illustrating the meaning of these acts.[594]

Procurement, possession or production of child pornography may lead to criminal liability under Article 171-1, but only if those acts are committed for the purposes of distribution and advertisement. In other words, mere procurement, mere possession and production for oneself for personal use are not treated as the 'turnover of child-pornography', and the legislator has not detailed the reasons why a mere possession of child pornography is not criminalised. Whereas, Article 9 of the Convention suggests the criminalisation of both the procurement of child pornography through a computer system for oneself and possessing child pornography in a computer system or on a computer-data storage medium. However, it is also agreed that parties may reserve the right not to apply, in whole or in part, these provisions.[595] The main controversy of the Article 171-1 in this regard remains the issue of non-criminalisation of the production of child-pornography for personal use. More importantly, the Convention on Cybercrime itself also demands the states to criminalise the act of production 'for the purpose of its distribution through a computer system'.[596] It can, therefore, be claimed that this provision of the Convention on Cybercrime seems incompatible with another Council of Europe Convention focused on the Protection of Children, which

[594] See paragraphs 94-96 of *Explanatory Report to the Convention on Cybercrime* (2001), for the definitions of acts covered by the provisions of offences related child-pornography.
[595] Article 9.4. Council of Europe Convention on Cybercrime (2001).
[596] Ibid. Article 9.1,

demands state parties to ensure the criminalisation of 'producing child pornography', without further attaching any specific intention.[597]

Article 171-1 does not explicitly require the offences to be carried out intentionally, and therefore the scope of criminalisation becomes broadened and covers the accidental dissemination of child-pornography as well. Simply, regardless of the presence of any specific intent, if the process of dissemination or transmission is finished, it should be treated as a 'child-pornography turnover'. When it comes to the production, procurement and possession of a child-pornography, these acts need to be backed with specific purposes, which are either dissemination or advertisement, in order to be treated as a crime under Article 171-1.

ii. Sanctions imposed over the commission of child-pornography offences are significantly stricter compared to those determined for offences contained in Chapter 30. The applicable penalty for these offences is a deprivation of liberty for a term of up to five years, in the absence of aggravating circumstances.[598] While the presence of aggravating circumstance results in the imposition of penalty which consists of deprivation of the right to hold a certain position for a term of up to 3 years and by deprivation of liberty for the term of up to 8 years. Noticeably, the severity of these offences has been reflected by the magnitude of the punishment prescribed by the Code.

iii. The pre-harmonised version of the Criminal Code contained provisions criminalising the illegal distribution of pornographic materials and things. However, it did not provide specific 'child-pornography' criminalisation provisions focused on the protection of minors from abuse, and the disruption of child pornographic materials to discourage offenders from seeking to produce and supply further materials and things.

[597] Article 20, Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) CETS No.201. Note: Azerbaijan has signed the Convention in 2008, but not ratified it yet.
[598] Article 171-1.2 of the Criminal Code (1999).

iv. The provisions of criminalisation of child-pornography offences under Article 171-1 are mostly compatible with those provided by the Convention on Cybercrime (Article 9). However, elements of 'intentionality' and 'without right' are not clearly and explicitly enclosed in Article 171-1, which are deemed to be necessary elements of criminalisation of a child-pornography according to Article 9 of the Convention. Moreover, the Convention on Cybercrime seeks to circumscribe more effectively 'the use of computer systems' in the commission of sexual offences against children, while Article 171-1 of the Criminal Code is not explicitly focused on criminalising various aspects of the electronic production, possession and distribution of child pornography.

II. Other content-related offences

In addition to the offences related to pornography and child pornography, there are offences criminalised in Azerbaijan the commission of which have been provided with vast opportunities and grounds by the growing use of ICTs and the Internet and thus, the scale and reach of these offences have been significantly enhanced. (1) 'Incitement to national, racial, social or religious hostility', (2) 'Libel' and (3) 'Insult', (4) 'Violation or humiliation of the honour and dignity of the head of the state', as well as (5) 'Public appeals directed against the state' can be included among these offences.[599] Given that these offences are also committed outside cyberspace and raise major issues about political freedoms that go beyond this study, their criminalisation is elaborated in brief for the purposes of this section.

(1) As mentioned above, the Constitution of the Republic of Azerbaijan prohibits any propaganda provoking racial, national, religious and social discord and animosity.[600] Thus, when committed openly, as well as through the use of mass media, actions aimed at the incitement of national, racial, social or religious hatred and hostility, humiliation of national dignity, as well as actions directed at restricting citizens' rights, or establishment of the superiority of citizens on the basis of their

[599] See: Articles 147,148, 281, 283, 323, Criminal Code (1999).
[600] Article 47, Constitution of the Republic of Azerbaijan (1995).

national or racial belonging are subjected to a criminal punishment under the Criminal Code.[601] The term 'mass media' also covers the Internet and social networking platforms,[602] which provide with powerful and modern means for supporting racism and xenophobia and enable to disseminate expressions containing such ideas easily and widely.[603] The Code, however, does not clearly define the concepts such as 'incitement of national, racial, social or religious hatred and hostility, or 'humiliation of national dignity'. Hence, the application of these concepts in practice by courts has resulted in serious consequences.[604]

Although the provisions of Article 283 have covered a wide range of acts related to the propagation of a racist and xenophobic nature, Azerbaijan has neither signed nor ratified the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. The Additional Protocol specifies that 'States Parties have not only to enact appropriate legislation but also to ensure that it is effectively enforced'.[605] Whereas, effective enforcement of relevant laws alone has also been problematic in Azerbaijan. Several human rights organization reports have stressed that in practice, relevant Criminal Code Articles on content-related offences have been applied in a discriminatory fashion and have been misused for curtailing freedom of expression in Azerbaijan.[606]

---

[601] Article 283, Criminal Code (1999).

[602] According to Article 3 of the Law on Mass Media, periodic print publications, TV-Radio programs, programs of a newsreel, information agencies, Internet and other forms of distribution are all considered as 'mass media'.; see also, para. 5, Resolution of the Plenum of the Supreme Court of the Republic of Azerbaijan 'On the judicial practice on considering complaints in private criminal prosecutions' (February 21, 2014 No 03).

[603] Council of Europe, Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003) ETS - No. 189, para. 3.

[604] See for example*, Fatullayev v Azerbaijan,* 40984/07, [2010] ECHR 623; see also, Media Rights Institute, *Execution of Judgments of the European Court of Human Rights in Azerbaijan, Status Quo Upon Azerbaijan's Chairmanship of the Committee of Ministers of the Council of Europe* (2014); Swiss Institute of Comparative Law*, Comparative Study on blocking, filtering and take-down of illegal Internet content (2015).*

[605] Article 1, 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 (2003) ETS - No. 189.

[606] See for example, Freedom House, *Freedom on the Net (*2016); Expression Online Initiative, *Searching for Freedom: Online Expression in Azerbaijan* (2012); International Bar Association's Human Rights Institute (IBAHRI), *Azerbaijan: Freedom of Expression on trial* (2014).

(2) and (3) The approach to the protection of the freedom of expression in Azerbaijan can also be scrutinised through elaborating legal responses to libel and insult, which are among the most widely occurring acts over the Internet, as was also confirmed during the interviews. Article 147 of the Criminal Code prohibits 'the distribution of obviously false information' which 'discredits the honour and dignity of any person or undermines his reputation'. Insult or 'deliberate humiliation of honour and dignity of a person, expressed in an indecent form' has been criminalised by Article 148. Rather than removing the provisions on criminal defamation, the scope of both of these articles was specifically extended in May 2013 to cover the content 'publicly expressed in internet resources'.[607] Both offences can be punished by six months imprisonment, and the punishment may be extended to three years imprisonment for aggravated instances of defamation.[608] The government favours the criminal liability for defamation as a means of combatting cybercrime, notwithstanding human rights groups are concerned that such provisions can be used to silence all critical voices.[609]

(4) Perpetration of the same acts against the head of the state – the president of the Republic of Azerbaijan - shall carry legal consequences of imprisonment up to five years in length according to Article 323 of the Criminal Code. Imposition of a prison sentence can be considered even more disproportionate interference with freedom of expression, and as recalled in by European Court of Human Rights in *Mahmudov and Agazade v Azerbaijan* case*,* '…in breach of Article 10, which could not be regarded as "necessary in a democratic society".[610]

[607] Law on Amendments to the Criminal Code of the Republic of Azerbaijan 2013, № 650-IVQD, see for discussion, New Legislative Amendments Further Erode Rights To Freedom Of Expression and Peaceful Assembly | Reporters Without Borders' (RSF, 2013) https://rsf.org/en/news/new-legislative-amendments-further-erode-rights-freedom-expression-and-peaceful-assembly.

[608] Accusing a person with committing a grave or especially grave crime is considered a circumstance aggravating the applicable penalty. See Article 147.2. Criminal Code (1999).

[609] Media Rights Institute, *Execution of Judgments of The European Court of Human Rights in Azerbaijan, Status Quo Upon Azerbaijan's Chairmanship of the Committee of Ministers of The Council of Europe* (2014) 39.

[610] *Mahmudov and Agazade v Azerbaijan,* 35877/04, 18 December 2008.

(5) Furthermore, it is not only the public appeal for seizing state power by force, or public calls to overthrow the constitutional order by force that has been criminalised. Distribution of the material containing such appeal is also punished under the Criminal Code.[611] Moreover, these acts bear legal consequences of imprisonment for up to five years in length, which is the most severe punishment adopted in the South Caucasus region.[612]

Given that the Internet and social media platforms 'are increasingly used to disseminate content critical of the government',[613] provisions of 'public appeals directed against the state', as well as the extended criminal defamation provisions might further accelerate the process of 'leading to a genuine media self-censorship and causing progressive shrinkage of democratic debate and of the circulation of general information'.[614]

It is worth recalling the constitutional provision which provides that 'the rights and freedoms are [also] limited by the rights and freedoms of others',[615] and it is, therefore, necessary not to overstep certain bounds while imparting information or ideas on any matter. However, as reiterated by the European Court of Human Rights in *Fatullayev v Azerbaijan* case, although statements made may be considered 'shocking or disturbing' by the public, '… the freedom of expression is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference but also to those that offend, shock or disturb the State or any sector of the population'.[616]

---

[611] Article 281. Criminal Code (1999).
[612] For example, the same acts are punished with a deprivation of liberty up to 3 years both in the Republic of Georgia and in the Republic of Armenia.
[613] Freedom House, *Freedom on the Net* 2014 *Report;* see also, Amnesty International, *Amnesty International Report 2015/16: The State of The World's Human Rights,* 2016, 76-77.
[614] Council of Europe Parliamentary Assembly, *Towards decriminalisation of defamation*, Resolution 1577 (2007), para. 8.
[615] Article 71, Constitution of the Republic of Azerbaijan (1995).
[616] *Fatullayev v Azerbaijan*, 40984/07, [2010] ECHR 623, para. 49; see also *Handyside v United Kingdom,* 5493/72 [1976] ECHR 5*,* para. 49

4.4 Conclusion

Laws are the main instruments used for regulatory purposes and thus, take a major role in combatting cybercrimes. However, Azerbaijan has not established specific laws to control and prevent cybercrime. The issue is rather regulated in a fragmented way through different laws that have rendered the regulation inconsistent. There are also inconsistencies between laws and requirements that should be addressed to appropriately deal with the specific challenges of cyberspace. This is because, the role of criminal law in virtual worlds is limited due to the several factors such as having a physical component as the primary focus, ignoring the societal structure of cyberspace, possessing the slow dynamic of development and enforcement, and thus, becoming easily outdated. Moreover, while Azerbaijan has taken some steps to develop a pluralist political system, democratic institutions and human rights protection mechanisms, yet the legal system in Azerbaijan still preserves the old traditions, due to it being a modified version of the Soviet communist legal system. Thus, adequate implementation of emerging laws and rights has been troublesome due to the absence of effective mechanisms or a supportive legal culture.

Cybercrime is still often regarded as either a ‘crime not representing great social danger’ or a ‘minor crime’ because the public has not been properly enlightened about the actual and potential threat, and the reflection of the government is based on reactions of its citizens to the problem. The inclusion of cybercrime offences among ‘crimes not representing great social danger’ or ‘minor crimes’ has the potential to stultify the full array of necessary responses to cybercrime. Differing perceptions of harm and risk caused by cybercrime may also lead to reluctance to becoming closely involved in international cooperation, especially with regard to prioritising incoming requests.

Some criminalisation gaps and inconsistencies remain, resulting in the potential to affect both Azerbaijan and cooperation with other countries. In terms of computer integrity crimes, specific criminal legislation on cybercrime, which is reflected through the Criminal Code (1999)/Chapter 30, has been harmonised with the Convention on Cybercrime in 2012. As a result, the Criminal Code has provisions

criminalising offences such as illegal access, illegal interception, data interference, system interference and misuse of devices as crimes. However, some of the potential computer assisted crimes, in particular, phishing and computer related identity theft offences have not been introduced as separate cybercrime offences by the Code. By contrast, in terms of 'Content – related offences', a broader number of offences have been criminalised besides pornography and child pornography related offences. Cyberstalking, however, has not been attended to.

Sanctions determined by the Criminal Code to be imposed on the acts studied have also presented inconsistencies. It was argued that imposition of equally severe or identical punishments for acts differing from each other by the inclusion of harm as a necessary element can be considered neither proportionate nor dissuasive.

Consequently, Azerbaijan should either place a proportionate effort in developing new substantive laws to overcome cyber-specific challenges and to appropriately respond to cybercrime or amend its existing criminalisation provisions so that the number of gaps and inconsistencies is reduced to a minimum.

CHAPTER 5: Procedural Laws and International Cooperation

5.1 Introduction

When considering the cybercrime challenges, extensively discussed in Chapter 2, it became evident that cybercrime poses specific design and legal challenges which facilitate crimes and create obstacles for the LEAs in fighting these crimes. These challenges necessitate the establishment and deployment of appropriate procedural instruments and investigative techniques, which enable fair, effective and efficient investigation and adjudication of cybercrime. Having analysed relevant substantive laws and the criminalization approach adopted and applied in Azerbaijan in Chapter 4, it is now crucial to scrutinise criminal procedure laws and investigatory powers. Thus, this chapter deals with the fourth research objective, which is to evaluate the appropriateness of the domestic procedural powers and instruments.

National procedural measures and instruments are critically analysed with reference to the procedural specifications of the Convention on Cybercrime, which contains a set of provisions regarding 'domestic criminal procedural law powers necessary for the investigation and prosecution' of cybercrime.[617] In addition, the chapter scrutinises national laws and practices adopted in Azerbaijan regarding jurisdictional issues and international cooperation provisions, as well as the provisions on the collection and admissibility of digital evidence that also go beyond the regulations of the Convention. Specific suggestions and recommendations to address the issues and problems raised are presented in Chapter 6.

5.2 Procedural Provisions

The legislation of the Republic of Azerbaijan on criminal procedure determines the legal procedures governing criminal prosecution and defence of suspects or accused persons,[618] which consists of the Constitution, the Code of Criminal Procedure, other specific laws, and the international instruments to which

[617] *Explanatory Report to the Convention on Cybercrime* (2001) ETS No. 185, para. 16.
[618] Article 1, Criminal Procedure Code of the Republic of Azerbaijan (2000).

Azerbaijan is a signatory.[619] Thus, only the powers and procedures determined by the criminal procedure legislation necessary for the realisation of criminal investigations or proceedings shall be applied to the criminal offences established in accordance with relevant articles of the Criminal Code (1999) and the Convention on Cybercrime (2001). By signing and ratifying the Convention, Azerbaijan has taken further the obligation of incorporating into its legislation the possibility of use of digital or electronic information as evidence in criminal proceedings. The Convention has also made it explicit that signatories have to ensure that evidence in the digital form of not only cybercrime offences but also any criminal offence can be gathered through the powers and procedures set out in it.[620] It is, therefore, important to identify the status of digital evidence in Azerbaijani criminal procedure laws before embarking on the analysis of key investigative powers.

5.2.1 Legal status of digital evidence

As a reconstructive process, a criminal investigation is meant to be a logical process, which draws conclusions based on specific pieces of evidence.[621] Identification, selection, collection, preservation, preparation, authentication, verification, evaluation and presentation of evidence are crucial to accurate criminal investigation and proceeding, as they establish grounds for the guilt or innocence of an individual at trial. However, all these processes face serious challenges by the complex/technical nature of cyberspace, the anonymity and speed of activities in cyberspace, the possibility of 'spoofing' and the potential for multi-stage action.[622]

The evidence is defined broadly in Article 124 of the Code of Criminal Procedure 2000 and covers any factual knowledge, obtained in accordance with the Code, by

[619] Article 2, Ibid.
[620] Ibid. Article 14 (b) (c). Council of Europe, Convention on Cybercrime (2001) ETS No. 185.
[621] Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics*, LAW COM No. 245, 1997; see also, Eoghan Casey (n. 495); Christine M. H Orthmann et al., *Criminal Investigation* (Delmar Cengage Learning, 2013) 8.
[622] Russell Buchan and Nicholas Tsagourias, 'Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence' (2016) 21 *Journal of Conflict and Security Law*, 377-381.

which the presence or absence of facts and circumstances necessary for the criminal proceedings can be proved. The Code further makes it explicit that the following shall be admitted as evidence in criminal proceedings:

> "1. testimony of the suspect, the accused, the victim and witnesses;
> 2. the expert's opinion;
> 3. material/demonstrative evidence;
> 4. records of investigative and court proceedings;
> 5. other documents."[623]

Digital/electronic evidence plays a central role in the investigation, prosecution and adjudication of cybercrime. Given the growth of ICT in Azerbaijan, it can be argued that the role of digital evidence will be even further evolved for cybercrime cases and will become an 'even more common aspect of criminal cases'.[624] In Azerbaijan, however, digital evidence has been neither widely scrutinised and analysed nor thoroughly understood, as revealed during the fieldwork in Azerbaijan. 8 out of 11 district courts contacted for the interview in the capital of Azerbaijan claimed that the number of trials involving digital evidence is limited and that there have been no cases involving cybercrime adjudication. The researcher did not go further with conducting interviews regarding non-cybercrime cases involving digital evidence as it would go beyond the scope of this study. During the interview with Parliament Officer 1, it was suggested that '...judges should be trained and acquire knowledge on different aspects of cybercrime adjudication and digital evidence handling'. During the informal meetings with the law enforcement officials/investigators, it was stated that where there is digital evidence involved, digital forensics experts or IT experts are generally called in for support. So, in general, investigators themselves are not prepared or trained to handle digital evidence and are strongly dependent on IT experts' help and opinions, which decreases the efficiency of prosecutions. The Code of Criminal Procedure 2000, however, stipulates that the preliminary investigator[625] and the investigator[626] are obliged to investigate the case thoroughly, fully and objectively and order examination of all evidence related to

[623] Article 124, Criminal Procedure Code (2000).
[624] Susan W Brenner (n. 175) 142.
[625] See Articles 85 for further information about the duties of preliminary investigator.
[626] Ibid. Article 86 of the Criminal Procedure Code for the duties of investigator.

crime through exercising the procedural powers, such as questioning the victim, witnesses and the suspect, calling for expert reports, ordering search and seizure, once it has been established that a crime has been committed.[627]

As discussed in Chapter 3, prosecutors' and judges' knowledge on technological issues, cyberlaw and digital evidence are also immature due to the scarcity of cybercrime related studies and lack of opportunity to adjudicate actual cybercrime cases.[628] These factors could be the reason behind their unwillingness to accept and deal with digital evidence. Another major drawback of these knowledge and training shortages is the possibility that judges and prosecutors might assume that the digital evidence produced is authentic and thus, will not dispute its authenticity, which can undermine the legitimacy of the proceeding.

Digital evidence is still relatively alien to the national legal system. No single definition of digital/electronic evidence is contained by the Code. Nor is the term 'digital/electronic evidence' used in any part of it. So, the rules on evidence appear to be based on the traditional general notion of the evidence and lack comprehensiveness in their scope. Nonetheless, according to CPC, electronic carriers bearing information in the form of letters, numbers, graphics or other signs are recognised as 'documents'.[629] The definition of the 'document' is provided by the Law on Information, Informatisation and Protection of Information 1998 as documented information fixed on a material carrier in the form of text, audio or image and bearing requisites allowing it to be identified.[630] Although the information in audio/voice form is also covered by this definition, it narrows the scope of regulation applied by the Code to electronic data and information by including only documented information fixed on a material carrier. The Law (1998) further limits the use of a document received from information systems, including automatised systems by requiring its validity to be obtained through its signature by an official.[631] By contrast, the definition is given by the Law on Electronic Signature

[627] Ibid. Articles 85 and 86.
[628] See Section 3.4.1, Chapter 3.
[629] Article 135, Criminal Procedure Code (2000).
[630] Article 2, Law on Information, Informatisation and Protection of Information 1998.
[631] Ibid Article 5.

and Electronic Document 2004 to the meaning of 'electronic document' seems to broaden the scope by excluding the requirement of being fixed on a material carrier. It determines that a document submitted in electronic form to be used in information systems is an electronic document; here, the document needs to be confirmed by an electronic signature.[632] Thus, it can be asserted that both laws lack comprehensiveness and demonstrate an insufficient understanding of the digital/electronic evidence as these laws impose restrictions over the use of documents through attaching validity requirements, which limits their utilisation for investigation purposes. Consequently, notwithstanding that evidence of some cybercrime acts, which mainly exist in electronic or digital form, can be considered as 'documents' according to the Code of Criminal Procedure 2000 and used for investigative proposes if fixed on a material carrier, or confirmed by an electronic signature, legal provisions directly regulating digital evidence are not in place.

The Code also determines that documents possessing the characteristics of material evidence – any object that can serve to identify circumstances bearing importance to the criminal prosecution due to its characteristics and features, origin, place and time of discovery or the imprints it bears - can also be considered as material evidence.[633] Since the computer system or data needs to be either the tool or target for the commission of a crime in order for it to be labelled as 'cybercrime', cybercrime cases necessitate the investigation of digital devices where the evidence is either stored or transferred in an electronic form.[634] Thus, provisions identified for material evidence should apply to the investigation of cybercrime where electronic carriers bearing information in the form of letters, numbers, or graphics are used as a tool or become an object of a crime, or bear imprints of it.

The Criminal Procedure Code 2000 appears to provide general investigative powers and techniques for the investigation of cybercrime. However, the lack of specific legal provisions on digital evidence poses additional challenges for LEAs in obtaining, analysing and presenting them. The importance of adopting specific

[632] Article 1, Law on Electronic Signature and Electronic Document 2004, № 602-IIQ.
[633] Article 135.2, Criminal Procedure Code (2000).
[634] Eoghan Casey (n. 495), 7.

optimised legal frameworks becomes visible when analysing the role of digital evidence, which varies depending on the phases of criminal investigation and proceedings. Various approaches exist in determining the stages of criminal proceedings in Azerbaijan.[635] It would be more systematic and easier to test the role and status of digital evidence through differentiating two major phases in which it is used: the investigation phase (survey/identification, collection/acquisition, preservation, and analysis) and report, presentation and use of evidence in court proceedings.[636] Techniques applied during the investigation phase can also be subdivided into coercive (powers of search and seizure) and covert (interception and surveillance) techniques.[637] Each of these phases will be thoroughly examined and scrutinised by the next sections of this Chapter, both as found in national and relevant multilateral instruments. At this stage, it needs to be highlighted that regardless of whether procedural laws are predominantly 'general/traditional' or 'cyber-specific', two essential requirements must be met in order to investigate cybercrime in a legitimate, effective and efficient way: a clear scope of application of the power in each abovementioned phase, in order to guarantee legal certainty in its application; and sufficient legal authority for actions.[638]

Satisfaction of these requirements is also crucial to ensure the admissibility of digital evidence in court. In Azerbaijan, a willingness to effectively address the admissibility of digital evidence or clearly distinguish between digital and physical evidence has not been adequately shown by lawmakers yet. It can, however, be claimed that not making a clear legal distinction between digital and physical evidence does not necessarily make the digital type inadmissible. According to a study conducted by United Nations, many countries considered that 'it was good practice not to make a distinction, as this ensures fair admissibility of electronic evidence alongside all other types of evidence'.[639] Thus, the same fundamental

[635] See for example, Miragha Jafarguliyev*, Criminal Procedure of the Republic of Azerbaijan (Azərbaycan Respublikası Cinayət prosesi)* (Baku, Ganun, 2008) 18-19, see also, Firuza Abbasova, *Criminal Process: General Part* (Baku, Zardabi, 2015) 23-27.
[636] Thomas J. Holt, Adam Bossler, Kathryn C. Seigfried-Spellar (n. 3), 330-333.
[637] Ian Walden (n. 476) 203.
[638] UNODC (n. 71) 123.
[639] Ibid, 166.

principles are applied to the admissibility of both digital and physical evidence, although there are notable differences between the two.

The legitimacy of evidence can be considered as one of the most fundamental principles of admissibility that is applied to either form of evidence. The Code of Criminal Procedure 2000, which sets the requirements for the collection, preservation, and use of evidence, has made it clear that evidence must be obtained in accordance with the requirements of the Code and without violating the constitutional human rights, or subject to restrictions determined by a court decision.[640] Satisfaction of this requirement is challenging with regard to digital evidence due to the existing uncertainty and lack of specific legal provisions on digital evidence. It can be helpful to establish cyber-specific provisions regarding digital evidence to address these challenges.

The Code has also attached further requirements to the admissibility of evidence, which are about its accuracy, source, and the circumstances in which it was obtained.[641] In an online environment, however, satisfying all of these requirements would be impossible due to the reasons that there might be faults, errors or other malfunctions that affected the reliability of the data, or such faults, errors or malfunctions can be generated by the criminal conduct itself.[642] Moreover, the likelihood of occurrence of these faults or errors increases even further as the volume of evidence to be collected in relation to a crime grows substantially due to the rising complexity of cyberattacks.[643] The code has made it explicit that there must be no doubt as to the accuracy, source, and the reliability of evidence in order for it to be admissible in criminal proceedings.[644] Thus, in the case of documentary evidence, only the original documents or a true copy of the originals are admissible to prove their contents and authenticity.[645] Application of these requirements to digital evidence raises a number of important questions since it is necessary to

[640] Article 124, Criminal Procedure Code (2000).
[641] Ibid, Article 125.
[642] Yvonne Jewkes, Majid Yar Eds, *Handbook of Internet Crime* (Willan, 2009) 622-623.
[643] Mark Walport, *Annual Report of the Government Chief Scientific Adviser 2015: Forensic Science and Beyond: Authenticity, Provenance and Assurance*, vol. 1 (Government Office for Science: London, 2015) 75.
[644] Article 125, Criminal Procedure Code (2000).
[645] Ibid. Article 135.3.

define what is meant by the 'original' or 'true copy', as it might not be possible to present the original data in court in all cases. The process might become more difficult due to the 'intangible and rather volatile' nature of electronic evidence.[646] Consequently, the admissibility of digital evidence in prosecuting cybercrime offences can be difficult from the legal standpoint. The lack of adequate training of those dealing with cybercrime exacerbates the problems.

In summary, Azerbaijan can be considered partially in line with Article 14 of the Convention, which requires the adoption of legislative and other measures as may be imperative for establishing the powers and procedures for the purpose of specific criminal investigations or proceedings provided for in the Convention on Cybercrime. This is because the possibility of use of digital or electronic information as evidence before a court in criminal proceedings has been provided by the general powers and procedures incorporated into the legislation, notwithstanding that specific legal provisions regulating digital/electronic evidence are not available, which poses additional challenges before law enforcement authorities during the investigation of cybercrime. Parliament Officer 1, NGO Representative 1, Independent expert 1, and all of the Ministry Officials (1-5) also confirmed this assessment. It can be suggested that the optimization of legal frameworks for digital evidence is crucial to enhance the capacity of the country in pursuing cybercrime.

5.2.2. Conditions and safeguards

Azerbaijan must ensure that all laws and procedural provisions are subject to the conditions provided for under its domestic law and implemented in a way that does not breach or undermine safeguards guaranteed by the Constitution,[647] as well as observing the international treaties to which the country is a party, since they are also an integral part of the legislative system.[648] Moreover, the country has to fulfil its statutory and specific obligations as a party to the major international human rights treaties, in particular, the ICCPR and ECHR, while acting against cybercrime.

[646] Paul De Hert, Gloria González Fuster and Bert-Jaap Koops (n. 434), 508.
[647] See Articles 30, 31, 32, 46, 47, 48 of the Constitution of the Republic of Azerbaijan (1995).
[648] Article 148, Constitution of the Republic of Azerbaijan (1995).

This is because the establishment, implementation and application of the powers and procedures provided for in the Convention on Cybercrime must be performed according to conditions and safeguards provided for under domestic law, which guarantee the adequate protection of human rights and liberties, including rights arising from International treaties to which Azerbaijan is a state party. [649]

The international instruments to which Azerbaijan is a signatory, the Constitution, the Code of Criminal Procedure, and other national laws constitute the sources of the laws of Azerbaijan on criminal procedure.[650] The norms of the Constitution and the rules of the international treaties shall be applied in case of conflict between those and the norms of the Code of Criminal Procedure. In addition, normative legal acts that abolish or restrict human and civil rights and liberties shall not be applied.[651] This can be regarded as a norm further demanding the inclusion of certain elements as 'conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties'.[652] More precisely, priority is given to the protection of human rights when balanced against the requirements of law enforcement. Pursuant to the Code, ensuring the protection of the rights, freedoms and dignity of an individual is mandatory for authorities participating in criminal proceedings. [653] The court can authorise by warrant temporary limitation of these rights and freedoms in connection with the application of coercive procedural measures only in cases, where its necessity is supported with appropriate legal grounds determined by the Code.[654]

For the purposes of evaluating the legality of steps taken during cybercrime investigations and criminal proceedings, it needs to be added that the Code even goes further through including a 'guarantee of the right to inviolability of private life'[655] and a 'guarantee of the right to inviolability of domicile',[656] among the fundamental principles of criminal proceedings. While the implementation of each

[649] Article 15, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[650] Article 2, Criminal Procedure Code (2000).
[651] Ibid.
[652] Council of Europe, *Explanatory Report to the Convention on Cybercrime (*2001), para. 145.
[653] Articles 12 and 13, Criminal Procedure Code (2000).
[654] Ibid.
[655] Ibid. Article 16.
[656] Ibid Article 17.

of these rights and liberties will be scrutinised by later sections in this Chapter, it is important to provide a brief overview here.

To ensure the protection of the right to private life and confidentiality of correspondence,[657] the Code makes clear that interception and collection of communication and information shall be permitted only upon 'a decision of the court and in the manner prescribed by law'.[658] It also prohibits the unnecessary collection, dissemination or use of information relating to the private life of any person and further adds that if a person requested to give or submit such information in pursuance of the relevant court decision, he could refuse to divulge it unless the need to collect this information for the purposes of the ongoing criminal case is reasonably justified.[659]

A court decision is also necessary for conducting examination and searching of property in the course of criminal proceedings.[660] As previously discussed in Chapter 2, when searching and collecting digital evidence, it is crucial to act rapidly and prevent the deletion of relevant data, as certain processes such as deletion can be completed in a few seconds.[661] However, techniques applied during the investigation phase need to be followed by a court decision (generally, 1-2 weeks is needed to obtain a court order), which compromise the speed and flexibility required for cybercrime investigations and international cooperation in favour of legality and protection of rights. To avoid negative impacts of waiting for a court decision, an agreement has been made with service providers for preserving data in an expedited manner, without a court order, which works in practice, despite some deficiencies.[662] Detailed analysis will be provided later in this Chapter.

---

[657] See for further discussion, Section 4.2. Chapter 4.
[658] Article 16, Criminal Procedure Code (2000).
[659] Ibid. Article 199.
[660] Ibid. Article 17.
[661] See Chapter 2, Section 2.4.
[662] See Law on Telecommunication 2005, № 927-IIQ, Law on Intelligence and Counter-Intelligence Activities 2004, № 711-IIQ; Council of Europe, Cybercrime Convention Committee (T-CY), *Assessment Report. Implementation of the preservation provisions of the Budapest Convention on Cybercrime,* (2012), 19; see for update; Cybercrime Convention Committee (T-CY), *Assessment Report. Implementation of the preservation provisions of the Budapest Convention on Cybercrime*. *Follow up given by Parties* (2015), 6.

Azerbaijan has also taken on additional specific obligations in the process of dealing with cybercrimes having become a signatory the Convention on Cybercrime in 2010. Article 15 of the Convention requires that the establishment, implementation and application of the powers and procedures adopted by Parties to the Convention shall be 'subject to conditions and safeguards provided for under its domestic law which shall ensure the adequate protection of human rights and liberties …and which shall incorporate the principle of proportionality'. [663]

So, the principle of proportionality has been given particular emphasis by the Convention on Cybercrime, and the Contracting States are obliged to incorporate this principle in their powers and procedures. As stated by Barak, '… every limitation of a constitutionally protected right, even if done by law, is to be considered as unconstitutional, unless it is done in conformity with the proportionality principle'.[664] As a '...structured test' that facilitates accountability by involving a detailed inquiry,[665] the principle is considered to establish a balance between individuals' right to the protection of private life and 'the interest for a safer society and protection of national interests'.[666]

This principle has not been directly consolidated within the legislation on criminal procedure. However, in broader terms, the principle of proportionality can be derived from the international instruments, in particular, international human rights instruments to which Azerbaijan is a signatory, since they are an integral part of national legislation. In addition, there are specific provisions ensuring that relevant powers or procedures are not excessive compared to the nature and circumstances of the offence. For example, the Code has made it clear that the collection of comprehensive evidence shall not result in the collection of unnecessary material for criminal proceedings.[667] Another explicit example of the application of this principle could be the requirement of 'a reasoned request', which

[663] Article 15, Convention on Cybercrime (2001).
[664] Aharon Barak, *Proportionality – Constitutional Rights and their Limitations* (Cambridge: Cambridge University Press 2012) 102.
[665] Lady Justice Arden, 'Proportionality: the way ahead?' (2013) Public Law 498.
[666] Nick Taylor, 'Policing, Privacy and Proportionality.' *European Human Rights Law Review*, 2003. Supp (Special issue: privacy 2003) 86 - 100.
[667] Article 146.3, Criminal Procedure Code (2000).

should elaborate the objective grounds and motivations, must be provided by LEAs in order to obtain a court decision that gives permission for a search or seizure.[668] Application of these requirements can also be regarded as examples of conditions and safeguards limiting the excessive powers and procedures through including 'judicial or other independent supervision, grounds justifying the application, and limitation of the scope and the duration of such power or procedure'.[669]

Consequently, from the theoretical perspective, Azerbaijan seems to be in line with Article 15 of the Convention on Cybercrime. However, the lack of cyber-specific provisions and adequate legal instruments enabling competent authorities to conduct an effective and efficient investigation of, and cooperation against, cybercrime leaves the human rights and liberties at risk of being compromised.

5.2.3 Expedited preservation of data

One of the crucial components of the digital forensic process is the preservation of digital evidence. The primary objective of preservation of digital evidence is to examine the data in a way that minimises the chances of any changes or modifications to the original data.[670] To comply with judicial scrutiny provisions in a court, it is imperative to examine the electronically stored data in the least intrusive manner.[671] Where there are grounds to believe that changes to the computer data are unavoidable or the data is particularly vulnerable to loss or modification, competent authorities shall be provided with such legislative and other measures enabling them to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, according to the Convention on Cybercrime.[672]

---

[668] Ibid. Article 243.1.
[669] Article 15.2, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[670] ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition and preservation of digital evidence,* (ISO copyright office, Geneva, Switzerland 2012*).*
[671] Rodney McKemmish, 'What is Forensic Computing?' (1999) 118 *Australian Institute of Criminology,* 1.
[672] Article 16 and 17, Council of Europe Convention on Cybercrime (2001) ETS No. 185.

The expedited preservation of computer data can enable LEAs (LEAs) to overcome the challenges of lengthy procedures, such as obtaining a court order, and thus, react faster and avoid the deletion of digital evidence that is crucial for investigation.[673] In this regard, as an alternative mechanism preventing the deletion of necessary data required for investigation processes, the limits on data retention have also been considered in several countries, such as the UK, France, and Sweden, and by the European Union.[674] These two approaches ('data preservation' and 'data retention') must be distinguished from each other. Data retention process may involve 'the retention of all data or any description of data', or 'it may relate to data whether or not in existence at the time of the giving, or coming into force, of the notice'.[675] It can be deduced that retention techniques can be applied for the accumulation of both presently existing data and to keeping or possession of it into a future period, whereas, data preservation connotes keeping the data which already exists in a stored form.[676] This feature also distinguishes the 'data preservation' from the 'real-time collection of data', which requires the collection or recording of data at the time of communication, or 'in real-time'.[677]

Only 'data preservation' is referred to by Articles 16 and 17 of the Convention on Cybercrime, so the collection and retention of all, or even some, data are not mandated by them, nor these articles provide for the regulation of the real-time collection of data.[678]

Azerbaijan has not established specific legal provisions regulating the expedited preservation of computer and traffic data. Nonetheless, obtaining data in a rapid manner, or in cases where it is believed that computer data is particularly vulnerable to loss or modification, can be realised in accordance with other laws. Article 10 of Law on Operative-Investigative Activity and Articles 177, 243 and 445

[673] ITU (n. 102), 260.
[674] Stein Schjolberg, *The History of Cybercrime: 1976-2014,* (Books on Demand, 2014) 118; see also, [674] European Commission, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Article 15.
[675] See for example, 1 (1)(b)(f), UK Data Retention and Investigatory Powers Act 2014.
[676] Council of Europe, *Explanatory Report to the Convention on Cybercrime* (2001), para. 151.
[677] Article 20, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[678] *Explanatory Report to the Convention on Cybercrime* (2001), para. 152.

of the Code of Criminal Procedure empower the authorities to conduct search operations and extract information from communication channels without a court decision on the basis of a reasoned decision by an authorised official of the body carrying out the search operation to prevent the commission of grave crimes against an individual, or especially grave crimes against the state security.[679] The reasoned decision by the authorised official of the body conducting the search and seizure operation on the conduct of the search operation must be submitted to the court exercising judicial supervision within 48 hours of carrying out the search and obtainment of data.[680]

Notwithstanding that digital evidence can be obtained for above purposes, this power cannot be applied for the investigation of 'cybercrimes', except the 'turnover of child pornography', if aggravating circumstances have been present.[681] This is due to the reason that the presence of any aggravating circumstance in the 'turnover of child pornography' results in the imposition of penalty consisting of deprivation of liberty for the term of up to 8 years, and thus, it qualifies as a 'grave crime'.[682] In all other cases, as noted in Chapter 4, 'cybercrimes', as identified by the relevant special part articles of the Criminal Code (Chapter 30), are regarded either as 'crimes not representing great social danger' or as 'minor crimes', depending on the type, consequences and punishments imposed.[683] Thus, investigations of 'cybercrimes' necessitate the issuance of a court order for obtaining required data, which makes the process lengthy and may result in leaving the LEAs without evidence.

However, as previously noted, an arrangement empowering law enforcement to obtain evidence has been made between LEAs and service providers, based on the powers provided by the Code of Criminal Procedure (Articles 143, 177, 243 and 445) and the Law on Operative-Investigative Activity (Article 10). According to this

[679] Articles 243 and 445, Criminal Procedure Code (2000); Article 10 (iv), Law on Operative-Investigative Activity 1999, № 728-IQ.
[680] Article 10 (v), Law on Operative-Investigative Activity 1999; Article 445, Criminal Procedure Code (2000).
[681] According to Article 171-1.2, Criminal Code (1999), for the full list of aggravating circumstances.
[682] Article 15.4, Criminal Code (1999).
[683] See Chapter 4. section 4.3.1.

agreement, mobile operators, access and other service providers can be ordered by specially appointed 'curators' to preserve data in an expedited manner, without a court order.[684] Traffic data can also be retained in accordance with bilateral agreements between the Ministry of National Security (currently the State Security Service) and service providers based on the Law on Telecommunications 2005 and the Law on Intelligence and Counter-Intelligence Activities 2004.[685] It is determined that operators, providers are obliged to promote in proper legal manner implementation of search actions, supply telecommunication nets with extra technical devices, solve organisational issues and keep methods used in the implementation of these actions as secret.[686] This requirement, however, does not generate a legal obligation for service providers to retain traffic data, as its primary concern is about enabling and assisting the LEAs in the execution of some of the procedural powers.

So, Azerbaijan has resorted to combining general investigative powers with an administrative agreement with service providers to enable LEAs to react faster and potentially increase the speed of investigative processes. Specific legal provisions, which are crucial to protect this power from being subjectively applied or misused, have not been developed yet. *Ex-ante* assessments of the proportionality of powers are also missing.

Another important factor leaving Azerbaijan only partially in line with Article 16 of the Convention is that legal or physical persons cannot be ordered to preserve data expeditiously. By contrast, to enable the competent authorities to seek the disclosure of data, the Convention requires the adoption of 'legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days'.[687]

---

[684] Cybercrime Convention Committee (T-CY), *Assessment Report. Implementation of the preservation provisions of the Budapest Convention on Cybercrime,* (2012),19; see for update; Cybercrime Convention Committee (T-CY), *Assessment Report. Implementation of the preservation provisions of the Budapest Convention on Cybercrime*. *Follow up given by Parties* (2015), 6

[685] Ibid, page 54

[686] Article 39.1, Law on Telecommunication 2005, See also, Article 17, Law on Intelligence and Counter-Intelligence Activities 2004.

[687] Article 16.2, Council of Europe Convention on Cybercrime (2001) ETS No. 185.

Consequently, Azerbaijan has taken steps to bring its legislation on criminal procedure in line with international human rights standards, and thus, can be considered to be close to implementing its procedural provisions fully in accordance with the provisions determined by the Convention on Cybercrime. However, Azerbaijan has not yet adopted specific legal provisions on expedited preservation of data in order to enhance the scope beyond operators and providers, and eliminate legal uncertainty that can lead to breach and misuse of powers by authorities. The need for expertise within a further legislative drafting exercise to ensure compliance with Articles 16 and 17 of the Budapest Convention on Cybercrime was also identified by the Council of Europe in the framework of the Cybercrime@EAP II project.[688] It can be concluded that existing incompliences and legal uncertainties create a clear risk of a serious breach of the rule of law and an invitation to breach human rights.

5.2.4 A production order for computer data

As noted in Chapter 3, the major part of the ICT infrastructure is used and owned by the private sector.[689] Thus, computer data processed and transferred across the internet are mostly controlled and stored by ISPs and other communication or web-service providers. Hence, LEAs are in a frequent need of contacting these service providers to obtain the data necessary for investigations. In this sense, coercive measures, such as search and seizure, do not seem to be feasible in most cases due to both the high-volume individual cases investigated, and disruption to legitimate business activity.[690] Therefore, less intrusive yet flexible measures are needed to balance the competing interests between the state and the private sector and individuals.

As a procedural instrument specified by the Convention on Cybercrime, a ‘production order’ can provide both this flexibility and a due legal process route in

[688] Council of Europe, ‘Workshop on reform of legislation to ensure compliance with Articles 16 and 17 of the Budapest Convention on Cybercrime’ (CyberCrime@EAP II, Baku, Azerbaijan, 13 – 15 February 2017) https://www.coe.int/en/web/cybercrime/-/eap-ii-workshop-on-reform-of-legislation-to-ensure-compliance-with-articles-16-and-17-of-the-budapest-convention-on-cybercrime
[689] See section 3.4. Chapter 3.
[690] UNODC (n. 71), 128.

obtaining digital evidence required for investigation purposes. This procedural mechanism allows LEAs to request the data required for investigation directly from suspects or service providers whose services were abused, instead of applying more intensive and coercive investigative techniques. Under Article 18 of the Convention on Cybercrime, a Party shall ensure that its competent law enforcement authorities have the power to order a person to submit specified computer data that is possessed or controlled by him and stored in a computer system or a computer-data storage medium.[691] Besides, Parties should also ensure that LEAs are provided with the power to order 'a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control' according to the Convention.[692] Simply, the production order is focused on obtaining computer data or subscriber information that is under the control or possession of a person or a service provider. Therefore, it is also important to maintain the definitions of the main concepts for the purposes of a 'production order' in national laws, such as 'subscriber information', and 'computer data' in domestic laws.

At present, the Code of Criminal Procedure does not maintain distinct cyber-specific provisions to achieve the submission of computer data or subscriber information. Instead, such orders may be possible under existing investigative powers set by Article 143 of the Code, which provides that the preliminary investigator, investigator, prosecutor or court can request from individuals and legal entities the presentation of documents and other items of significance to the prosecution. While service providers are required to cooperate with LEAs based on the Law on Intelligence and Counter-Intelligence Activities 2004 and the Law on Telecommunications 2005 to some extent, neither service providers nor individuals are legally obliged to supply computer data.[693] In addition, pursuant to the Code providing 'items, documents and samples as required by the prosecuting authority'

[691] Article 18.1(a), Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[692] Ibid. Article 18.1 (b).
[693] Article 39.1, Law on Telecommunication 2005, See also, Article 17, Law on Intelligence and Counter-Intelligence Activities 2004.

are recognised among the duties of only 'the victim'[694] and 'witnesses',[695] while 'the suspect', or 'the accused' are not bound to act.[696]

In general, LEAs apply Article 10 of the Law on 'Operative-Investigative Activities' to obtain necessary information (regardless of its type) from service providers on the basis of Articles 177, 243, 259, and 445.1.3 of the Code of Criminal Procedure, which allows the collection of information from technical communication channels and other technical means. This information can only be obtained upon adoption of the appropriate ruling by a court, except when the turnover of child pornography (in the presence of aggravating circumstances) is investigated, due to the reasons discussed in the previous section. Nor can the specially appointed 'curators' by the State Security Service order the release of computer data or subscriber information without a court order, as the administrative agreement made between the State Security Service and service providers covers only the preservation of data. Notwithstanding that there are no clear rules and procedures for obtaining traffic data also, as previously noted, LEAs rely on bilateral memoranda of cooperation with service providers on the basis of Article 39 of the Law on Telecommunications 2005 and Article 17 of the Law on Intelligence and Counter-Intelligence Activities 2004.[697]

Compared to the Convention on Cybercrime, the Code of Criminal Procedure does not differentiate between 'computer data' and 'subscriber information'. In fact, Azerbaijan has not established a legal definition for 'subscriber information', although the definition of 'computer data' for criminal law purposes is provided in domestic legislation.[698] 'Subscriber information' can be covered by 'computer data' if it is contained in the form of computer data. Noticeably, however, the Convention on Cybercrime determines 'subscriber information' as 'any information contained in

[694] Article 87.7.3, Criminal Procedure Code (2000)
[695] Ibid. Article 95.4.3.
[696] Ibid. Articles 90 and 91.
[697] See also Council of Europe, Cybercrime Convention Committee (T-CY), *Rules on obtaining subscriber information* (2014), 36.
[698] According to Article 271 of the Criminal Code 2000 computer data is used to represent 'any representation of facts, information, programs or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function'.

the form of computer data or any other form that is held by a service provider.[699] Thus, in principle, the Convention seeks to enable LEAs to request from the service providers the submission of information that is kept in both digital and non-digital form, while individuals can only be ordered to submit specified computer data, which is stored in a computer system or a computer-data storage medium.[700] Nonetheless, in Azerbaijan, both individuals and service providers can be requested by LEAs to supply data regardless of it being in a digital or non-digital form.[701]

Although Article 18 of the Convention on Cybercrime is not directly reflected in national law, in most cases service providers, especially those run by the state, will cooperate with LEAs to avoid a negative impact on their business. This can be regarded as an example of public-private partnership. At the same time, these partnerships can potentially lead to the violation of contractual obligations of service providers with customers, if the data request is not provided with a clear legal basis.[702] Since significant control and ownership of the leading ISPs are held by the State in Azerbaijan, as discussed in Chapter 3, it can be argued that those service providers will be unlikely to persist in demanding from the State an appropriate legal basis for such assistance. Thus, the privacy of customers who utilise the services provided by state-run ISPs might be sacrificed. The situation might be different with regard to partnerships with privately owned and regulated ISPs, which have their business interests and typically not subject to the same accountability standards as investigators or prosecutors. Due to their business interests, those ISPs might act more hesitantly in revealing necessary information or evidence.

It can be concluded that legal provisions regarding cyber-specific production orders have not been harmonised with the Convention on Cybercrime, notwithstanding that general procedural measures have been implemented to order the submission

[699] Article 18.3, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[700] Ibid. Article 18.1(a).
[701] Article 143, Criminal Procedure Code (2000).
[702] *ICB4PAC - Electronic Crimes: Knowledge-based Report* (Assessment) (2013), 98.

of the data necessary for investigating cybercrime cases. These measures, however, are not effective and efficient in addressing challenges posed by cybercrime before investigations, nor do they ensure legal certainty that can adequately protect against breach and misuse of powers by authorities. LEAs are obliged to respond to crimes besides protecting the rights and freedoms of individuals. Application of traditional powers for the investigation of cybercrime does not ensure the balance between those interests, as it either makes the law enforcement responses inefficient, or the rights undermined, or both. The Convention of Cybercrime does not address 'appropriate safeguards for the fundamental rights of individuals or including oversight mechanisms to ensure that these powers are not abused' and thus, mandates extensive national surveillance powers.[703]

5.2.5 Search and seizure

Search and seizure procedures are frequently used by LEAs to collect evidence with respect to specific criminal investigations or proceedings.[704] This is an active mode of investigation, which involves identifying suspects, discovering evidence, apprehending offenders, and interviewing witnesses.[705] Compared to the production order, search and seizure require the LEAs to go to the place where it is believed that the information exists in order to obtain it by seizing. Therefore, this power can be considered as more coercive and intrusive than the production order, where the person or service provider in possession of the information produces it on request.

The Code of Criminal Procedure stipulates that the investigator may search if there is a sufficient ground to suspect that a residential, service or industrial building or other place contains, or certain persons are in possession of objects or documents

[703] Ben Hayes et al. (n. 137), 28.
[704] See (n. 635).
[705] Cameron S. D. Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' (2015) 9 *International Journal of Cyber Criminology*, 66.

of potential significance to a criminal case.[706] So, 'a sufficient ground' is the threshold level of suspicion to justify the necessity of issuing a search warrant by the investigator, who is required to establish a substantial nexus between the evidence and the criminal activity. Compared to conventional searches, establishing sufficient grounds for searches in cybercrime cases might be quite challenging for investigators due to the nature of the location, that is not physical, and the involvement of intangible evidentiary materials.[707] The investigation process might be even further hindered when the evidence should be remotely obtained without physically accessing the property, or when the evidence is not in the particular residence or computer, such as in the cloud context.[708] According to the Code, the investigator can also seize the objects and documents significant for the case if it is known for sure - established on the basis of the evidence collected or the material discovered - where or in whose possession they are.[709] In this respect, this power can be regarded as being partly in line with Article 19 of the Convention on Cybercrime, which requires State Parties to empower LEAs to access or similarly search computer data contained within either a computer system or part of it, or on an independent data storage medium.

Prior to commencing a search, LEAs should ensure that all relevant applicable procedural laws are abode and that the exercise of the power will not lead to the collection of inadmissible evidence. As a rule, searches and seizures can only be conducted based on a court decision.[710] Nonetheless, in the circumstances, which admit no delay, the investigator can conduct search and seizure without court permission but only if there is precise information indicating that objects or documents concealed in a residential building constitute proof of the commission of

[706] Article 242.1, Criminal Procedure Code (2000).
[707] EC-Council, *Computer Forensics: Investigating Network Intrusions and Cybercrime* (EC-Council Press, Cengage Learning, 2017) 4; see also, Eoghan Casey (n. 495) 35-48.
[708] See David S. Wall, 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds) *The Oxford Handbook of the Law and Regulation of Technology* (Oxford: Oxford University Press 2017); Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar (n. 3) 386-421; Darren Quick, Ben Martini and Kim-Kwang Raymond Choo, *Cloud Storage Forensics* (Syngress; 1st edn, 2014) 3-8*;* Keyun Ruan, *Cybercrime and Cloud Forensics: Applications for Investigation Processes* (IGI Global, 2013) 199.
[709] Article 242.3, Criminal Procedure Code (2000).
[710] Ibid. Article 243.1.

an offence or preparations for the commission of an offence against a person or the state.[711] Compared to the Law on Operative-Investigative Activity 1999, the Code of Criminal Procedure 2000 does not limit the scope of this power only to the cases where 'grave' or 'especially' grave crimes against a person or the state are concerned. However, this power can only be exercised through inspecting certain physical areas (for example, 'a residential building'). Thus, without a court warrant, this power can be applied neither to perform an online search, nor to seize data from external servers accessed via the Internet (such as e-mail, cloud storage solutions). An e-mail message, for example, can be considered as part of a communication and therefore its content can only be obtained by applying the power of interception according to Article 259 of the Code. The Law on Operative-Investigative Activity 1999 allows obtaining such data without a court decision only in limited circumstances, such as for preventing the commission of 'grave' or 'especially grave' crimes against the state or a person. However, since most 'cybercrimes' do not qualify as 'grave' or 'especially' grave crime, as discussed in the previous section, it is necessary to issue a court warrant to obtain the evidence for investigation.

As discussed in previous sections, waiting for a court warrant to identify and collect digital evidence compromises the efficiency of criminal investigations. Moreover, the court decision limits the scope of this power through determining the place where the search or seizure is to be carried out, and the objects and documents to be seized.[712] However, it does not imply that this power cannot be extended to other objects and documents that can be of potential significance as evidence. The Code allows seizure of additional objects and documents, but only pursuant to an additional new court decision, which prolongs the procedure even more. The application of these powers to computers, which are composed of hardware and software components, might prove to be a difficult and complicated task, as these components require distinct methods and approaches in search and seizure

[711] Ibid. Article 243.3.
[712] Ibid. Article 242.1 and 243.2.

processes.[713] Another problem might arise when a seizure of computer network is required, if attainable, as this might negatively influence businesses and those not associated with the crime, as well as breach individual privacy. Fortunately, it is prohibited to disclose and use information collected during operative-investigative actions, if that information does not fit with the purposes of those actions.[714] The Code also prohibits the collection of unnecessary material for criminal proceedings.[715]

Powers for search and seizure involve collection of evidence that has already been recorded or registered. Thus, this power does not cover the real-time collection or the interception of computer data. However, the Code provides powers to intercept information sent by communication media and other technical means, and of other information.[716] These powers will be studied in the next section.

The Convention on Cybercrime also requires the State Parties to provide LEAs with further powers to address the practical problem of dealing with complex nature of computer systems and operations, the deployment of security measures and the quantity of data that can be processed and stored. Article 19(1) urges member states to adopt such legislative and other measures as may be necessary to empower LEAs 'to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of search and seizure measures'.[717] In this respect, the Code allows the investigator to request the involvement of a specialist in the facilitation of the search or seizure.[718] However, the Convention limits the scope of information given by a specialist through attaching an element of 'reasonableness'. Thus, if the assistance provided to the investigator threatens the privacy of others or other data unauthorised to be searched, then it may not be considered reasonable. As noted,

[713] Robert C. Newman*, Computer Forensics: Evidence Collection and Management* (Auerbach Publications 2007), see also, EC-Council (n. 707), 4.
[714] Article 16, Law on Operative-Investigative Activity 1999.
[715] Article 146.3, Criminal Procedure Code (2000).
[716] Ibid. Article 259.
[717] Articles 19 and 20, Council of Europe Convention on Cybercrime (2001) ETS No. 185; see also, Council of Europe, *Explanatory Report to the Convention on Cybercrime* (2001), para. 200-203.
[718] Article 244.3. Criminal Procedure Code (2000).

the Code also allows the search and seizure of the objects or documents authorised in the court decision. Failing to satisfy this requirement may render the evidence collected to be inadmissible at the trial. Moreover, according to the Code, besides the privacy of other persons, the investigator is also obliged to take measures to prevent the dissemination of any information concerning the private life of any person affected.[719]

In summary, similar to the approach adopted with respect to other investigatory powers necessary for the investigation of cybercrime, Azerbaijan seems to rely on extending its general search and seizure procedures designed to deal with search and seizure of physical objects to digital evidence rather than establishing cyber-specific powers. Thus, it becomes challenging for LEAs to investigate cybercrime as general search and seizure procedures do not provide them with required flexibility and speed. This criticism was also voiced by NGO Representative 1 and Independent Expert 1 who pointed out the requirement to pass through 'lengthy procedures' and obtain a court warrant to conduct online searches to avoid the need to enter the suspect's house to search and seize computer equipment. This option ensures better protection of individual rights and freedoms since the necessity and proportionality of search and seizure need to be assessed *ex-ante* both by the investigator and further by the court. At the same time, the activities should be carried out only in limited venues and in respect to limited objects. Thus, both speed and flexibility are undermined. Necessary speed and flexibility to ensure the effectiveness and efficiency of cybercrime investigation can be further undermined by the fact that most law enforcement officers, prosecutors, judges and lawyers in Azerbaijan are seldom aware of the characteristics of the digital world, its opportunities and challenges to be accounted for, and most of them have very limited vision on the potential impacts of the digital world on search and seizure concepts. It is, therefore, crucial to update existing procedural provisions to reflect the environment of digital evidence along with pursuing relevant awareness-raising and training campaigns to form adequate basis and resources to conduct effective and efficient prosecution and adjudication that also conforms legal rules

[719] Article 245.4, Criminal Procedure Code (2000).

and standards. Otherwise, evidence admissibility and individual rights, privacy in particular, could be simultaneously jeopardised.

5.2.6 Interception of computer data

As noted in previous sections, both production orders and search and seizure activities represent investigative measures for obtaining data that already exist in computer systems or data storage mediums, or simply, stored computer data. Due to the sensitivity, urgency, or complexity of a law enforcement investigation, LEAs may require 'real-time' collection, if digital evidence is never stored at all (existing only in the chain of communication, or related to the exchange process).[720] In this regard, the Convention on Cybercrime contains provisions on the real-time collection of traffic data and the real-time interception of content data.[721] Pursuant to Articles 20 and 21, the State parties are required to empower its competent authorities either to collect or intercept such data directly, or by compelling service providers to collect or record, or to co-operate with, and assist, the competent authorities to do so. Noticeably, the Convention distinguishes between two types of data that can be collected: 'traffic data' and 'content data'.

At present, Article 259 of the Code of Criminal Procedure enables LEAs to intercept conversations via telephone and other devices, information sent by communication media and other technical means, and other information. As a rule, these activities can be carried out on the basis of a court decision and cannot last for longer than six months. It is also made explicit that interception of such conversations and information must be carried out in accordance with Article 177.2-177.5 of the Code, which defines the right to forcibly carry out investigative procedures. Moreover, as previously noted, LEAs also apply Article 10 of the Law on Operative-Investigative Activity 2004 to obtain necessary information (regardless of the type of information) from service providers on the basis of Articles 177, 243, 259, 445.1.3 of the Code of Criminal Procedure. The Code 2000 and the Law on Operative-Investigative Activity 2004 allow the interception of such

[720] UNODC (n. 71), 130.
[721] Articles 20 and 21, Council of Europe Convention on Cybercrime (2001) ETS No. 185.

information without a court decision, however, investigation of 'cybercrime', except in the cases of 'the turnover of child pornography' (in the presence of aggravating circumstances), necessitates the issuance of a court decision, due to the reasons discussed in the previous sections. Moreover, the Code further restricts the interception of information that comprises personal, family, state, commercial or professional secrets, without a court decision, even if 'grave' or 'especially' grave crimes are investigated.[722]

Real-time collection of traffic data and interception of content data are not differentiated, and the legal framework established for interception of content data is also applied for the real-time collection of traffic data. In addition, neither the traffic data nor the content data is defined under the Code. This omission breaches legal certainty, as it is imperative to state about the exact type of communication or information to be intercepted in any decision authorising interception. However, the lack of these definitions does not exclude any of these data from being subjected to interception. In principle, the text provided by the Code enables the interception of any information sent by communication media and other technical means, and of any other information. Nevertheless, in terms of legal prerequisites for authorising an interception measure, it is important to make a distinction between the two. This distinction is important to ensure legal certainty, to limit the scope of interception and thus, to avoid the misuse of power by LEAs. In addition, the real-time collection of content data may attract the imposition of greater limitations than traffic data, as 'the privacy interests in respect of content data are greater due to the nature of the communication content or message'.[723]

Execution of this power by LEAs encounters specific difficulties. As discussed in Chapter 3, offenders apply various tactics to conceal their identities, such as using fake emails and spoofed IP addresses, proxy servers, anonymous communication servers, public Internet terminals or open wireless networks. If perpetrators use these tactics, LEAs remains largely unable to analyse the data and identify the communication partners successfully. Besides, the Code of Criminal Procedure

[722] Article 259.3. The Criminal Code (1999).
[723] *Explanatory Report to the Convention on Cybercrime* 2001, para. 210.

requires the inclusion of 'the family name, first name, father's name and exact address of the person(s) whose information or conversations are to be intercepted' in the court warrant. Thus, the application of general interception tactics for cybercrime investigation becomes ineffective and inefficient. In addition, an investigation of cybercrimes becomes even more conscientious and time-consuming where the computer data that must be 'cracked' before they become legible because they are protected by openly and widely available, easy-to-use software tools and encryption technologies.[724] The Code does not set explicit rules for handling the cases where de-encryption is needed. Moreover, according to Article 304 of the Code, if the accused goes into hiding and his whereabouts is unknown, the proceedings in the criminal case must be suspended.

Ensuring the confidentiality of the investigation is another crucial element to be satisfied while exercising this power. The Convention obliges the Parties to compel a service provider to keep confidential the fact of and any information about the execution of this power,[725] without further providing additional clear legal instruments ensuring the protection of privacy rights against the misuse of surveillance powers. As regards to cooperation between LEAs and ISPs, the bilateral memoranda on cooperation with service providers on the basis of Article 39 of the Law on Telecommunications 2005 and Article 17 of the Law of the Law on Intelligence and Counter-Intelligence Activities 2004 can partially serve as a guarantee for satisfying this requirement. In practice, as noted before, in most cases service providers, especially those run by the state, will also tend to involve in the cooperation with LEAs to avoid a negative impact on their business. Given the manifest disagreement among service providers in many jurisdictions concerning the legal process that LEAs must follow to obtain data,[726] stricter and more transparent rules need to be established to reach a balance between individual rights and the surveillance powers.

[724] Majid Yar (n. 161)*;* see also: Michael Cross and Debra Littlejohn Shinder (n. 240) 518-524.
[725] Articles 20.3 and 21.3, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[726] Cameron S. D. Brown (n. 705), 68.

Consequently, compared to the procedural powers and instruments analysed in previous sections, provisions established for intercepting computer data seems to be more focused. However, there are certain safeguards attached to the implementation of this power that makes it ineffective and inefficient in dealing with cybercrime in practice. Therefore, it is crucial to develop more cyber-specific rules to ensure a better balance between individual rights and freedoms, and investigative measures, which does not compromise any of them, as was also suggested by NGO Representative 1 and Independent Expert 1 during the interview.

5.2.7 Conclusion

Grounded in the foregoing analysis of the procedural powers, laws and the results of interviews, it can be claimed that procedural measures applied in Azerbaijan are insufficient for dealing with the growing number of cybercrime cases. Azerbaijan lacks specific legal provisions regulating digital/electronic evidence. Digital evidence has not been scrutinised, analysed or thoroughly understood, and comprehensive national guidance to be followed when dealing with digital evidence has not been developed in the country.

It has also become evident that, in theory, the protection of human rights and liberties has been given a priority when balanced against the requirements of law enforcement. However, national powers and procedures have not directly incorporated the principle of proportionality, although the laws have made it clear that relevant powers or procedures cannot be excessive compared to the nature and circumstances of the offence.

Cyber-specific procedural powers have not been developed, so the country still heavily relies on extending the application of its general procedural powers to the prosecution and adjudication of cybercrime cases. These ‘offline’ procedural powers have not been developed for application in the virtual environment and therefore, pose substantial problems for prosecution and adjudication.

In addition, the Council of Europe Convention on Cybercrime provisions on evidence and procedures have been left largely unattended. Given that the Convention provides minimum settings necessary for the investigation and prosecution of cyber offences, it is suggested that criminal procedure laws of Azerbaijan should be brought in line with the Convention. This would also ensure the consistency of the responses of the country to cybercrime and enable the LEAs to carry out fair, effective and efficient investigations.

5.3 International cooperation

As discussed in Chapters 2 and 3, cybercrime easily traverses geographical borders and elude state control. However, cybercrime is by no means the first and the only type of criminality that can transcend state borders and pose challenges for investigation and eventual prosecution. Over the past decades, global responses have been required to fight against other forms of transnational crimes, such as illicit drug and firearm trafficking, terrorist activities, theft of art and cultural objects, commercial sex and human trafficking, maritime crime and piracy, and money laundering.[727] Nonetheless, cybercrime poses unique challenges for national criminal justice systems, due to the wide global dispersion of evidence, offenders, and victims, as well as rapidly growing demand of technical expertise necessary for its investigation and prosecution.[728]

Cybercrime is commonly perceived as incorporating a 'transnational dimension', as was also suggested by Parliament Officer 1 and NGO Representative 1 during interviews. It is, therefore, important to elaborate what is meant by cybercrime acts

[727] See for further discussion on other crimes such as international terrorism, drug trafficking, human trafficking and migrant smuggling, illicit trafficking of firearms, maritime crime and piracy, money laundering and etc; United Nations Office on Drugs and Crime, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (United Nations, 2010); Aniceto Masferrer and Clive Walker, 'Countering Terrorism and Crossing Legal Boundaries' in Aniceto Masferrer and Clive Walker, *Counter-Terrorism, Human Rights and The Rule of Law* (Cheltenham: Ed. elgar, 2013); Frank G Madsen, *Transnational Organized Crime* (London: Routledge, 2010).

[728] Susan W. Brenner, *Cyberthreats and the Decline of the Nation-State* (Routledge, Taylor & Francis Group 2014) 9-22; Thomas J Holt, Adam M Bossler, *Cybercrime in Progress: Theory and prevention of technology-enabled offenses* (Routledge 2016) 106-136.

containing ‘transnational dimensions’. According to the United Nations Convention against Transnational Organised Crime, an offence is ‘transnational in nature’ if:

> ‘(a) it is committed in more than one state; (b) it is committed in one state but a substantial part of its preparation, planning, direction or control takes place in another state; (c) it is committed in one state but involves an organised criminal group that engages in criminal activities in more than one state; (d) it is committed in one state but has substantial effects in another state.’[729]

Notwithstanding that important features have been captured by this approach, it does not appear to be completely relevant to cybercrime acts, as ‘organised criminal groups’ are not central to cybercrime acts, and the transnational ‘dimension’ may arise in a way that does not amount to ‘preparation, planning, direction or control’ within another state.[730] At its simplest, transnational crime can be described as criminal phenomena transcending borders and transgressing the laws of several states or having actual or potential trans-boundary effects of national or international concern.[731] Thus, cybercrime can be considered a typical transnational crime, since, in most cases, it affects and involves different jurisdictions. In practice, the percentage of cybercrime acts involving a ‘transnational element’ is generally high, according to a UN study,[732] and Azerbaijan is no exception to this, as many cybercrime acts reported to and investigated by LEAs (LEAs) also involve transnational dimensions.[733]

The transnational nature of cybercrime necessitates cooperation between various LEAs, both within a country and across geographical borders, through sharing their

---

[729] Article 3.2, *United Nations Convention against Transnational Organized Crime* (2000).
[730] UNODC (n. 71), 188; see also, Anita Lavorgna, ‘Cyber-Organised Crime. A Case of Moral Panic?’ (2018) *Trends in Organized Crime*. 1-18.
[731] See for further discussion, Gerhard O.W. Mueller, ‘Transnational crime: Definitions and Concepts’, in P. Williams and D. Vlassis (Edn), *Combating Transnational Crime* (Portland, Oregon: Frank Cass publishers, 2001) 13; Neil Boister, ‘Transnational Criminal Law?’ (2003) 14 *European Journal of International Law*, 954.
[732] According to a study conducted by United Nations Office on Drugs and Crime, percentage of cybercrime acts involving a transnational dimension was over 70% in responded European countries.
[733] See Section 2.4, Chapter 2.

data or intelligence.[734] This section is therefore devoted to the analysis of key principles and provisions related to international cooperation in Azerbaijani laws with reference to the Convention on Cybercrime. Before embarking on the analysis, it is also important to elaborate what is the established jurisdiction over the criminal offences enumerated in the national laws of Azerbaijan, since cybercrime has given rise to complex jurisdictional issues and triggered an increase in concurring or competing jurisdictional claims.

5.3.1 Jurisdiction

The jurisdiction of a state mainly refers to the power of a sovereign state to regulate, adjudicate and enforce certain norms.[735] In the context of cybercrime prosecution and investigation, 'jurisdiction' may be understood as the legal authority of a state to enforce its domestic law.[736]

The most common determinant incorporated in jurisdiction provisions is the location of the criminal act, which is also specified as the primary constituting factor of jurisdiction by the Convention on Cybercrime.[737] The jurisdiction clause contained in Article 22 of the Convention recognises the principle of territoriality through obliging Parties to exercise jurisdiction over any offence established in accordance with the Convention when the offence is committed within the state's geographical territory.[738] In addition, States Parties are required to establish criminal jurisdiction over offences committed upon ships flying its flag or aircraft registered under its laws.[739]

Similar to the Convention, the Code of Criminal Procedure and the Criminal Code contain jurisdictional clauses that recognise this principle. Pursuant to Article 11 of

---

[734] Mark Walport (n. 643) 76

[735] See e.g., United Nations Report of the International Law Commission, 58th session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, 517; see also, Bernard H. Oxman, 'Jurisdiction of States', in Rudolf Bernhardt, *Encyclopedia of Public International Law*, vol. 3 (Amsterdam: Elsevier Science Publishers, 1997) 55; Ian Brownlie, *Principles of Public International Law* (6th ed. Oxford: Oxford University Press, 2003) 297.

[736] Henrik Kaspersen, *Cybercrime and Internet Jurisdiction* (Council of Europe, 2009) 5-6,

[737] Susan W. Brenner, Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4 *Journal of High Technology Law*, 10

[738] Article 22 (1)(a), Council of Europe Convention on Cybercrime (2001) ETS No. 185.

[739] Ibid. Article 22 (1)(b)(c),

the Criminal Code, a person who committed a crime in the territory of the Republic of Azerbaijan is subject to the criminal liability under the Criminal Code. Throughout the territory of the Republic, as well as upon ships flying its flag, or aircrafts registered under its laws, only the legislation of the Republic of Azerbaijan on criminal procedure shall be applied, unless otherwise prescribed by the international treaties to which the country is a signatory.[740] It is further determined that the crime, which has been initiated, proceeded, or completed in the territory of the country shall be admitted as a crime committed in the territory of the Republic of Azerbaijan.[741] This provision reflects the idea that in order for the country to assert territorial jurisdiction, it is not necessary for the whole offence to take place within the country. To put it differently, the application of territorial jurisdiction does not require all elements of the crime to occur within the territory of the state. This approach has also been supported in the Explanatory Report to the Convention on Cybercrime. It clarifies that under the territoriality principle, a party can also assert territorial jurisdiction if the computer system attacked is within its territory, even if the attacker is not, in addition to the cases where the person is attacking a computer system and the victim system, are located within its territory.[742]

The place of impact of crime has long been regarded as one of the constituent elements of the offence in the criminal context.[743] As stated by Ryngaert, 'international law seems to have satisfied itself with the requirement that either the criminal act or its effects have taken place within a State's territory for the State to legitimately exercise territorial jurisdiction'.[744] This is also reflected in the Criminal Code, which provides that foreign citizens and stateless persons, who committed a crime outside the territory of the Republic of Azerbaijan against its citizens or interests, can be subjected to criminal liability if these persons have not been convicted in the foreign state.[745] Thus, indictments can also be issued by

[740] Article 3, Criminal Procedure Code (2000).
[741] Article 11, Criminal Code (1999).
[742] Council of Europe, *Explanatory Report to the Convention on Cybercrime*2001, para. 233.
[743] See for example, the *SS Lotus (France v Turkey)* [1927] PCIL Reports, Series A No. 10, [55].
[744] Cedric Ryngaert, *Jurisdiction in International Law* (Oxford: Oxford University Press, 2nd edn, 2015) 78.
[745] Article 12.2., Criminal Code (1999).

Azerbaijani LEAs where the crime result or effect was within its territory, but the conduct and location of the offender were extra-territorial. However, enforcement of this provision seems quite challenging and might generate an issue of concurrent jurisdiction on a previously unseen scale. More importantly, both the national laws and the Convention on Cybercrime largely neglect the issue of jurisdictional concurrency. Therefore, more straightforward and clear solutions are needed for eliminating existing ambiguities and complexities in jurisdictional concurrencies. Otherwise, as stated by Kohl, 'territorially focused criminal law is … moving towards a tipping point, albeit not because it is too refined, but because it is fair neither on individuals nor on states'.[746]

The nationality of the perpetrator is widely recognised as the second major constituting factor of jurisdiction in cybercrime cases after territoriality.[747] The principle of nationality is also incorporated in the Convention – requiring the Parties to ensure jurisdiction when the act has been committed 'by one of its nationals if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State'.[748] Azerbaijan has a comparable clause with a requirement of dual criminality and the so-called '*ne bis in idem*'[749] principle. Article 12 of the Criminal Code specifies that the citizens of the Republic of Azerbaijan who committed crime outside its territory as well as stateless persons permanently residing in the country shall be subjected to criminal liability under the Criminal Code, if this action is recognised as a crime in the Azerbaijan Republic and in the state on the territory in which it was committed, and if these persons were not convicted in the foreign state.

In the context of cybercrime, the principle of nationality can be viewed as being less relevant, because cybercrime does not require the perpetrator to leave a country to commit it abroad. Arnell, however, argues that the nationality jurisdiction

[746] Uta Kohl, *Jurisdiction and the Internet* (1st edn, Cambridge: Cambridge University Press 2007) 106.
[747] Susan Brenner and Bert-Jaap Koops (n. 737), 24.
[748] Article 22 (1)(d), Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[749] *Ne bis in idem* principle has been described as a fundamental principle of law, which restricts the possibility of a defendant being prosecuted repeatedly on the basis of the same offence, act, or facts. See for further information, Bas van Bockel, *The Ne Bis In Idem Principle in EU Law* (1st edn, Austin: Wolters Kluwer Law & Business, 2010) 2-7.

should be placed alongside territoriality as a general basis of criminal jurisdiction, as the existing territorial jurisdictional scheme is inadequate due to the declining importance of borders, and thus, territory for the purposes of jurisdiction, because of the growing ability of individuals to commit crimes remotely.[750] These factors seem to be of practical relevance in defending the importance of the nationality principle from the enforcement perspective. At the same time, it is the collective interest of individuals in having a criminal law system in force which explains the state's normative power to punish, and the inhabitants of a state may feel horrified by a particular crime committed outside its territory by a co-national, but these offences do not always undermine their belief in the criminal law system under which they live.[751] Simply, it can be argued that unless the state's interests are affected, the government might be uninterested in its citizens' actions abroad and may wish to avoid the inconvenience of prosecution that will inevitably involve complex and costly mutual legal assistance. Therefore, Brenner suggests that in the cybercrime context, perpetrator's nationality should operate as 'a factor that militates against, rather than for, the assertion of jurisdiction'.[752]

Analysis of the two major constituting factors of jurisdiction shows that jurisdiction over a particular cybercrime offence can be asserted by more than one country. It can be suggested that in the realm of cybercrime, jurisdictional disputes will arise even at a faster pace in the near future, as the cyberspace and the internet architecture have provided States with the ability to conduct investigation extraterritorially and thus, claim jurisdiction over a wide range of offences. Therefore, it is necessary to develop specific legislation. However, such legislation is lacking in Azerbaijan. Article 22 of the Convention on Cybercrime provides a mechanism for consultation in this regard. According to the Convention, in order to facilitate the efficiency and fairness of the proceedings, when more than one Party claims jurisdiction over an alleged offence, the affected State Parties should consult with a view to determining the most appropriate jurisdiction for

[750] Paul Arnell, 'The Case for Nationality Based Jurisdiction' (2001) 50 *International & Comparative Law Quarterly*, 955–962.
[751] Alejandro Chehtman, *The Philosophical Foundations of Extraterritorial Punishment* (1st edn, Oxford: Oxford University Press, 2010) 60-61.
[752] Susan W. Brenner, 'Cybercrime jurisdiction' (2006) 46 *Crime, Law and Social Change,* 202.

prosecution.[753] This is not an absolute obligation but is to take place 'where appropriate' and thus, a party may delay or decline consultation if it is believed to impair its investigation or proceedings.[754]

It is noticeable that the Convention does not provide concrete criteria for solving jurisdictional concurrencies in cybercrime cases. Nor does it provide guidance on how and when several parties can or should claim jurisdiction over the same offender or offence.[755] It has been suggested that a mechanism of prioritising jurisdiction claims is still feasible, notwithstanding that factors to be considered in prioritizing jurisdictional claims, such as place of commission of the crime, custody of the perpetrator, harm, nationality, strength of the case against the perpetrator, punishment, fairness and convenience seem to have lost some applicability to the Internet.[756]

5.3.2 Cooperation provisions and mechanisms

As previously noted, transnational cybercrimes necessitate cooperation of LEAs in the different countries involved. Formal mechanisms, such as mutual legal assistance and extradition, can be utilised by LEAs along with informal ways (such as 24/7 networks) to support this purpose. The Convention on Cybercrime contains a number of provisions related to extradition and mutual legal assistance among the State Parties, although these provisions are very slow and difficult to apply in practice, due to their bureaucratic features. Therefore, in most cases, using informal cooperation makes more sense, as it is faster, particularly as an investigation unfolds. In this regard, a friendly political atmosphere and pre-existing relationships between countries (and more so between operational staff) can be

[753] Article 22 (5), Convention on Cybercrime, (2001); see also, *Explanatory Report to the Convention on Cybercrime*, para. 239.
[754] Ibid.
[755] Susan W. Brenner, 'Cybercrime jurisdiction', (2006) 46 (4) Crime, Law and Social Change, pp. 189-206, 197.
[756] Henrik Kaspersen, *Cybercrime and Internet Jurisdiction*, (Council of Europe, 2009) 25; For 'factors to be considered in prioritizing jurisdictional claims' See Susan W. Brenner (n. 752), 189-206.

considered as significant factors in the cooperation against cybercrime.[757] Investigations can be complex and murky if authorities in another country are not inclined to cooperate and thus, even where parties are obliged to cooperate based on a treaty or formal agreement, bureaucratic procedures, delay, and a search for an exception may cause matters to grind a halt.[758] Therefore, reliance on informal relationships with other countries might be not highly promising for Azerbaijan, as the country is still in the early phases of the development of multilateral and mutually productive working relationships with other countries.

Notwithstanding its bureaucratic features, the Convention on Cybercrime can be regarded as being innovative in many respects, particularly in providing foundational provisions relating to cooperation among the countries against the cybercrime. The Convention addresses the growing significance of international cooperation in Articles 23 to 35. Before starting to test whether Azerbaijan is in line with those articles, it is important to note that cyber-specific legislation on international cooperation has not been passed in Azerbaijan. Although existing laws on international cooperation are not cyber-specific, extradition and mutual legal assistance in general criminal matters are covered. The Convention provides that co-operation must be carried out both 'in accordance with the provisions of this Chapter (Chapter III of the Convention)' and 'through the application of relevant international agreements on international cooperation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws'.[759] According to the general principle established by the latter clause, the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition.[760] Consequently, separate general regimes on mutual assistance and extradition are not intended to be created by the Convention. Thus, parties are required to establish a legal basis for enabling the international cooperation as defined by the

[757] James Sheptycki, *In Search of Transnational Policing*. *Towards a Sociology of Global Policing* (Ashgate, Burlington 2002).
[758] Russell G Smith, Peter N Grabosky and Gregor Urbas, *Cyber Criminals on Trial* (Cambridge University Press 2004) 57.
[759] Article 23, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[760] Council of Europe, *Explanatory Report to the Convention on Cybercrime (*2001) para. 244.

Convention only in those cases where such provisions are not contained in the existing treaties, laws and arrangements.[761]

In Azerbaijan, international cooperation, particularly mutual legal assistance (MLA) and extradition related measures, is primarily based on signed bilateral and multilateral agreements. The country has signed and ratified the European Convention on Mutual Assistance in Criminal Matters (1959), which sets out rules for the enforcement of letters of request by the authorities of a Party ('requested Party') aiming to procure evidence or to communicate the evidence (records or documents) in criminal proceedings undertaken by the judicial authorities of another Party ("requesting Party").[762] In addition, Azerbaijan has become a signatory to the United Nations Convention against Transnational Organised Crime 2000, which also contains significant tools for international cooperation.[763] The Law on Mutual Legal Assistance on Criminal Matters 2001 incorporates the provisions of the Convention and constitutes the primary legal basis for handling MLA requests, alongside with the Criminal Procedure Code (Chapter LVII). In addition, Azerbaijan has officially recognised partnerships on mutual assistance in criminal matters with Russia, China, India, Bulgaria, United Arab Emirates, Georgia, Iran, Kirgizstan, Lithuania, Morocco, Moldova, Uzbekistan and others.[764] Furthermore, the country has signed and ratified the European Convention on Extradition 1957 and its two Additional Protocols.[765] Extradition cases are governed in accordance with these international treaties, the Law on Extradition, adopted in 2001, and the Criminal Procedure Code (Chapter LVII). However, none of the instruments or partnerships mentioned in this paragraph has been particularly designed for addressing cybercrime related issues. Nor do these instruments provide specific

[761] ITU (n. 102) 287.

[762] Council of Europe, European Convention on Mutual Assistance in Criminal Matters, CETS No.030, 1959, Azerbaijan has signed the Convention since 07/11/2001 and ratified since 04/07/2003.

[763] UN General Assembly, United Nations Convention against Transnational Organized Crime, 2000, Azerbaijan has signed the convention since 12/12/2000, and ratified since 30/10/2003.

[764] The full list and the content of the agreements are available online at, http://www.justice.gov.az/images/toplu-2014.pdf.

[765] European Convention on Extradition (1957) ETS 024; Additional Protocol to the European Convention on Extradition (1975) ETS 086; Second Additional Protocol to the European Convention on Extradition, ETS 098, 1978. All were signed by Azerbaijan in 07/11/2001 and ratified in 28/06/2002.

provisions dealing with urgent requests to preserve data. However, it does not mean that extradition and MLA related legal instruments are completely irrelevant for cybercrime cases.

As for extradition, Article 24 of the Convention on Cybercrime, which is grounded on the principle of dual criminality, specifies that the obligation to extradite applies only to offences established that are punishable 'by deprivation of liberty for a maximum period of at least one year or by a more severe penalty'. Azerbaijan is in line with Article 24 of the Convention, given that the dual criminality principle is clearly incorporated in the national law,[766] and the Law has provided the same threshold for extradition on the Law on Extradition 2001 for any crimes. Pursuant to Article 2.1 of the Law on Extradition, extradition shall be granted in respect of offences punishable under the laws of the requesting country and of its own by deprivation of liberty or under a detention order for a maximum period of at least one year or by a more severe penalty.

As regards MLA measures, general MLA provisions contained by Article 2 of the Law on Mutual Legal Assistance on Criminal Matters 2001, which is the reflection of Article 18 of the United Nations Convention against Transnational Organised Crime 2000, seem to be relevant for cybercrime investigations, since the Convention on Cybercrime has contained similar regulation. Article 2.3 of the Law on Mutual Legal Assistance on Criminal Matters 2001 provides a complex list of possible specific MLA related actions ranging from obtaining evidence or statements to determining criminally obtained income, property, and means for committing a crime.[767] Although, specific wording relating to computer data or information related requests are not contained in the Law, 'other actions taken in accordance with national legislation of the Republic of Azerbaijan' further open the provision to other data-related requests.[768]

To ensure immediate assistance for criminal investigations and the collection of electronic evidence, it is required by the Convention that the state parties to 'afford

[766] See Article 12, Criminal Code (1999); see also Article 2.1. Law on Extradition 2001. № 132-IIQ.
[767] For the full list of possible actions sought, see Article 2.3., Law on Mutual Legal Assistance on Criminal Matters 2001.
[768] Ibid. Article 2.3.11.

one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings'[769] and 'to designate a contact point 'available on a twenty-four hour, seven-day-a-week basis'.[770] As discussed in Chapter 3, besides the relevant units and departments operating within Prosecutor General's Office and the Ministry of Justice, a 24/7 point of contact has been created under the Department of Combating Crimes in Communications and IT Sphere, State Security Service, to provide specialised assistance, order the expeditious preservation of computer data or traffic data, after getting court decision the seizure of objects containing data and perform or facilitate the execution of procedural documents. The Department has the competence to order the preservation of data, and therefore, immediate orders can be made if requested by foreign contact point regarding the preservation of data, which potentially speeds up communication and investigation. Moreover, the Department is also authorised to carry out investigations right after receiving requests. So, the combination of these two functions under the same department makes it possible 'to converge the speed of international investigations to the level reached within national investigations'.[771] It can be concluded that, in addition to Article 35 of the Convention on Cybercrime, the law of Azerbaijan can also be considered to be in line with Article 27 as well, which obliges the Parties to designate 'a central authority or authorities' for mutual legal assistance requests that communicate directly with each other.

However, problems arising from discrepancies between legal systems and time issues (multi-layered steps and duration of the procedures (steps)) are still present, which makes it difficult to deliver extensive co-operation or to 'minimise impediments to the smooth and rapid flow of information and evidence internationally'.[772] All expedited forms of communication, including fax, email or other online systems, are accepted and used to request, for example, stored computer data by mutual assistance. In this regard, the country can be considered

[769] Article 25, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[770] Ibid. Article 35.
[771] ITU (n. 102), 293
[772]See for the procedure followed by other countries: The Cybercrime Convention Committee (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime (*2014), 61-81.

to be in line with Article 25 of the Convention on Cybercrime, which obliges the requested Party to 'accept and respond to the request by any … expedited means of communication (including fax or e-mail)' in urgent circumstances. Moreover, requests are accepted in three languages - English, Turkish or Russian, to speed up the investigations.[773]

At the same time, there are still lengthy and time-consuming procedures to be followed. For example, after receiving a request to preserve data in an expedited manner, the 24/7 point of contact examines the request (reciprocity, interests of national security etc.), then sends it to the Head of General Directorate for Combatting Transnational Organised Crimes who approves execution and forwards it to Cybercrime Unit which interacts with ISP.[774] This is the procedure to be followed only for the requests to preserve the data. However, prior to collecting and transmitting the data a formal MLA request is required. In order to process the MLA request as a requested State, the following procedures must be followed. 1) The central authority should receive the request. 2) The central authority should request the court decision to obtain data. 3) The central authority should obtain data from ISP's after the court decision. 4) After internal procedures, the central authority should send the data to the requesting state.[775]

MLA requests, on the one hand, as a legal process, can be considered as the most resilient way of obtaining data, given that it can tie together the laws of interacting countries and make the process legally robust throughout all stages. However, MLA is not completely fit for purpose in contexts involving requests for digital

[773] Whereas, according to Article 16, Law of Azerbaijan Republic on Legal Assistance in Criminal Matters (2001) documents submitted with regard to legal assistance shall be translated into Azeri or with consent of Ministry of Justice into one of official languages of United Nations; see also the Cybercrime Convention Committee (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime* (2014) 42.

[774] The Cybercrime Convention Committee (T-CY*), Assessment report*: *Implementation of the preservation provisions of the Budapest Convention on Cybercrime (*2012) 20. See also, Council of Europe, *Revised Assessment Report (2018) on International cooperation on cybercrime in the Eastern Partnership region* (Cybercrime Programme Office, Cybercrime@EAP 2018 Project, 2018) 13.

[775] Cybercrime Convention Committee (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime* (2014), 63.

information and evidence needed to investigate criminal activities.[776] As a form of international cooperation mechanism, it is quite cumbersome, inappropriately slow and ponderous in the digital context, as well as bureaucratic, unresponsive, and therefore, inefficient, which causes delays in the prosecution and investigation of cybercrime cases. For example, the UN Cybercrime Study (2013) found that use of formal cooperation mechanisms occurs on a timescale of months, rather than days, given that most countries 'reported median response times of ... 150 days for mutual legal assistance requests, received and sent'.[777] It is especially challenging to get a positive outcome in Azerbaijan from MLA requests, where, as broadly discussed in section 5.2., enforcement of all data-related procedural powers necessary for the investigation and prosecution of cybercrime requires a court order (except for the preservation of data, and except when the 'turnover of child pornography' (in the presence of aggravating circumstances) is investigated). Consequently, significant challenges are created by long cooperation response times also due to the volatility of electronic evidence.[778] It is, thus, worth considering the establishment of detailed arrangements to speed cooperation processes up. Specific recommendations are provided in the next chapter.

The government does not publicise statistics on the number of requests received and sent by Azerbaijan's 24/7 contact point as well as information about response times. According to the Revised Assessment Report (2018) prepared by the Cybercrime Programme Office of the Council of Europe, the number of 24/7 requests went from zero requests processed to 15 received and 25 sent in the years 2015-2017 compared to five-year period before.[779] As regards the MLA requests, only about 4-5 requests per year were sent or received by Azerbaijan, according to the Assessment Report prepared by the Cybercrime Convention Committee (T-CY) in 2012. A substantial change on the number of sent or received

[776] David P. Fidler, 'Cyberspace, Terrorism and International Law' (2016) 21 *Journal of Conflict and Security Law*, 490.
[777] UNODC (n. 71), 206.
[778] Ibid. 214.
[779] Council of Europe, *Revised Assessment Report (2018) on International cooperation on cybercrime in the Eastern Partnership region* (Cybercrime Programme Office, Cybercrime@EAP 2018 Project, 2018) 11.

MLATs on cybercrime was not observed in Azerbaijan for the years 2015-2017, as only 2 MLATs were received and 7 MLATs were sent during that period.[780] Considering that the Convention on Cybercrime even further extends MLA provisions by requiring the Parties to afford one another mutual assistance for the collection of evidence in electronic form of any criminal offence (not only cybercrime offences),[781] there seems to be a clear indication of underutilisation of MLATs and 24/7 networks by Azerbaijani LEAs. Although statistics about the number of reported cybercrimes are not currently available, it seems that there is an inconsistency between the total number of MLAs and 24/7 requests and the total number of cybercrime cases encountered by LEAs. Pursuant to the study conducted by United Nations, countries typically reported an average of almost 1,000 cybercrime cases per year,[782] and given that most cybercrime acts reported and investigated by Azerbaijani LEAs involve transnational dimensions,[783] the number of requests processed through 24/7 point of contact should have been higher than the reported number. The investigation and prosecution of most transnational cybercrime cases could have been mostly unsuccessful due to the limited use of this mechanism.

The cooperation with 'foreign' private service providers has also been extremely low. According to the transparency reports published by major service providers - Apple, Facebook, Google, Microsoft, Twitter and Yahoo – Azerbaijan LEAs did not send any request for data to Apple, Google, Microsoft, Twitter and Yahoo, while only 1 request for data was received by Facebook in 2017.[784] By comparison, more than 70000 requests were sent from the UK to these service providers in 2017, and the providers met most requests. It can be contended that in Azerbaijan LEAs do not or cannot utilise the MLA related mechanisms available to them properly,

[780] Ibid.
[781] Article 25, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[782] UNODC (n. 71), 213.
[783] See Chapter 2. Section 2.4.
[784] For Transparency reports see: Apple http://www.apple.com/privacy/transparency-reports/; Facebook https://transparency.facebook.com/government-data-requests/country/AZ; Google https://transparencyreport.google.com/user-data/overview?hl=en; Microsoft https://www.microsoft.com/en-us/about/corporate-responsibility/lerr; Twitter https://transparency.twitter.com/; Yahoo https://transparency.oath.com/.

although they have been enabled to receive and execute MLA requests both from legal and technical perspectives. However, the dominance of US companies as global providers of cyber services, particularly those discussed above, and restrictions US law imposes on the companies sharing content data with foreign governments should also be accounted for.[785] So, in addition to the shortage of resources in Azerbaijan, the lack of a friendly political atmosphere and pre-existing relationships between the US and Azerbaijan, as well as discrepancies between the legal systems compound this problem.

The Convention on Cybercrime provides mutual assistance regarding provisional measures in Articles 29-33, which reflect procedural instruments contained by Articles 16-21. As discussed in section 5.2, a number of procedural instruments designed by the Convention to be applied at the national level for investigating and prosecuting cybercrimes, such as production order, as well as expedited preservation, search and seizure, real-time collection and interception of data. In addition, LEAs are also enabled and obliged, to apply these procedural instruments on request of their foreign counterparts in accordance with the provisions contained by Articles 29-33. Thus, enforcement of these provisions and outcomes of requests remain almost completely dependent on the requested state's capacity and legal framework. With regard to MLA related provisional measures contained by the Convention, it can be argued that Azerbaijan is partially in line with Articles 29-33. Notwithstanding that specific procedural powers to be applied in 'cyberspace' have not been developed yet and the country heavily relies on extending its 'traditional' procedural powers to cybercrime cases, existing powers enable LEAs to receive and execute MLA requests. More precisely, the same powers, discussed in section 5.2., apply for the enforcement of international requests. By contrast, international requests are processed on the basis of the Law on Mutual Legal Assistance on Criminal Matters 2001, United Nations Convention against Transnational Organised Crime, European Convention on Mutual Assistance in Criminal Matters, which provide similar regulations to those contained by the Convention on Cybercrime.

[785] David P. Fidler (n. 776), 490.

5.4 Conclusion

The existing regime of laws does not provide LEAs with effective and efficient powers and instruments in investigating and prosecuting cybercrime. Azerbaijan has not developed specific procedural rules to be applied in 'cyberspace' and heavily relies on extending its general procedural powers crafted for physical space and context to cybercrime cases. Although granted, these 'offline' procedural powers are proving to be largely ineffective and inefficient for the virtual environment and therefore, pose significant problems before enforcement and jeopardise expediency and individual privacy at once. This was also supported by all the interviewees, notwithstanding the specificities of the problem were not thoroughly presented.

In general, the country has not harmonised its procedural laws with the Convention on Cybercrime. Notwithstanding that the Convention itself does not seem to be fully appropriate in dealing with cybercrime, it provides minimum settings necessary for the investigation and prosecution of criminal offences committed via computer systems both at national and international level. The Convention can also be regarded as being innovative in providing foundational provisions relating to cooperation among the countries against the cybercrime. Having discussed in Chapter 4 that Azerbaijan brought its substantive criminal laws in line with the Convention on Cybercrime, it can be argued that this process needs to be followed by the harmonisation of the rules of criminal procedure and international cooperation related instruments to ensure the consistency of its responses to cybercrime and enable the LEAs to conduct effective and efficient investigations. Otherwise, extending the application of general investigative and cooperation related powers to prevent and combat cybercrime will continue to be counter-productive, and since the right tools are not put in place, LEAs may operate beyond the law out of necessity.[786] It is, thus, crucial to develop the procedural instruments in a way that does not interfere with individual rights of the suspect, and other participants of criminal proceedings. However, the measures undertaken to protect

[786] Ben Hayes et al. (n. 137), 51.

these rights and freedoms should not lead to the ineffectiveness and inefficiency of powers.

As regards international cooperation against cybercrime, countries have become more dependent on each other's legal framework and technical capabilities due to the importance and necessity of cooperating against cybercrime. However, there is a lack of procedural harmonisation in criminal justice systems worldwide, which makes it even more challenging to enforce investigation and particularly, cooperation related mechanisms and Azerbaijan is no exception in this regard. Although, being quite cumbersome, inappropriately slow and ponderous in the digital context, Mutual Legal Assistance was considered as the most resilient way of obtaining data since it can tie together the laws of interacting countries and make the process legally robust at all stages. Azerbaijani LEAs have been enabled to receive and execute cooperation requests both from legal and technical perspectives to some extent. However, they have not been keen on utilising the MLA related mechanisms available to them to the widest extent possible due to various factors, such as the lack of informal cooperation channels and staff that possess the technical and legal skills. Also, delivering extensive co-operation was found to be challenging because of the problems arising from discrepancies between legal systems, time issues (multi-layered steps and duration of the procedures (steps)).

Consequently, Azerbaijan should focus on developing adequate procedural laws and cooperation mechanisms so that cybercrime cases are appropriately investigated, prosecuted and adjudicated. Specific recommendations and blueprints to address the challenges emphasised in this Chapter are presented in Chapter 6.

CHAPTER 6: Enhancing Responses to Cybercrime in Azerbaijan

6.1 Introduction

In the preceding Chapters, the policy and legal responses of Azerbaijan to cybercrimes were analysed, and the deficiencies and possible improvements were identified. This chapter will now apply and develop the analysis and criticisms presented in previous chapters to ensure that the responses given are more effective and efficient, and thus, augment the strength of Azerbaijan in its fight against cybercrime. The primary sources of ideas, recommendations and suggestions being presented in this chapter are based on the analysis of different documentary sources on cybercrime control and prevention, as well as interviews conducted with relevant experts in Azerbaijan. The Chapter also covers policy transfer lessons from the UK to make further suggestions for enhancing the capacity of the country. Drawing lessons from the existing experience and insights of the UK can offer advantages of reduced time and cost for making improvements in Azerbaijan. However, the author acknowledges the differences between the two countries in terms of resources and capabilities, as well political environment and socio-legal contexts. Hence, the processes of 'emulation' and 'hybridization' are applied.[787] 'Emulation' is adopted to ensure the effectiveness of policy transfer and flexibility in proposing ways for overcoming the challenges posed by the differences. 'Hybridization' is applied to supply additional flexibility to lesson-drawing and increase the chances of success through allowing the combination of the recognizable elements of UK's and Azerbaijan's relevant programmes in cases of incompatibility or absence of necessary components.

6.2 Identifying and Measuring Cybercrime

Appropriate responses to cybercrime necessitate clarity in the usage of the term 'cybercrime', which can then lead to better understanding and measuring the nature, scale and extent of the threat posed by cybercrime to a given country. Specific challenges in this regard have been extensively discussed in Chapters 2,

[787] See Chapter 1, Section 1.4.

3, and 4, and it was revealed that the term had not been defined in Azerbaijan. Albeit that the existence of cybercrimes is commonly recognised and agreed at the national level, substantial ambiguity remains about which acts are incorporated or omitted by the term 'cybercrime', and what is the extent of their harmfulness. This deficiency was also asserted during the fieldwork in Azerbaijan. Almost all the interviewees believed that cybercrime is becoming a greater threat to the country than ever before. However, the definitions given by them to cybercrime varied substantially. It would be helpful to achieve greater clarity in defining the terms around cybercrime.

As discussed in Chapter 2, approaches to defining cybercrime have evolved significantly, and the term has been defined in many academic publications.[788] Considering that 'cybercrimes' analysed by this study have been allocated to different chapters of the Criminal Code (1999) due to the variation between the objects and values to be safeguarded, it would be impractical to reconfigure the Code and bring all cybercrime offences under the same chapter as 'cybercrime'. It is more important to ensure that the Code properly addresses all the acts deemed to be cybercrime by this study. Therefore, it might be more practical and appropriate to stick with the criminalisation approach adopted by the Convention on Cybercrime, despite its shortcomings, and to ensure that, all the provisions set by the Convention are adequately met somewhere in the Code. Azerbaijan is a signatory to the Convention, and the approach taken by the Convention has already largely influenced the national legislation. Moreover, the Convention seeks to pursue a common criminal justice policy aimed at the protection of society against cybercrime, especially by fostering appropriate legislation and fostering international cooperation.[789] However, considering that the Convention has already shown signs of reform, it is important to establish an efficient update mechanism ensuring that 'the new forms of cybercrimes or specific problem areas such as phishing, identity theft and crime in "virtual worlds"' are also covered.[790] The approach adopted by the United Kingdom Home Office to defining cybercrime in

[788] See Chapter 2, Section 2.2.
[789] Preamble, Council of Europe Convention on Cybercrime (2001) ETS No. 185.
[790] Ian Brown, Lilian Edwards and Christopher Marsden (n. 291) 12.

the Serious and Organised Crime Strategy (2013) can be considered as a possible solution to this problem. The UK Home Office used 'cybercrime' as an umbrella term referring to cyber-dependent crimes - those that can only be committed using computers, computer networks or other forms of information communication technology (ICT), and cyber-enabled crimes - crimes which 'can be conducted on or offline, but online may take place at an unprecedented scale and speed'.[791]

Aside from resulting in the inconsistency of legal and institutional responses, especially by leading to ineffectiveness and inefficiency of coordination and cooperation among institutions against cybercrime, the lack of an adequate definition for cybercrime also produces the significant undercounting of cybercrimes.[792] In Azerbaijan, potential and actual victims of cybercrime have not been sufficiently acknowledged, nor have they been adequately informed about how to report cyber incidents. Under-reporting and under-counting of cybercrime, in turn, have blurred the understanding of the current cyber threat landscape and obscured the full impact on the country. As noted in the UK Cyber Security Strategy 2011, a clear and shared understanding of the nature and scale of threats and vulnerabilities is crucial for raising the importance of investing in protection and prevention.[793] The UK National Cyber Security Strategy 2016-2021 has included a better understanding of the scale of the threat among the indicative success measures of the country's capability to respond effectively to cyber incidents, to reduce the harm and counter cyber threats.[794] Thus, it can be argued that achieving a clear understanding of the nature and scale of threats and vulnerabilities caused by cybercrime is vital for Azerbaijan for ensuring an effective defence against cybercrime, which requires the country to ensure that a higher proportion of incidents is reported to the authorities.

Of utmost importance in this regard might be the establishment of a centralised incident reporting and response mechanism, such as the UK National Cyber

[791] UK Serious and Organised Crime Strategy (2013) (n. 85), 22. For further discussion see Chapter 2, Section 2.2.
[792] Thomas J Holt, *Crime On-Line* (Durham, N.C.: Carolina Academic Press, 2nd edn. 2013) 8.
[793] The UK Cyber Security Strategy (2011) (n. 9) 2.12.
[794] The UK National Cyber Security Strategy 2016 to 2021, 5.6.9.

Security Centre (NCSC), which specifies transparent processes for reporting cyber incidents, and increases awareness about the existence of such a mechanism among businesses and public. The existence of an operational mechanism might be especially favourable for Azerbaijan, as the public and businesses could report only to the national security agency until 2015 when the Ministry of Internal Affairs was also tasked with the investigation of cybercrimes. However, the observation by Wall about the UK context, that 'public expectations of the police that cybercrimes do not fit into the broader public perception of what the police do', seems pertinent to the Azerbaijani context, given the limited number of reports and investigations.[795] It is, thus, important to ensure that the reporting of cybercrime and cybersecurity incidents is made much more straightforward and accessible, as in the UK. The Electronic Security Service in Azerbaijan, which formally has similar roles and responsibilities to those exercised by the NCSC (UK), might achieve success in increasing the levels of reporting. However, the Centre does not seem to prioritise awareness-raising campaigns and so has not achieved significant results to date. The main obstacle to achieving high-level participation in awareness-raising and enlightenment campaigns has been claimed to be 'high levels of bureaucracy', as the Centre operates under the Ministry of Transport, Communication and High Technologies.[796] Thus, in addition to addressing the challenges of administration, the government also needs to develop specific programmes for public awareness raising, including users in the education, legal, as well as justice systems with regard to the need to respond to cybercrime. In the UK, on top of the campaigns constantly delivered by Action Fraud, the UK Home Office has launched the UK's national fraud and cybercrime reporting centre, a cross-government awareness and behaviour change campaign called Cyber Aware.[797] Cyber Aware (formerly Cyber Streetwise) focuses on driving behaviour change amongst small businesses and individuals, so that simple, secure online behaviours are adopted by them to help protect themselves from cyber criminals.

[795] David S. Wall, (n. 133) 195; for Azerbaijani context, see Section 3.3. and Section 3.4., Chapter 3.
[796] Ministry Official 1, 2, 3, 4, 5.
[797] The campaign has been launched by the UK Home Office in conjunction with Department of Culture, Media & Sport alongside the National Cyber Security Centre. For further information, see: https://www.cyberaware.gov.uk/.

There seems to be a correlation between the lack of public perceptions of the social dangers of cybercrime and the problems of under-reporting and underestimation of cyber incidents/offences. Therefore, it is vital to reconsider the reasons leading to under-reporting and to take serious steps to address its challenges.[798] However, addressing the challenges of under-reporting will be slow and laborious work in the Azerbaijani context, given that there is a low public expectation of the ability of the law enforcement authorities to deal with cybercrime. Mandatory reporting of cyber-incidents, at least for the critical infrastructure providers in energy, transport, financial markets, banking, health and water, would help in ensuring that the most serious incidents are reported, and thus, contribute to improving understanding of cyber threats and risk.[799] Encouraging 'operators of essential services and digital service providers to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities' would also help in shaping the responses to cybercrime more appropriately.[800] Furthermore, a new mandatory reporting duty on data controllers to report certain types of a data breach to authorities, and in some cases to the individuals affected, would also ensure higher protection of personal data and, thus, help to avoid detrimental effects on individual rights. For example, the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) obliges data controllers 'to notify the personal data breach to the supervisory authority …not later than 72 hours after having become aware of it, unless the controller is able to demonstrate …that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons'.[801] It further stipulates that if a personal data breach is likely to cause a high risk to the rights and freedoms of the natural person, the controller

[798] See Chapter 3, section 3.4., for the reasons leading to underreporting. See for further information about the challenges of under-reporting: David S. Wall (n. 6) 164-165. See also further information: Fafinski, S. and Minassian, N. *UK Cybercrime Report* (2009), pages 23-24.

[799] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS directive), para 4. https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

[800] Ibid, para 62.

[801] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119 (4 May 2016) para 85.

should notify the data subject of a personal data breach to allow him or her to take the necessary precautions.[802] When trying to address the problem of under-reporting, it also needs to be considered whether the internet industry themselves can also contribute to the response rate to certain types of cybercrime. For example, Internet Watch Foundation (IWF) allows internet users to report anonymously and confidentially and then works with LEAs to seek the removal of images of child sexual abuse.[803] Azerbaijan would benefit from adopting this tactic, especially for enhancing online child protection, as no officially recognised agency offers an avenue for reporting online child sexual abuse materials.

As stated by Osborne and Gaebler, without the correct measurement the success and failure of administrative structures cannot be assessed, and without recognising failure, it is impossible to correct it.[804] So, access to accurate information about the actual extent and scale of cybercrime is a vital prerequisite.[805] The mapping and measurement of cybercrimes are needed to inform crime reduction initiatives, enhance local and national responses, provide intelligence and risk assessment, facilitate reporting, educate and inform the public, and identify preventative measures, gaps in response as well as areas for further research.[806]

Maintaining statistics are also key to building a better intelligence picture of the threat and facilitating more informed decisions on resource allocation and the distribution of limited funds across the criminal justice sector.[807] Therefore, developing methodologically sound national surveys measuring cybercrime, which are currently unavailable in Azerbaijan, is of utmost significance.

General difficulties in obtaining accurate measures of the quantification of cybercrimes have been emphasised in Chapter 2.[808] In Azerbaijan, both statistical

[802] Ibid, para 86.
[803] 'Homepage' (IWF, 2017) https://www.iwf.org.uk/.
[804] David Osborne and Ted Gaebler (n. 267) 146.
[805] ITU (n. 102), 14.
[806] Stefan Fafinski, William H. Dutton and Helen Margetts (n. 186).
[807] TechUK, 'Partners against crime- How can industry help the police to fight cyber-crime?' (October 2015) 7.
[808] See Chapter 2, Section 2.4.

information on cybercrime occurrence is largely absent,[809] and the accuracy of available data is doubtful. The LEAs and government authorities keep statistics on cybercrime confidential and treat them as a 'sensitive matter',[810] even though disclosing consolidated statistical data, including 'consolidated statistics on crimes' has been determined as an obligation of information owners by the Law on the Right to Access Information 2005.[811] The Government should make data transparency a key priority about cybercrimes, to foster accountability, and achieve improvements in its responses, as well as to meet public interests. In general, the management of statistical data should be improved at both investigation and prosecution levels. Collection of such data would provide a clearer picture on the extent and scale of the threat and would further inform concerning strategies and criminal justice initiatives. Furthermore, in addition to statistical data, it is also crucial to ensure that those involved in controlling cybercrime have access to the necessary intelligence, especially to the information on offences, offenders, as well as techniques and methods used in cybercriminal activities. This can be achieved through the establishment of a common database that grants direct access to relevant authorities.

Despite criticism of the methodology,[812] the UK has included cybercrime offences in its annual national crime statistics in the year ending September 2016. Notwithstanding the differences in terms of the resources available in Azerbaijan, a transfer of this UK methodology would be a viable option for Azerbaijan.

According to the UK Office for National Statistics, crimes recorded by the police are not a wholly reliable source for measuring trends in crime, as they are dependent on recording practices and police activity, as well as changing behaviour in public

[809] See also, The Overseas Security Advisory Council (OSAC), *Azerbaijan 2018 Crime & Safety Report* (the Bureau of Diplomatic Security, U.S. Department of State, 2018) https://www.osac.gov/pages/ContentReportDetails.aspx?cid=23379.
[810] State Security Service employee (via informal telephone conversation); Ministry Official 1, 2, 3, 4 and 5.
[811] Article 29.1.1., Law on the Right to Access Information, 2005. See also, Chapter 3, Section 3.4.
[812] Office for National Statistics, *Improving Crime Statistics For England and Wales – Progress Update - Office for National Statistics* (Ons.gov.uk, 2017) https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/improvingcrimestatisticsforenglandandwalesprogressupdate.

reporting of crime.[813] In comparison, the source of the national crime statistics in Azerbaijan has long been official statistics reports submitted by the Ministry of Internal Affairs to the State Statistical Committee.[814] Therefore, crime statistics might be insufficient in revealing the true picture about cybercrime offences due to underreporting. In response, the methodology applied by the Crime Survey for England and Wales (CSEW) might be adopted in Azerbaijan to overcome the limitations of police recorded crime. The CSEW is 'a face-to-face survey in which people resident in households in England and Wales are asked about their experiences of crime in the 12 months before the interview', it covers a broad range of victim-based crimes, not just those that have been reported to, and recorded by, the police.[815] To achieve a higher level of objectivity, the CSEW survey is conducted by an independent (from the government or the police) organisation using trained interviewers who have no subjective interest in the results of the survey. Questions related to cybercrime offences can be introduced onto survey samples, and the process, in general, has already revealed a higher number of reported offences than police recorded crime.[816] However, the identification of cybercrime offences still requires several stages of development in the CSEW including a desk review, the development and testing of new questions using a mix of qualitative and quantitative research, and a large-scale field trial of 2,000 interviews.[817] Therefore, to secure accurate results from a similar survey in Azerbaijan about cybercrime, similar preparations would be required, subject to learning from experience in the UK.[818]

---

[813] Assessment of compliance with the Code of Practice for Official Statistics on Crime in England and Wales (produced by the Office for National Statistics) 1.2.3.

[814] See 'Metadata on indicators' ('Göstəricilərə Dair Məlumat Sistemi') (*Azstat.org,* 2017) http://www.azstat.org/MetaDataG/bchapgos.jsp?prkod=90001&prskod=36.

[815] Office for National Statistics, *Crime in England and Wales: year ending Sept 2016* (Ons.gov.uk, 2016).

[816] Ibid*;* see also, Office for National Statistics, *Crime in England and Wales: year ending March 2018* (Ons.gov.uk, 2018).

[817] TNS BMRB, *CSEW Fraud and Cyber-crime Development: Field Trial – October 2015* (TNS-BMRB, 2015).

[818] For the methodology and questions see also, Office for National Statistics, *Methodological note: Work to extend the Crime Survey for England and Wales to include fraud and cyber-crime* (Ons.gov.uk, 2014); Office for National Statistics*, Improving Crime Statistics for England and Wales – progress update July 2018* (Ons.gov.uk, 2018).

6.3 Enhancing Policy Responses

As discussed in Chapter 3, dedicated and comprehensive cyber security and cybercrime strategy and policies have not been introduced in Azerbaijan. Yet, the country has been exposed to the relentless growth of cybercrime and information security related threats and offences. Therefore, security, resilience, reliability and trust in ICT and an effective criminal justice response to cybercrime should be proportionately enhanced by pursuing comprehensive strategies, policies and legislation. Under this heading, my aim is to present specific recommendations and solutions that can potentially enhance policy responses of the country to cybercrime.

As regards strategies, it is important to note that cybersecurity and cybercrime strategies are interrelated and complementary, but not identical. In general, cybersecurity is focused on ensuring the confidentiality, integrity and availability of computer data and systems, while cybercrime strategies primarily focus on a criminal justice rationale and link to broader crime prevention and criminal justice policies.[819] Nonetheless, cybersecurity and cybercrime-control and prevention related strategies are equally important and mutually reinforcing. Thus, an appropriate criminal justice response to cybercrime reinforces cybersecurity.[820] Therefore, the development of technical, procedural and institutional measures for the protection against, mitigation of, and recovery from, cyber-attacks and incidents affecting, in particular, its critical information infrastructure, should be implemented in Azerbaijan.

Having elaborated the national cybersecurity context in Chapter 3, it can be suggested that the introduction of a national cyber security strategy would also add to the enhancement of the anti-cybercrime capacity of the country. The strategy could ensure better protection through assisting the initiation of a systematic national programme to secure cyberspace, prioritizing threats and risks, and allocating roles and responsibilities. A national cyber strategy would also help to

[819] Alexander Seger, *Cybercrime strategies - Discussion paper* (Global Project on Cybercrime, Council of Europe 2011) 5.
[820] Council of Europe, *Capacity building on cybercrime – discussion paper,* (Strasburg 2013) 7.

establish a clear overview of the funding dedicated to the responses to cybercrime. It could provide all stakeholders with the awareness of relevant risks, preventive measures and effective control mechanisms, as well as help to mobilise resources and technical assistance for capacity building.[821] An anti-cybercrime strategy should also be an integral element of a cybersecurity strategy, as its development contributes to ensuring that legal and criminal justice responses mirror the challenges of cybercrime and assists in determining operational and strategic priorities before any legislative reform processes.

Establishment of a general strategy could provide for the public demonstration of the efforts to be undertaken by publishing a cybercrime and cybersecurity strategy, but at the same time could facilitate concrete measures, if necessary in confidence.[822] Having a comprehensive, clear and transparent national cybersecurity strategy is also crucial for Azerbaijan to attract more foreign and local investors, especially in the 'post-oil' era. While developing such a strategy, however, it is essential to be cautious in revealing technical details about actions undertaken for enhancing cybersecurity that could lead to the identification of weaknesses by potential attackers.[823]

Since cybersecurity and cybercrime are distinct concepts, it is not easy to incorporate all aspects necessary for a cybercrime strategy into a broader cybersecurity strategy. Nevertheless, the National Strategy for the Development of the Information Society for the years 2014-2020 cannot be regarded as a comprehensive approach to the problem of ensuring cybersecurity, so clearer directions to address its challenges are required somehow. Combining all relevant measures and activities in a single document is not the only way of establishing a comprehensive approach. As revealed in Chapters 3, 4 and 5 and during the fieldwork, the lack of a cyber security strategy has not completely prevented Azerbaijan from pursuing responses to cybercrime, albeit the efforts have been piecemeal.

[821] Alexander Seger (n. 819), 22.
[822] ITU (n. 102), 104.
[823] See Section 3.2., Chapter 3.

Along with a strategy, appropriate responses to cybercrime also necessitate the establishment of dedicated cybercrime policies. In comparison to a strategy, policies define various elements applied in addressing the strategy, in particular, the government's response to the strategy.[824] The policies enable the government to define its response to a certain problem comprehensively and may incorporate a broad range of replies to achieve specific goals that may not be mentioned in an overall strategy and legislation. Specific policies can also ensure that legal and strategy related measures do not cause conflicts.[825]

Therefore, Azerbaijan should focus on establishing an explicit cybercrime strategy, or specific cybercrime components within cybersecurity strategy, and comprehensive and dedicated policies to ensure an effective criminal justice and security responses. The legislation, preventive measures, specialised law enforcement units and prosecution services, law enforcement and judicial training, interagency cooperation, public/private cooperation, and effective international cooperation can be considered as necessary elements within an overall strategy.[826] The failure to devise comprehensive strategy and policies could also raise the danger that consequent legislation will be fragmented, partial and ill-directed.

The development of legal frameworks can be considered as another major requirement of securing trust and confidence in ICT. While elaborating the legal measures undertaken in Azerbaijan in Chapters 3, 4 and 5, it became apparent that legal measures play a crucial role in responding to cybercrime and operate in distinct aspects, including 'criminalization, jurisdiction, procedural powers, international cooperation, and responsibility and liability of internet service provider[s]'.[827] The negative implications of not adequately reflecting dedicated policies in the legislation were highlighted in Chapter 3.[828] It would be more productive to establish specific policies, which can be utilised to identify the areas where legal development and harmonisation should take place and determine the

[824] Marco Gercke (n. 279), 15.
[825] ITU (n. 102), 114.
[826] Council of Europe (n. 239), 5.
[827] UNODC (n. 71), xviii.
[828] See Section 3.2 and 3.3, Chapter 3.

regional/international standards to be enforced in the particular national circumstances of Azerbaijan.[829]

Adopting a comprehensive approach against cybercrime might also ease the cooperation of different actors with overlapping competences in the same field, and increase the effectiveness and efficiency of laws.[830] Overlapping competencies can be addressed through the elaboration of the roles and responsibilities of different actors in securing the national cyberspace, which needs to be given special attention when establishing a comprehensive approach in the form of policies, strategy and law, as also provided by the UK National Cyber Security Strategy 2016 to 2021.[831] This response is needed because cybercrime is a cross-sector topic relating to the mandates of different institutions and sectors. Thus, it is essential to define the roles and responsibilities of the various stakeholders more clearly and allocate resources accordingly.

6.3.1 Roles and responsibilities

6.3.1.1 The government

As noted in Chapter 3, Azerbaijan has preferred a state-centric approach to protect its citizens from cyber-attacks and cybercrime. State intervention is inevitable and proper where economic issues or public concerns are strong motivators.[832] Yet, despite the highly centralised approach, there are still problems in clarifying the roles and responsibilities in government and thus, guaranteeing that government authorities are provided with essential resources and clear directions. As an evolving law enforcement matter, cybercrime necessitates the clarification of the roles and responsibilities of a range of actors, determining the specific focuses and

[829] Marco Gercke, (n. 279) 15.
[830] See Section 3.3. and 3.4. Chapter 3.
[831] The UK National Cyber Security Strategy 2016 to 2021, 4.6.
[832] David S. Wall and Matthew Williams, 'Policing Diversity in The Digital Age' (2007) 7 *Criminology & Criminal Justice,* 409.

aspects of law enforcement responses, and the allocation of appropriate resources to do this properly.[833]

It was highlighted in Chapter 3 that roles and responsibilities between the state agencies concerned with law enforcement and policing, civil protection, national security and military force in the fields of cybercrime and cybersecurity in Azerbaijan are blurred. Any uncertainty can result in operational ineffectiveness and individual unfairness. Thus, operational challenges in law enforcement cannot be treated as excuses not to ensure the protection of constitutional values or fundamental rights.[834] With regard to the investigation of cybercrime offences, the significance of the targets of a crime and the severity of its social danger may be considered as important factors when distributing investigative competencies. Thus, unless national or state security interests are threatened or attacked, a national security authority should not be involved in the investigation of cybercrime. More investigative powers would be transferred to the Ministry of the Interior from the State Security Service, and by consequence, the Ministry of the Interior would have a greater role in investigating cybercrime offences and dealing with electronic evidence in Azerbaijan soon.[835] Therefore, the capacity and capability of the police need to be strengthened through developing structures, guidelines, resources, competencies and capabilities in the field of cybercrime, as well as through ensuring that a sufficient number of individuals recruited to cope with a large number of cases.

As noted in Chapter 3, the country experiences scarcity of qualified specialists and sufficient resources within the government authorities dealing with cybersecurity and cybercrime.[836] These deficiencies should also be addressed. Strong substantive and procedural domestic criminal laws and assenting to international instruments such as the Convention on Cybercrime do not provide the law enforcement authorities with all necessary capabilities.[837] Thus, as has been widely

[833] Michael Levi et al. (n. 87*),* 29.
[834] Ben Hayes et al. (n. 137), 8.
[835] Council of Europe (n. 304).
[836] See. Section 3.4. Chapter 3.
[837] Cameron S. D. Brown (n. 705), 57.

practised in the UK, the government in Azerbaijan should invest significantly in law enforcement capabilities at different levels to ensure that law enforcement authorities have the required capacity to control the increasing level and sophistication of cybercrime.[838] It would be particularly helpful to establish highly developed organisational structures, ones that avoid overlap and are based on clear competences with the ability to conduct complex investigations that require the involvement of legal as well as technical experts.[839] The functions and financing of specialised units should be reviewed on a regular basis to meet emerging problems and growing demands.

It was argued in Chapter 3 that it has been difficult to deal with all cybercrime cases effectively and efficiently due to the existing single central divisions under the Ministry of Internal Affairs and the State Security Service.[840] Capacity enhancement at the local level is, thus, crucial, since national specialised units can investigate a limited number of cases, while cyber aspects and digital evidence are contained in more localised crimes.[841] Thus, the Government should consider the establishment of provincial/local cybercrime divisions tasked with the investigation of cybercrime. Furthermore, once established, the promotion of inexperienced supervisors into management positions in these divisions should be strictly avoided, as they might 'fail to account for staff welfare, negatively impact case outcomes, and ultimately undermine the credibility of the department or agency that they represent'.[842]

Furthermore, contrary to the experiences of Azerbaijani LEAs, engagement in training, international conferences and forums devoted to the fight against cybercrime is needed for enhancing the capacity against cybercrime. For example, over £1.3 million on 39,438 officers and staff has been spent on cybercrime training

[838] *The UK Cyber Security Strategy 2011-2016,* Annual Report, April 2016*,* section 2.31.
[839] ITU (n. 102), 111.
[840] See Section 4.5. Chapter 4.
[841] Police Executive Research Forum, 'The Role of Local LEAs in Preventing and Investigating Cybercrime' (Critical Issues in Policing Series, Washington, 2014) 4; see also, Sameer Hinduja, 'Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams' (2004) 27 *Policing: An International Journal of Police Strategies & Management.*
[842] Cameron S. D. Brown (n. 705), 94.

courses by UK police forces in the past three years.[843] In Azerbaijan, training and development programs should focus on ensuring that LEAs have acquired the skills and competencies required for cybercrime investigations, digital evidence handling, computer forensic analysis and cooperation with other local and international partners. Once law enforcement staff involved in cybercrime and computer forensics training programmes, which are expensive, to receive an adequate return for the investment, they should be appointed to, and remain in, posts that reflect the level of knowledge and skills they have.[844] It would also be cost effective for LEAs to prioritise the recruitment of officers with existing cyber skills and share key security training services with other LEAs.[845]

Detection and investigation of cybercrime should be followed by adequate prosecution and adjudication structures, which again need to be performed by those who have received appropriate training and resources. So, the prosecution and adjudication of cybercrime cases also call for specialisation within the criminal justice system.[846] Therefore, it is vital to have personnel with an understanding of concepts of computing and the internet, knowledge of cybercrime legislative frameworks, and the ability to present and understand electronic evidence in court.[847] Lacking the technical expertise required to manage cybercrime cases may contribute towards the acquittal of cybercrime offenders, which would pose a significant threat to public safety.[848] Hence, systematic and sustainable compulsory training programs integrating basic and advanced training modules on cybercrime and electronic evidence should be introduced for all judges and prosecutors, including basic knowledge about computers and networks, cybercrime and cybercrime legislation, jurisdiction and territorial competencies and electronic evidence.[849] To face situations where basic knowledge is insufficient, a substantial number of judges and prosecutors should be provided with advanced and

[843] Parliament Street, *Policing and Cybercrime* (A Parliament Street Policy Paper 2018) 3.
[844] Council of Europe (n. 239), 8.
[845] Parliament Street (n. 843) 5.
[846] UNODC (n.71), 172.
[847] Ibid.
[848] Cameron S. D. Brown (n. 704), 99.
[849] Council of Europe, *Cybercrime training for judges and prosecutors: a concept* (Strasbourg, France 2009) 12-13.

specialist knowledge related to cybercrime and electronic evidence.[850] Moreover, it would be helpful to keep a record of all training received by judges and prosecutors to inform requirements for further specialised training and to ensure the right people are trained and their skills are utilised properly.[851]

In general, police/investigators, lawyers, prosecutors and judges can be provided with ongoing up-to-date online and offline training programs and courses offered by various organizations such as the United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol, Interpol, SANS Institute, High Technology Crime Investigation Association, as well as via massive open online course (MOOC) platforms.[852]

In addition to personnel specialisation, Azerbaijan should also ensure a sufficient degree of organisational cybercrime specialisation for the Prosecution Service.[853] Development of the necessary capabilities and a team/unit for cybercrime prosecution is critical to ensure that actions undertaken by LEAs responsible for cybercrime investigation are compliant with laws, as well as to enhance the capabilities and improve potential outcomes from prosecutions. The UK Crown Prosecution Service Cybercrime Strategy (2016) might be adopted as a model for making further improvements in this regard, as it provides the ways to achieve success by:

> '1. allocating cases in line with internal expertise;
>
> 2. building capability within the CPS and across law enforcement partners;
>
> 3. providing regular up-to-date and relevant training for prosecutors;
>
> 4. using our international network to prosecute cybercrime criminals overseas;
>
> 5. improving our service to victims of cybercrime.' [854]

---

[850] Ibid. 14-17.
[851] Council of Europe (n. 239) 9.
[852] Such as *edX* (https://www.edx.org/); *Coursera* (https://www.coursera.org/); *FutureLearn* (https://www.futurelearn.com/); *iversity* (https://iversity.org/); Udacity (https://www.udacity.com/).
[853] See Chapter 3, Section 3.4.
[854] CPS Cybercrime Strategy (2016), para.6 accessed online through: http://www.cps.gov.uk/publications/docs/cps_cybercrime_strategy_2016.pdf.

In addition, Cybercrime - Prosecution Guidance of the Crown Prosecution Service is another notable document to be considered while developing a specific guideline for prosecution. [855] It would also be productive to actively involve with Global Prosecutors E-Crime Network (GPEN), which is focused on improving international cooperation among cybercrime prosecutors and jointly organises training courses and the exchange of best practices.[856]

As noted in Chapter 3, courts in Azerbaijan show minimal levels of specialisation in cybercrime because of the lack of necessary resources for cybercrime-related training and expertise within the judiciary. So, in addition to introducing essential knowledge and skills to judges and prosecutors through training and development programs, it is incumbent to provide courtrooms with modern multimedia technology to effectively present digital evidence during criminal proceedings.[857] Alternatively, if a surge in cybercrime case load is experienced in the future, designation of specialised cybercrime courts or special courts for cases involving the Internet can help to fast track process of delivering justice and ensure that the number of cases does not stay pending too long.[858] The UK government, for example, has announced in July 2018 that a £170m flagship court to deal with cybercrime is to be set up in the City of London.[859]

The ability to identify, collect, preserve, prepare, present and evaluate electronic evidence is vital in ensuring the effectiveness and legitimacy of criminal investigation and proceedings. Therefore, Azerbaijan should make investments to address the existing lack of resources through developing/acquiring technical forensic equipment and devices, as well as recruiting and providing staff with

---

[855] 'Cybercrime - Prosecution Guidance | The Crown Prosecution Service' (*Cps.gov.uk,* 2018) https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.
[856] For further information, see http://www.iap-association.org/GPEN/Home.aspx.
[857] Cameron S. D. Brown (n. 705), 96.
[858] For example, Malaysia and Philippine have established special courts in 2016 for cases involving the Internet and to fast track the prosecution of offenders, which is equipped with facilities to function as an e-Court, as well as having technology-savvy judges and prosecutors.
[859] 'World-Class Fraud And Cybercrime Court Approved For London's Fleetbank House Site' (*GOV.UK*, 2018) https://www.gov.uk/government/news/worldclass-fraud-and-cybercrime-court-approved-for-londons-fleetbank-house-site; see also, 'UK To Establish Court For Cybercrime In London' (*Bankinfosecurity.com*, 2018) https://www.bankinfosecurity.com/uk-to-establish-court-for-cybercrime-in-london-a-11174.

essential skills to deal with cybercrime cases and digital evidence. Furthermore, it is equally important to develop computer/digital forensics laboratories to enhance the capacity of authorities in investigating, prosecuting and adjudicating cybercrime.

6.3.1.2 Private sector, academia and civil society

As provided in Chapter 3, the businesses, academia and civil society organisations in Azerbaijan's have not been sharing an active role alongside with government sector in ensuring cybersecurity and combatting cybercrime. The state does not pursue a holistic approach. Since it is mainly the private sector and businesses that use and owns the Internet infrastructure, they should be attached a share of liability for the consequences of cyber-attacks, and should, therefore, take all reasonable steps to 'safeguard the assets which they hold, maintain the services they provide, and incorporate the appropriate level of security into the products they sell'.[860] The private sector and businesses should also be regarded as the repository of technical skills and attack trend information, and as possessing the knowledge to help deliver a safer internet.[861] Also, it is important to consider that industry can actively cooperate and collaborate in formulating policies related to cybercrime, including monitoring, investment, counter-measures, harmonisation of terminology, and design of laws.

Although not widely practised in Azerbaijan, as discussed in Chapter 3, the involvement of academia, civil society organisations and the public can enhance the country's anti-cybercrime and cybersecurity strategy. Especially the role of academia, assisting the government in the formulation of legislation, policies and standards, supplying necessary knowledge and training materials and developing cutting-edge solutions to respond to cybercrime should not be understated. Azerbaijan needs to promote cyber-security and cybercrime-control related studies through the establishment of specialised educational programs, research and training centres and units within different institutions and must align its curricula

[860] The UK National Cyber Security Strategy 2016 to 2021, section 4.8.
[861] The UK Cyber Security Strategy (2011).

with its regulatory and industry demands. Particularly, the law schools should integrate a curriculum teaching fundamental knowledge on cybercrime and cybercrime legislation, jurisdiction and territorial competencies and electronic evidence.

The UK government has undertaken measures to enhance private sector involvement. For example, to identify and promote required knowledge and capabilities, 14 universities have been recognised as Academic Centres of Excellence in Cyber Security Research (ACE-CSRs) by the UK Government.[862] Besides, to further stimulate cyber security research in the UK, the National Cyber Security Centre supports Doctoral students across the ACE-CSRs, and by 2021, it is expected that around 150 new Doctoral Students will have completed research studies in essential cyber security topics.[863]

Given the absence of specific programs or campaigns pursued or lessons offered at schools in Azerbaijan, it would be useful to draw lessons from the UK at this level as well. To address the skills shortage and to prepare the general public to deal with cybersecurity, the Cyber Schools Programme was launched, which is aimed at those aged between 14 and 18, who will be expected to commit to four hours a week, with a target for at least 5,700 teenagers to be trained by 2021.[864] Applying this education programme in Azerbaijan and informing young people about the threats, vulnerabilities and risks of the cyber world would be helpful and viable.

Engaging with civil society organisations possessing valuable knowledge and experience is also crucial for Azerbaijani context. The reluctance to host stakeholder consultation in the drafting process of such documents influences

[862] For further information see 'Academic Centres of Excellence in Cyber Security Research - NCSC Site' (*Ncsc.gov.uk*, 2018) https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research; see also, HM Government, 'Developing our capability in cyber security' (2015).
[863] Ibid.
[864] 'Cyber Schools Programme' (*GOV.UK,* 2018) https://www.gov.uk/guidance/cyber-schools-programme; see also, 'Extracurricular Cyber Clubs to Inspire and Identify Tomorrow's Cyber Security Professionals' (*GOV.UK*, 2018) https://www.gov.uk/government/news/extracurricular-cyber-clubs-to-inspire-and-identify-tomorrows-cyber-security-professionals; 'Cyber Security Lessons Offered to Schools in England' (*BBC News,* 2017) https://www.bbc.co.uk/news/education-38938519.

negatively on ensuring that various concerns are sufficiently addressed. Civil society organisations should also jointly engage in facilitating cooperation among existing security networks while making the network's actions more transparent and accountable.[865]

When communities are empowered to solve their problems, they function better than communities that depend on services provided by outsiders.[866] Considering the challenges posed by cybercrime to the LEAs, law enforcement can also be supported if civilians are allowed into the crime control sphere since the target of cybercrime is mostly civilian victims. Innovative use of volunteers with technical knowledge and skills can significantly assist under-resourced LEAs having difficulties with non-critical or immaterial cybercrime cases awaiting forensic analysis.[867] For example, civilians are recruited to assist police to solve cybercrime under an expansion of the role of volunteers in England and Wales.[868] Additionally, volunteers certified in Forensic Toolkit (FTK), a software program that enables investigators to access deleted e-mails, crack passwords and uncover chat logs, can be involved to help the police to recover and investigate material found in digital devices. However, it is also argued that civilians should be incorporated into the process of prevention of cybercrime, rather than only reacting to it. According to Susan Brenner, having civilians work with the LEAs would consume resources, as they would have to be given some degree of law enforcement training.[869] Yet, the security of IT products can be improved through the work of independent security researchers engaged in vulnerability research, which is also indispensable to preventing cybercrime.[870] It is argued that this way of support to law enforcement

[865] Organisation for Economic Co-operation and Development (n. 235) 16.
[866] David Osborne and Ted Gaebler (n. 267) 51.
[867] Cameron S. D. Brown (n. 705), 94.
[868] 'Civilians to Help Police Investigate Cybercrimes, Says Theresa May', (*BBC News,* 2016 http://www.bbc.com/news/uk-35354139; See also, 'Platform To Match Volunteer Skills To Cybercrime Investigations | Office Of Northamptonshire Police And Crime Commissioner' (*Office of Northamptonshire Police and Crime Commissioner*, 2018) https://www.northantspcc.org.uk/platform-to-match-volunteer-skills-to-cybercrime-investigations/.
[869] Susan W. Brenner (n. 197), 215-216.
[870] This very diverse group can include students, academics, free-lance professionals or just amateurs in computer science who may be knowledgeable but work in their spare time'. See for further information Audrey Guinchard, 'Transforming the Computer Misuse Act 1990 to support

might descend into vigilantism, and thus, the process may become difficult to control and monitor.[871] However, proper police vetting would 'get rid of the risks'.[872] Also, as a most passive endeavour, deputising civilians to prevent cybercrime does not raise the resource and control issues and therefore, encouraging cybercrime prevention would probably increase the effectiveness of law enforcement efforts to combat cybercrime.[873]

6.3.2 Towards more effective and efficient cooperation

Cybersecurity challenges cannot be overcome alone by any country, agency, company or individual. A collective effort is required to ensure the security of the national cyberspace, as emphasised by the UK National Cybersecurity Strategy 2016 to 2021.[874] Due to the complex interdependencies created between the public and private sectors in cyberspace, communication and cooperation in national, regional and international levels should involve, and be supported, by all stakeholders.[875] Therefore, as stated by the UN General Assembly Resolution 64/211, 'governments, business, organisations and individual owners and users of information technologies must assume responsibility for and take steps to enhance security'.[876]

6.3.2.1 Intra-state cooperation

It is crucial to establish a strong public-private partnership for mitigating threats and identifying and disrupting cybercrimes.[877] As the critical infrastructure lies largely in the hands of the private sector, every measure undertaken should require

---

vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime.' (2018) 2 (2) *Journal of Information Rights, Policy and Practice,* 7.

[871] İbid; See also Susan W. Brenner (n. 197), 215-216;

[872] 'Ex-CEOP Boss: 'Recruit Paedophile Hunters' (*BBC News*, 2018) <https://www.bbc.co.uk/news/uk-northern-ireland-41350389>

[873] Susan W. Brenner (n. 197), 217.

[874] The UK National Cyber Security Strategy 2016 to 2021, 4.6; see also; *The ITU National cybersecurity strategy guide* (ITU, Geneva, 2012) 38.

[875] UN General Assembly (n. 243).

[876] Ibid.

[877] National Crime Agency Strategic Cyber Industry Group, *Cyber Crime Assessment 2016,* 14.

consultation with the private sector.[878] The state-centric governance approach preferred in Azerbaijan, however, has significantly ignored the complex and dynamic nature of the Azerbaijani information space.[879] One of the significant deficiencies with this approach is that flexibility in perceiving the 'set of available alternative policies and institutional arrangements' is limited, and central decision makers lack a full understanding of actions to be undertaken in dealing with fast and novel changes brought by the increasing use of the ICT.[880] However, this criticism does not mean that the private sector or markets can provide everything necessary for addressing challenges in cyberspace. Interconnection and coordination are among the activities that cannot be provided by markets alone. To put it differently, markets can provide these necessary activities 'if they are appropriately governed and if the rights and expectations of remote participants are secured and sustained'.[881] The law and further mechanisms of state regulation can ensure appropriate governance, security, and sustainment of the rights and expectation of distant participants. After these prerequisites are met, markets can start to provide interconnection and coordination, but here it is important to note that governance produces optimal outcomes when extraneous institutional regulation least impedes its workings.[882]

The European Court of Human Rights underlined in the case of *K.U. v. Finland* that cooperation between law enforcement authorities and private sector entities, including in particular Internet service and hosting providers, is essential to minimise the extent to which services are used for criminal activity.[883] Thus, engaging in public/private cooperation, as well as developing cooperation between law enforcement bodies and service providers should be included among the

[878] Jakub Harašta, 'Cyber Security in Young Democracies', (2013) *Jurisprudence*, 1457-1472.
[879] For further discussion see Section 3.5. Chapter 3.
[880] Andreas Duit, Victor Galaz. 'Governance and Complexity Emerging Issues for Governance Theory' (2008) 21 *Governance,* 311-335.
[881] Paul Hirst & Grahame Thompson 'Globalization and the future of the nation state', (1995) 24 *Economy and Society*, 423.
[882] Ibid.
[883] *K.U. v Finland,* 2872/02, [2008] ECHR; see also, Council of Europe, *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime* (Strasbourg 2008).

measures to be considered for a cybercrime strategy.[884] Given the essential role potentially played in cybercrime investigations by internet service and hosting providers, it is crucial to improving the effective and efficient cooperation between those providers and LEAs, without compromising rights of individuals.[885] Therefore, special importance should be given to ensure that private sector entities and service providers respond to legitimate requests for assistance and to collaborative initiatives within cybercrime investigations, prosecutions, and digital forensic investigations.[886] Developing informal relationships between law enforcement and service providers would speed up the process of information exchange and trust-building.[887] It is, however, crucial to prioritise the protection of human rights when doing so.

Cybercrime control strategy or policies should not be dependent only on the implementation of Council of Europe's Convention on Cybercrime, or on other national legal instruments alone. Development of technical protection measures along with proper cybercrime legislation and bringing anti-cybercrime strategies into line with international standards,[888] as well as promoting self-sufficiency and increasing the level of preparedness and awareness of Internet users should be ensured by involving all actors. Because of the complex nature of ICTs and the security threats, and more importantly, the legal complexity (such as trans-jurisdictional problems) of cyberspace, the threats cannot be overcome by exercising a single-industry agency jurisdiction and a limited number of state officials, as is the case in Azerbaijan. The state should focus more on cooperating with the private sector, as it is only through public-private collaboration that information can be gathered together and different dimensions of the problem are brought into focus.[889] It is vital to establish efficient platforms and arrangements for

[884] Council of Europe (n. 239), 5; see also; The UK Cyber Security Strategy (2011).
[885] For instance, see the letter to Facebook by the UN Special Rapporteur, 'OHCHR | UN Human Rights Expert Says Facebook'S 'Terrorism' Definition Is Too Broad' (*Ohchr.org, 2018*) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23494&LangID=E.
[886] Cameron S. D. Brown (n. 704), 100.
[887] UNODC (n. 71), xxiii.
[888] ITU (n. 102), 4.
[889] KPMG International Cooperative, *Cyber threat intelligence and the lessons from law enforcement,* 2013.

inter-agency cooperation and an 'operational partnerships with the private sector to share information on threats in cyberspace'[890] to appropriately respond to cybercrime.

In the UK, collaborative arrangements exist between the Internet Watch Foundation (IWF), the Association of Chief Police Officers (ACPO), the Crown Prosecution Service (CPS), the Child Exploitation Online Protection Centre (CEOP), the Serious Organised Crime Agency (SOCA) and Internet Service Providers Association (ISPA).[891] In addition, as a joint industry and government initiative, the Cyber Security Information Sharing Partnership (CISP) was established to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.[892] Another initiatives fostered by the UK government to bring together the skills of the police, industry experts and academics is the Cyber Crime Reduction Partnership (CCRP),[893] as well as the Defence Cyber Protection Partnership (DCPP), the partnership between the Ministry of Defence (MOD) and industry to decide upon new cyber security standards for industry and to improve the protection of the defence supply chain.[894]

Azerbaijan would also benefit through the creation of similar partnerships and permanent and secured information sharing channels between the government and the private sector. These partnerships and channels would be particularly helpful for sharing information related to cyber threats, vulnerability and consequences, including experiences from investigations and prosecutions, technical prevention and protection measures, technological development trends and achievements,

---

[890] The UK Cyber Security Strategy (2011), 9.

[891] Michael Levi and Matthew Leighton Williams, 'Multi-Agency Partnerships in Cybercrime Reduction' (2013) 21 *Information Management & Computer Security*; see also Internet Service Providers Association - https://www.ispa.org.uk/.

[892] For more information see 'Cyber Security Information Sharing Partnership (CISP) - NCSC Site' (*Ncsc.gov.uk*, 2018) https://www.ncsc.gov.uk/cisp.

[893] For further information, see 'Cyber Crime is No Longer the Preserve of Bedroom Hackers' (*GOV.UK*, 2013) https://www.gov.uk/government/news/cyber-crime-is-no-longer-the-preserve-of-bedroom-hackers.

[894] 'Defence Cyber Protection Partnership' (*GOV.UK*, 2016) https://www.gov.uk/government/collections/defence-cyber-protection-partnership.

best practices related to IT education and training of end users.[895] A combination of the public sectors' role of 'policy management, regulation, ensuring equity, preventing discrimination or exploitation, ensuring continuity and stability of services, and ensuring cohesion with the private sectors' expertise and expediency at 'performing economic tasks, innovating, replicating successful experiments, adapting to rapid change, abandoning unsuccessful or obsolete activities, and performing complex or technical tasks'[896] would all be beneficial. However, it should be remembered that imposition of obligations on private sector entities could lead to excessive costs for them, which needs to be compensated.

6.3.2.2 International cooperation

The internet is fundamentally transnational, hence, threats are cross-border.[897] The transnational nature of cybercrime necessitates cooperation between various LEAs across geographical borders, through sharing their data and intelligence.[898] Hence, relying only on national measures, in particular on national laws, for tackling cybercrimes might not produce sufficient protection and can be even a 'waste of time'.[899] The country, therefore, needs to be more oriented towards the harmonisation of the relevant laws, and the development and implementation of formal mechanisms in accordance with these laws besides developing informal cooperation mechanisms. Harmonisation of legislation with the Convention on Cybercrime would reduce discrepancies between national laws, eliminate criminal safe havens, and enable transnational evidence collection. This will also assist the country to overcome the challenges arising from the transnational character of cybercrime, by making the laws globally applicable and interoperable, and by allowing global cooperation on cybercrime investigations and prosecution. This can potentially result in reducing the possible disagreements between the countries when the cooperation is needed, thus increasing the effectiveness and efficiency of

[895] World Economic Forum, *Recommendations for Public-Private Partnership against Cybercrime*, 2016.
[896] David Osborne and Ted Gaebler (n. 267), 30.
[897] The UK Cyber Security Strategy (2011), 3.4.
[898] Section 3.5., Chapter 3; See also section 5.3. Chapter 5.
[899] Katherine S. Williams (n. 287).

their fight against cybercrime. In addition to unilateral and multilateral efforts to deal with cybercrime through national legal frameworks and international mechanisms and instruments, increased cooperation between LEAs is vital for raising awareness about emerging cybercrime trends and potential mechanisms of criminal justice.[900]

Next, development of sufficient informal collaboration channels would help to avoid bureaucratic entanglements and delays in collecting digital evidence necessary for the investigation and prosecution of cybercrime cases, which can be opened through networking with foreign counterparts, for example, at international conferences.[901] Countries are recommended to make informal contact with the requested country before submitting a formal MLA request to find out whether a request can be carried out locally, specific information required in the formal requests, the best way to make a request, and languages and formats to be used.[902] Moreover, as, for example, data preservation requests do not typically require a formal MLA request, they can be initiated through informal channels while the formal request is being prepared.[903]

As regards cyber-specific requests, Azerbaijan needs to establish more specific regulation of requests for cooperating against cybercrime, given that traditional methods are extensively applied for cyber-specific requests, which have proven to be largely inefficient in dealing with transnational cybercrime. In addition, given that cooperation with 'foreign' private service providers has not been widely experienced due to a number of challenges to requesting digital evidence,[904] comprehensive and practical short, medium and long term plans should be developed to improve the situation with regard to requesting digital evidence.[905] It

[900] Ali Alkaabi, George Mohay, Adrian McCullagh, Nicholas Chantler, 'Dealing with the Problem of Cybercrime' In: Baggili I. (Edn.) *Digital Forensics and Cyber Crime.* ICDF2C 2010. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 53. Springer, Berlin, Heidelberg).
[901] Cameron S. D. Brown (n. 705), 92.
[902] Joshua I. James and Pavel Gladyshev, 'A Survey of Mutual Legal Assistance Involving Digital Evidence' (2016) 18 *Digital Investigation*, 24.
[903] Ibid.
[904] Section 5.3. Chapter 5.
[905] Gail Kent, 'Sharing Investigation Specific Data with Law Enforcement - An International Approach', (2014) Stanford Public Law Working Paper, 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413#.

should also be added that the United Nations Office on Drugs and Crime (UNODC) is working on the development on 'the Mutual Legal Assistance Request Writer Tool (MLA Tool)' which:

> '- Requires virtually no prior knowledge or experience with drafting mutual legal assistance requests
>
> - Helps to avoid incomplete requests for mutual legal assistance and therefore minimises the risk of delay or refusal.
>
> - Is easily adjustable to any country's substantive and procedural law
>
> - Enables the user to retrieve key information on treaties and national legislation
>
> - Features an integrated case-management tracking system for incoming and outgoing requests.' [906]

Next, law enforcement personnel, particularly, those functioning within 24/7 point of contact and the central bodies for delivering legal assistance should be provided with sufficient training and knowledge to be able to utilise the MLA related mechanisms available to them properly. Moreover, the personnel and coordinators of the contact points need to be selected based on strict professional criteria. Knowledge of domestic laws and policies, relevant knowledge of information technologies, and knowledge of the Council of Europe official languages should be considered as requirements for selection.

In summary, Azerbaijan needs to foster more effective and efficient international cooperation against cybercrime, and allocate more efforts and resources in international cooperation. In general, it would be beneficial for Azerbaijan to become a more active participant of the international community in learning and sharing experiences with other international actors also for improving the capacity for cross-border investigations and cooperation. The country should consider making full use of Articles 23 to 35 of the European Convention on Cybercrime in relations to police-to-police and judicial cooperation, including legislative adjustments and improved procedures.[907] Moreover, the effectiveness of international cooperation, as well as 24/7 contact points and other forms international cooperation should be reviewed on a regular basis through collecting

[906] UNODC, Mutual Legal Assistance Request Writer Tool, 2016 https://www.unodc.org/mla/.
[907] Council of Europe (n. 239), 12.

statistical data on international cooperation requests regarding cybercrime and electronic evidence and monitoring the quality of requests processing.[908] This would also help to identify good practices and eliminate obstacles to international cooperation.

6.3.3 Preventing cybercrime

Crime control and prevention can be considered as primary purposes of criminal justice. 'Crime control' denotes the maintenance and management of a given or existing level of behaviour,[909] while 'crime prevention' comprises strategies and measures aimed at reducing the risk of crimes occurring, and their potentially harmful impacts on individuals and society, including fear of the offence, through interventions that influence their multiple causes.[910] The United Nations Guidelines for the Prevention of Crime highlight that a leadership role in crime prevention should be played by all levels of government, which should also establish effective cooperation/partnerships working across ministries and between authorities, community organisations, non-governmental organisations, the business sector and private citizens.[911]

Having discussed the particular design and legal challenges presented by cybercrime in Chapter 2, organisation, methods and approaches adopted for cybercrime prevention need to reflect those challenges. Yet, neither a cybercrime prevention plan nor a general crime prevention plan encompassing clear priorities and objectives has been introduced in Azerbaijan, although such a plan is considered to be an integral part of the organisational aspect of crime prevention by the United Nations Guidelines for the Prevention of Crime.[912] The importance of prevention was also emphasised by the UK Cybersecurity Strategy 2011, which makes it clear that 'the prevention is key', and therefore, work should be conducted

[908] Ibid. 12.
[909] Steven P. Lab, *Crime Prevention: Approaches, Practices, and Evaluations* (9th edn. Routledge, 2016) 29.
[910] UNESC (n. 342), para 3.
[911] Ibid, para 7 and 9.
[912] İbid, para 17, see also, for further discussion, Section 3.6. Chapter 3.

‘to raise awareness and to educate and empower people and firms to protect themselves online’.[913]

In addition to a plan with clear priorities and targets, the government also needs to develop a comprehensive approach for the organisation of cybercrime prevention, by establishing:

> ‘centres or focal points with expertise and resources; linkages and coordination between relevant government agencies or departments, as well as partnerships with non-governmental organizations, the business, private and professional sectors and the community; [and] by seeking the active participation of the public in crime prevention by informing it of the need’.[914]

As regards to awareness raising, a national plan or a program integrating the cooperation of a multitude of governmental institutions and private actors can be launched to raise awareness in the country, though increasing threat awareness might not immediately lead to behaviour change. It is, therefore, necessary to conduct regular evaluations (such as through surveys/questionaries) among internet users to see whether applied awareness-raising techniques have been useful and to make adjustments according to the results. As regards effective partnerships with non-governmental organizations, the business, private and professional sectors and the public, collaborative arrangements and joint industry and government initiatives established in the UK (such Cyber Security Information Sharing Partnership (CISP), Cyber Crime Reduction Partnership (CCRP), Defence Cyber Protection Partnership (DCPP) might be considered.[915] The government also needs to strive to develop cybercrime prevention skills through training and capacity building further and achieving sustainability of demonstrably effective crime prevention programmes and initiatives.[916]

In general, the model provided by UK National Cyber Security Strategy 2016-2021 can be applied to measure the success in preventing cybercrime. It suggests that progress towards the following outcomes needs to be assessed to do this: a full

[913] The UK Cyber Security Strategy (2011), 4.5.
[914] UNESC (n. 342*),* para 17.
[915] See Section 6.3.2. of this Chapter for further discussion.
[916] UNESC (n. 342), para 18-20.

understanding of risk posed by cybercrime, through identification and investigation of cybercrime threats to the country; and close monitoring, and disruption of cybercriminal capability at the earliest opportunity, with the aim of preventing an increase in such cybercriminal capability in the long term.[917]

6.4 Enhancing Legal Responses

The role of existing legal measures and laws in the prevention and combating of cybercrime was extensively studied in the preceding Chapters. It was defended in Chapter 3 and 4 that as a relatively dynamic tool enabling the state to respond to new societal and security challenges, the law identifies acts as crimes, defines the tools for addressing them as well as distributes the roles and powers of actors in this fight.[918] To be more specific, criminal and procedural laws, as a source of authoritative standards, are the foundation for the main processes of combatting, primarily investigating and prosecuting serious social wrongs such as cybercrimes. However, as also noted in Chapter 4, laws also reflect a slow dynamic of development and enforcement, and thus, can become easily outdated in the virtual world. Therefore, to effectively control and prevent cybercrime, the mechanism of the legislative amendment should also be dynamic.

Furthermore, not only substantive criminal laws and investigatory powers are needed for the prevention and combating of cybercrime. Based on the analysis of legal responses in Azerbaijan in Chapters 3, 4 and 5, it can be emphasised that in addition to criminalisation and extra investigatory powers, effective and efficient fight against cybercrime also requires the legal measures to address jurisdiction, electronic evidence and international cooperation. Attention to these issues will allow for ‘an arsenal of well-defined cybercrime offences for use in prosecuting cybercriminals, and procedural rules governing evidence-gathering and investigation’ at both international and national levels.[919]

[917] The UK National Cyber Security Strategy 2016 to 2021, 50.
[918] See Section 3.3. Chapter 3; see also, Section 4.1. Chapter 4.
[919] Susan W Brenner (n. 356).

Consequently, Azerbaijan needs to ensure that its legal measures cover all the areas necessary to appropriately responding cybercrime. It is also important to harmonise the laws in a way that will reduce discrepancies between national legislation, eliminate criminal safe havens and enable transnational evidence collection.[920] However, relying only on national legislation for tackling cybercrimes might not produce sufficient protection and can be even a 'waste of time'.[921] The modern information systems exhibit transnational and borderless character, which is also reflected in the attacks that are often trans-border, and therefore, there is a need for further harmonisation of relevant laws in these areas.[922] So, to adequately criminalise conduct, provide law enforcement with necessary investigatory powers as well as to establish safeguards and conditions limiting those powers the laws should be harmonised with international standards.[923]

6.4.1 Substantive criminal law

When reflecting upon the criminalisation provisions in Chapter 4, it was noted that the dominant source of criminal norms in Azerbaijan is the Criminal Code. So, the Criminal Code needs to ensure that the 'most common and internationally widely accepted forms of cybercrime, as well as those offences that are of specific interest for the region', are adequately covered.[924] It is vital to address criminalisation gaps and differences resulting from general principles and provisions of the criminal law applied to cybercrime.

6.4.1.1 General provisions

It was highlighted in Chapter 4 that the criminalisation of acts is dependent on the extent to which the society and legislators perceive those actions as harmful/dangerous.[925] Regarding cybercrime as either a 'crime not representing

[920] UNODC (n. 71), 60-61.
[921] Katherine S. Williams (n. 287) 53.
[922] EU Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, para. 5.
[923] Alexander Seger (n. 819) 15.
[924] ITU, *Cybercrime/e-crimes: Model policy guidelines and legislative texts*. (HIPCAR. BDT, Geneva. 2012) 12.
[925] See Section 4.3, Chapter 4.

great social danger' or a 'minor crime' directly reflects the government's views, which is based on reactions of its citizens to the problem. Perceiving the problem in this way may result in the full array of responses of the country to cybercrime being rendered inadequate and may lead to reluctance to becoming closely involved in international cooperation, especially with regard to prioritising incoming requests. If one state assumes a crime to be of 'low priority', it might not prioritise an incoming request from a state, which believes the crime is of 'high priority'.[926] As discussed in Chapter 4, criminal law in Azerbaijan has been widely reactive and focused on harm or the threat to harm.[927] However, continuing technological, social, and legal-political trends have necessitated the crime control to do more than simply manage problems of crime and insecurity.[928] Therefore, criminal law in Azerbaijan should be inclined to shift to 'a new paradigm',[929] by becoming more proactive and preventative, and more focused on risk, rather than being primarily reactive and focused on harm.

Another general provision of the Criminal Code affecting cybercrime offences to be addressed is the minimum age of criminal responsibility (MACR) for cybercrime offences. As discussed in Chapter 5, in Azerbaijan, individuals under the age of 16 who commit cybercrime act cannot be charged with committing those acts as the law sees them as incapable of having committed those acts. Fixing the MACR at this age level might become problematic from the perspective of combating cybercrime, as young people are increasingly involved in online delinquency and can be drawn into cyber-criminality.[930] For example, albeit that the setting of the MACRs for cybercrime is not internationally uniform, the median MACR for

[926] Joshua I. James and Pavel Gladyshev (n. 902), 23.
[927] Section 4.3, Chapter 4.
[928] David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (OUP Oxford, 2001) 194.
[929] Bert-Jaap Koops, 'Technology and the Crime Society: Rethinking Legal Protection', (2009) 1 *Law, Innovation and Technology*, 116.
[930] See for example, 'Fifth Arrest in Talktalk Investigation' (*Metropolitan Police,* 2015) http://news.met.police.uk/news/fifth-arrest-in-talktalk-investigation-139221; see also, Martin Evans, 'Teenager Who Hacked Governments Worldwide Is Spared Jail' (*The Telegraph,* 2016) http://www.telegraph.co.uk/news/2016/07/20/teenage-hacker/. It was reported that the 16-year-old from Plympton in Devon, began hacking the sites of organisations and governments he disagreed with when he was just 14.

cybercrime among the States Parties to the Convention is 13.6 years.[931] It would, thus, be desirable to align the MACR for cybercrime with this median age. Given the importance of international standards, criminological, psychological and neurological implications, as well as the ongoing online delinquency and cyber-criminality trends, setting the MACR at 14 years of age for cybercrime seems to be less problematic for establishing appropriate measures for dealing with child offenders.[932]

When elaborating the provisions of corporate liability in Chapter 4 it was also highlighted that legal entities do not incur criminal liability for the commission of offences related to infringements of copyright and related rights. Thus, Azerbaijan needs to ensure that legal persons can be held liable for a criminal offence established in accordance with the Convention on Cybercrime. Article 94-4.2 of the Criminal Code clarifies that corporate liability does not exclude individual responsibility. It can, however, be argued that corporations, associations and similar legal persons should also be held criminally liable, at least, for intentional infringements of an intellectual property right on a commercial scale as well as for attempting, aiding or abetting and inciting such infringements. A range of penalties should be imposed on legal persons, such as 'fines; and confiscation of the object, instruments and products stemming from infringements or of goods whose value corresponds to those products', as laid down by an EU Proposal for a Council framework decision to strengthen the criminal law framework to combat intellectual property offences.[933]

6.4.1.2 Specific provisions

Before embarking upon the analysis of specific offences in Chapter 5,[934] the meanings of the underlying concepts that relevant criminal acts imply were explored. It was concluded that elements of the definition of surrounding concepts

[931] Elvin Balajanov (n. 438).
[932] Ibid. 15.
[933] Article 4, *Proposal for a Council framework decision to strengthen the criminal law framework to combat intellectual property offences (Brussels* 2005), COM (2005)276 final, 2005/0127(COD) 2005/0128(CNS).
[934] See Sub-section 4.3., Chapter 4.

to the term ‘cybercrime’ in the Criminal Code are predominantly similar to those incorporated in the Convention on Cybercrime due to the harmonisation required by ratification. However, the Convention does not contain all necessary definitions, and Azerbaijan, thus, needs to establish necessary clarifications for key terms associated, the meanings of which are inherent to understanding the objects and/or protected legal interests which cybercrime acts concern.[935]

Such key terms include:

- ‘Computer programme’. Common elements of this term can be summarised as ‘instructions [in machine-readable form] that [enable a computer/information system to [process computer data/information] [perform a function/operation]] [can be executed by a computer/information system]’. [936]
- ‘Device’. This is particularly used in relation to the criminalization of ‘misuse devices’.[937] The definition contained by the HIPCAR Model Legislative Text can be adopted:

  ‘Device includes but is not limited to

  a. components of computer systems such as graphic cards, memory, chips;

  b. storage components such as hard drives, memory cards, compact discs, tapes;

  c. input devices such as keyboards, mouse, track pad, scanner, digital cameras;

  d. output devices such as a printer, screens.’[938]

So, the legislator should focus on ensuring sufficiently broad wording in the definition of concerning terms, coupled with a list of illustrative examples and training materials to provide investigators, prosecutors, judges as well as other stakeholders with the necessary interpretation of those terms.[939]

Analysis of specific cybercrime offences in Chapter 4 has also revealed certain criminalisation gaps and inconsistencies that might lead to challenges to effective and efficient transnational cooperation against cybercrime. The criminal legislation

[935] UNODC (n. 71), 12.
[936] Ibid.13.
[937] Article 273-1, Criminal Code (1999), see for discussion, Sub-section 4.3.2., Chapter 4.
[938] ITU, *Cybercrime/e-crimes: Model policy guidelines and legislative texts* (HIPCAR. BDT, Geneva. 2012) Section 3.
[939] UNODC (n. 71), 11.

must, therefore, be made more compliant with both international standards and best practices, as well as to existing regional standards and best practices.

Based on the analysis of cyber-specific and general offences in Chapter 4, Azerbaijan should consider the following recommendations to develop its criminal law responses to cybercrime.

Illegal access: Mere unauthorised access to a computer system should not be required to include 'infringement of security measures' for it to be a crime. A broader scope of protection should be merited for computers, because the level of control to prevent digital spaces from intrusions is lower, for example than for private physical spaces. It should also be taken into account that the use of licensed computer security software among general publicity has not yet reached a sufficient level in Azerbaijan.

More proportional punishment should be imposed for 'Illegal access' in the absence of aggravating circumstances, rather than a deprivation of liberty for a term of up to two years. It is difficult to assess the material nature of damage that can assist in examining the proportionality of that counter-action in this case. Yet, individuals involved in illegal access are also potentially more reformable in that they could be convinced more easily to use their skills for good, rather than for criminal purposes.[940] Notably, however, as a result of the changes made by sections 41 – 44 of the UK Serious Crime Act 2015, the punishment stipulated by the UK Computer Misuse Act 1990 for unauthorised access to computer material has been increased from imprisonment for a term not exceeding six months to imprisonment up to two years (on indictment).

However, the presence of aggravating circumstances, particularly, for the commission of an act against computer system of 'infrastructure facility of public importance or any part thereof', might merit a stricter punishment than presently a deprivation of liberty for a term of up to six years in Azerbaijan.[941] In the UK, for

[940] David S. Wall (n. 73).
[941] See Sub-section 4.3.2., Chapter 4.

example, unauthorised acts causing or creating a significant risk of serious damage to human welfare or national security could result in life imprisonment.[942] Yet, a life term may not seem to be a reasonable response, especially when considering that these provisions could be misused to target political opposition and dissent as well as whistle-blowers in Azerbaijan.

Illegal interception/acquisition of computer data: The criminalisation of illegal interception should also be expanded to cover the 'confidentiality of private communications', besides the integrity of 'data' and 'electromagnetic emissions…carrying such computer data'. Breach of confidentiality in private communications should be the major concern behind the criminalisation of the interception of computer data.[943] The legal object to be protected from an unlawful interception in the UK, for example, is 'communication in the course of its transmission' according to section 3 of the UK Investigatory Powers Act 2016.[944] Moreover, Article 5(1) of the Directive on Privacy and Electronic Communications also provides that 'the confidentiality of communications and the related traffic data using a public communications network and publicly available electronic communications services" should be ensured.[945]

The sanctions determined for 'Illegal interception/acquisition of computer data' should be stricter than those for 'illegal access'. The imposition of identical punishments for these two distinct offences raises the question of effectiveness, proportionality and dissuasiveness of the sanctions imposed. This is due to the reason that the main concern of 'illegal interception' is non-public computer data, while 'unauthorised access' protects the security (confidentiality, integrity and availability) of the computer system and public computer data stored in this computer system. Thus, it can be argued that the interception of public and non-

[942] Section 3ZA (7), UK Computer Misuse Act 1990.
[943] Ian Walden, *Computer Crime and Digital Investigations* (OUP, Oxford, 2007), 184.
[944] Section 3 (1), UK Investigatory Powers Act 2016.
[945] European Commission, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications*)* Article 5(1).

public computer data should be regarded differently and should not be prescribed same levels of punishment.

Illegal interference. The clarification of different acts covered needs to be provided by the legislation. In this sense, the Explanatory Report to the Convention on Cybercrimes can be helpful to illustrate the meaning of the acts. According to the Explanatory Report,

> ‘‘damaging’ and ‘deteriorating’ relate in particular to a negative alteration of the integrity or of the information content of data and programmes;
>
> ‘deletion’ of data is the equivalent of the destruction and making them unrecognisable;
>
> ‘suppressing’ of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored;
>
> ‘alteration’ means the modification of existing data.’ [946]

Identical punishments, which are neither proportionate nor dissuasive, should not be imposed for acts differing from each other if harm is included as a necessary element. For example, the same levels of criminal punishment, which is two years’ imprisonment in the absence of aggravating circumstances, is determined both for mere illegal access to a computer system/data and for illegal interference with a computer system/data. As suggested by Edmund O’Neil, ‘the law must endeavour to keep the costs of criminal conduct high’.[947] The imprisonment for a period of up to two years for the act resulting in a large scale of financial losses cannot be considered as an effective deterrent. Comparing it, for example, to the punishment imposed for the ‘deliberate destruction or damage of property’, it can be seen that the approach adopted for sanctioning cybercrimes is inconsistent with the general philosophy of sanctioning adopted by national criminal law.[948]

---

[946] see *Explanatory Report to the Convention on Cybercrime* (2001) para. 61.
[947] Michael Edmund O’Neill, ‘Old Crimes in New Bottles: Sanctioning Cybercrime’ (2000) 9 George Mason Law Review, 253.
[948] See Article 186, Criminal Code (1999). Deliberate destruction or damage of property is sanctioned by imprisonment for a period of up to seven years when inflicting damage on a large scale.

This inconsistency becomes even more notable when compared, for example, to the approach adopted by the UK Computer Misuse Act 1990. According to the section 3ZA(6) of the Act, unauthorised acts that cause, or create the risk of, serious damage are punishable with a sentence of 14 years in prison or to a fine, or to both.[949] Furthermore, section 3ZA of the Act has a maximum of life imprisonment (on indictment), or a fine, or both, where an offence is committed as a result of an act causing or creating a significant risk of serious damage to human welfare or to national security.[950] In Azerbaijan, the commission of the same act against the computer system of any 'infrastructure facility of public importance or any part thereof' is punished by imprisonment for a period of four to six years, which is significantly lenient. As previously noted, in Azerbaijani context, imposition of life term might not be the best option, albeit tougher sanctions for this particular offence would be largely proportionate.

Misuse of Devices: The presence of harm should be considered in determining a range of penalties as the imposition of equally severe punishments (imprisonment for a term not exceeding two years) regardless of the presence of harm does not seem sensible. Moreover, the infliction of harm/damage in 'large quantities' should be regarded as a separate aggravating circumstance with the requirement of more aggravated penalties than the penalties determined for a crime followed by the infliction of a 'significant harm'. For example, 'Crimes against the property' (Chapter 23) are punished based on the size/quantity of the harm/damage and the Code distinguishes between 'damage in the significant size' and the 'damage in large size' and determines a stricter punishment for the latter. It provides that 'the significant size' shall be understood as sum at a rate of from three up to ten thousand (AZN), and 'the large size' as over ten thousand (AZN). In terms of cybercrime offences, the Criminal Code (1999) refers only to 'significant harm', which is understood as material damage at a rate of at least one thousand AZN.

[949] Section 3ZA (6), UK Computer Misuse Act 1990.
[950] Ibid. Section 3ZA (7).

Computer-related fraud and forgery: As noted in Chapter 4,[951] unlike computer-related forgery, which was created as a parallel offence to traditional forgery, the Criminal Code does not contain cyber-specific provisions criminalising computer-related fraud. Therefore, Azerbaijan needs to introduce cyber-specific offences for computer-related fraud, because, prosecution of computer fraud under a combination of general 'fraud (swindle)' (Article 178) and 'illegal access' (Article 271) provisions might result in inefficiency of prosecution of suspects. Moreover, introducing cyber-specific offences for computer-related fraud would help to address legal uncertainties regarding the applicability of offline fraud provisions. Alternatively, existing deficiencies and uncertainties can be dealt through further clarifications that can ensure that the scope of protection adequately covers computer-related fraud offences. The UK Fraud Act 2006, for example, introduced a new general offence of fraud, which could be committed by false representation, by failing to disclose information, and by abuse of position. Clarification of fraud by false representation is of particular importance, as it would ensure that phishing offences are adequately criminalised.[952] It was provided by the Fraud Act 2006 that 'a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)'.[953]

As regards computer related-forgery, it is important to clarify the acts covered by Article 273-2 regarding the computer-related forgery (such as input, alteration, deletion, or suppression of computer data). Clarifications of these acts provided by the Explanatory Report to the Convention on Cybercrime could be used since Azerbaijan has made no reservations regarding the provisions of computer-related forgery determined by the Convention on Cybercrime. According to the Explanatory Report, the unauthorised 'input' must correspond to the making of a false document, while subsequent alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back,

[951] Section 4.3.2., Chapter 4.
[952] Section 1(2), UK Fraud Act 2006 (UK).
[953] Ibid. Section 2(5).

concealment of data) correspond in general to the falsification of a genuine document.[954]

In addition, either a set of aggravating circumstances with the requirement of aggravated penalties for crimes of computer related forgery should be introduced, or a stricter penalty depending on the harm inflicted as a result of the act should be allotted. For example, a person guilty of the offence of forgery in the UK is liable on conviction on indictment to imprisonment for a term of up to ten years, according to the Forgery and Counterfeiting Act 1981 (UK).[955]

Identity theft: Notwithstanding that the Criminal Code protects certain legal interests which can be attacked by using identity-related information,[956] identity theft is not criminalised as a separate offence. The importance of setting up effective measures against identity theft and other identity-related offences is acknowledged by the EU Directives on attacks against information systems as constituting an important element of an integrated approach against cybercrime.[957] Introducing a specific provision focusing on protecting identity-related information would help to ensure the integrity and security of all forms of identity-related information and to close existing gaps. When doing so all three phases of identity theft ('obtaining through transfer'; 'possessing'; and 'using the identity-related information') must be taken into account. Since the Convention of Cybercrime does not contain a specific provision related to identity theft offences, Article 14 of the ITU HIPCAR Model Legislative texts can be used as a benchmark:

> 'A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits

[954] *Explanatory Report to the Convention on Cybercrime* (2001), para 83.
[955] Section 1. UK Forgery and Counterfeiting Act 1981 (UK).
[956] See Sub-section 4.3.2., Chapter 4 for further discussion.
[957] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems (NIS Directive), para 14 (Preamble).

an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.'[958]

Alternatively, Section 2 of the UK Fraud Act 2006, making provisions for computer related identity theft and impersonation, might be used as a guide:

'(1) A person is in breach of this section if he —
(a) dishonestly makes a false representation, and
(b) intends, by making the representation—
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.'[959]

Infringements of copyright and related rights: Considering the high rates of piracy and low levels of actual protection of copyright and related rights in Azerbaijan, the condition of 'large' damage as a prerequisite for criminal sanctions for infringements of copyright and related rights should be re-evaluated. The consensus is also needed to foster better cooperation against copyright infringements internationally, particularly with countries, which apply criminal sanctions with no threshold condition. Moreover, the element of 'wilfulness' should be explicitly attached to the provisions of criminalisation determined by Article 165, as well as by Articles 165-1, 165-2, 165-3, which is also acknowledged as a prerequisite for the criminalisation of infringements of copyright and related rights pursuant to Article 10 of the Convention on Cybercrime.

Next, Chapter 4 also drew attention to the discrepancy between the maximum penalties for online and physical offences while reviewing the sanctions imposed for infringements of copyright and related rights.[960] Disparity in sentencing between online and offline crime could send out all the wrong messages with regard to their significance, as was argued by Mike Weatherley MP to justify the need for harmonising sentencing in the UK.[961] Online copyright infringement dealt with under s107(2A) and s198(1A) of the UK Copyright Designs and Patent Act 1988,

[958]Article 14, ITU, *Cybercrime/e-crimes: Model policy guidelines and legislative texts*. (HIPCAR. BDT, Geneva. 2012).
[959] Section 2 (1), the UK Fraud Act 2006.
[960] See Sub-section 4.3.2. Chapter 4.
[961] Mike Weatherley MP, 'Follow the Money': Financial Options to Assist In The Battle Against Online IP Piracy (A Discussion Paper, 2014) 6.9.

were punishable by a maximum of two years imprisonment in the UK, while the maximum custodial sentence for infringement in respect of physical goods was ten years.[962] In 2015, the UK government launched a consultation on plans to increase the sanctions for criminals (from 2 to 10 years imprisonment) who infringe the rights of copyright holders for large-scale financial gain and will make clear that online copyright infringement is no less serious than physical infringement.[963] Although, the proposed increase in maximum sentence was criticised for being the same or higher than other serious offences such as rape, some firearms offences, rioting and child cruelty, the Government believed that a maximum sentence of 10 years, which is currently imposed,[964] would allow the courts to apply an appropriate sentence to reflect the scale of the offending.[965] So, in line with the above, it can be recommended that to establish a further deterrence to copyright related crimes, stricter sanctions should be introduced. In addition, availability of more diverse sanctions, such as, deprivation of the right to hold certain positions or engage in certain types of activities, besides imprisonment for a certain period, would allow the courts to apply more appropriate sentences to reflect the scale of the offending.

As noted in Chapter 4, the LEAs in Azerbaijan have not provided with necessary resources to deal with a large amount of copyright infringement cases. However, even if they were allocated an adequate level of resources, it would still be insufficient to prosecute the majority of all detected cases. One could argue that graduated response measures or 'three strikes and you're out' model that was comprised by the UK Digital Economy Act 2010 (DEA), might be exercised to address the challenges, in which Internet access is suspended or terminated by a user's ISP following the user's receipt of three successive notices of copyright

[962] Intellectual Property Office, 'A consultation on changes to the penalties for offences under sections 107(2A) and 198(1A) of the Copyright, Designs and Patents Act 1988 (Penalties for Online Copyright Infringement)' (2015).
[963] 'Changes to Penalties for Online Copyright Infringement' (*GOV.UK*, 2015) https://www.gov.uk/government/consultations/changes-to-penalties-for-online-copyright-infringement.
[964] See s107(2A) and s198(1A), the UK Copyright Designs and Patent Act 1988.
[965] Intellectual Property Office, 'Criminal Sanctions for Online Copyright Infringement: Government Consultation Response' (2016).

infringement.[966] Although, the system seemed to be theoretically simple, practically it was flawed to a substantial degree and thus, the government abandoned its implementation.[967] The Internet Service Providers' Association (ISPA) suggested that the issue of online copyright infringement might be more effectively tackled if the content industry continued to innovate to fully embrace the benefits the internet affords though fully licensed and user-friendly services.[968] A global licensing theme was also considered as a better alternative instead of resorting to tactics, such as, terminating subscribers internet connections to strike a fairer balance between the interests of copyright holders and users. In *Twentieth Century Fox Film Corp v Newzbin Ltd*, the court recognised the possibility of s.97A of the Copyright Designs and Patent Act 1988 being used to grant blocking injunctions against ISPs, especially where that service provider has actual knowledge of another person using their service to infringe copyright. [969] So, instead of holding the users/individuals accountable, ISPs would be required to block access to infringing websites, which would prevent user access at source. This approach would also be more effective in Azerbaijani context. In addition, the close involvement of ISPs in fighting copyright infringers through registering their IP addresses and taking actions by also collaborating with rights-holders and authorities would also ease the current situation in Azerbaijan.[970]

Azerbaijan further needs to introduce provisions dealing with cybersquatting or domain squatting, a term used to describe the bad faith, abusive registration of

[966] Business Software Alliance, BSA Position on Appropriate Measures to Deter Online Piracy of Content; see also, Annemarie Bridy, 'Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement. (2010) 89 *Oregon Law Review*, 84; Romero Moreno, F., 'The Three Strikes and You Are Out Challenge' (2012) 3 European Journal for Law and Technology.

[967] Dinusha Mendis, 'Digital Economy Act 2010: fighting a losing battle? Why the 'three strikes' law is not the answer to copyright law's latest challenge' (2013) 27 *International Review of Law, Computers & Technology.*

[968] 'Three Strikes and You're out? Delays Are Costing the UK's Piracy Laws -Intellectual Property Magazine' (*Intellectualpropertymagazine.com*, 2018) https://www.intellectualpropertymagazine.com/incoming/three-strikes-and-youre-out-delays-are-costing-the-uk-s-piracy-laws-87365.htm.

[969] *Twentieth Century Fox Film Corp v Newzbin Ltd* [2010] EWHC 608 (Ch).

[970] See for further collaboration practices and mechanisms, Thomas Hoeren, Guido Westkamp,*Study on voluntary collaboration practices in addressing online infringements of trade mark rights, design rights, copyright and rights related to copyright* (EUIPO 2016); see also, Infringements of Intellectual Property Rights on the Internet (2014),(A conference co-chaired and hosted by the Office for Harmonisation in the Internal Market (OHIM), Europol and Eurojust).

Internet domain names.[971] However, it is more proportionate not to regard the problem as a criminal matter. For example, currently, no specific criminal legislation against cybersquatting exists in the UK, where cybersquatting is challenged through litigation under either the Trade Marks Act 1994 or passing-off law.[972] The courts have assessed the conduct with the aim of deciding whether a conduct may or may not have been 'Infringement of registered trade mark' per se.[973] Alternatively, the abusive registration of domain names is claimed through the UK's domain name registration authority's Dispute Resolution Service - Nominet, which is claimed to be 'a fast, efficient way to resolve *.uk* domain name disputes'.[974] The Nominet Dispute Resolution Service Policy could be transferred as a comprehensive tool to establish the rules and procedures governing the complaint about someone else's domain name registration in Azerbaijan.[975]

Content – related offences: As provided in Chapter 4, many content-related acts have been criminalised in Azerbaijan despite the absence of concrete harm caused to others. Although, the harm principle does indeed sound sensible, its practical use might become challenging with regard to the scope of criminalisation of the content-related offences. Azerbaijan should impose a higher threshold to criminalising offences relating to defamation, obscene material, and insult.

As regards the criminalisation of pornography, it is important to clearly define what amounts to 'legal dissemination, preparation or trading' with pornographic materials.

---

[971] *Anticybersquatting Consumer Protection Act (ACPA*), 15 U.S.C. § 1125(d).
[972] Shereen Abu Ghazaleh, 'Fighting Cybersquatting: Nominet Disputes Resolution Service Policy' (2011) *32 Business Law Review*, 31–34; see also; *British Telecommunications Plc and Others v. One in a Million* [1999] 1 WLR 903.
[973] Trade Marks Act 1994, s.10; see also, Chris Dent, 'Confusion in a Legal Regime Built on Deception: The Case of Trade Marks' (2015) 5 *Queen Mary Journal of Intellectual Property*.
[974] 'UK Domain Dispute Resolution Service' (*Nominet,* 2017) https://www.nominet.uk/domains/resolving-uk-domain-disputes-and-complaints/
[975] The Dispute Resolution Service Policy – Nominet, https://s3-eu-west-1.amazonaws.com/nominet-prod/wp-content/uploads/2017/10/17150434/final-proposed-DRS-policy.pdf; see Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press 2016).

'Procuring child pornography through a computer system for oneself'[976] and 'possessing child pornography in a computer system or on a computer-data storage medium'[977] should also be criminalised. This is also because Azerbaijan, as a signatory to the UN Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, also has certain obligations to the UN in terms of criminalizing the intentional possession of child pornography.[978] At the very least, the elements of 'intentionality' and 'without right' should be clarified and explicitly contained in Article 171-1, which are deemed to be necessary elements of criminalization of a child-pornography according to Article 9 of the Convention. Otherwise, the scope of criminalization becomes broadened and might be interpreted to cover the accidental dissemination of child pornography by a person who 'merely possesses', as well as sending material for criminal investigation purposes.

As regards to 'Incitement to national, racial, social or religious hostility' the concepts such as 'incitement of national, racial, social or religious hatred and hostility, or 'humiliation of national dignity' should be clearly defined to avoid serious consequences to freedom of expression in Azerbaijan.[979]

Cyberstalking has not been attended to by the Criminal Code in Azerbaijan, as noted in Chapter 4.[980] So, specific provisions should be introduced to criminalise cyberstalking, especially because proliferation of social networking platforms has given a rise and opportunity for the commission of cyberstalking, which can potentially have adverse physical and psychological consequences on individuals.[981] It should also be ensured that provisions introduced to criminalise

[976] Article 9.1 (d), *Convention on Cybercrime* (2001).
[977] Ibid. Article 9.1 (e),
[978] Article 3.1, UN General Assembly, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 16 March 2001, A/RES/54/263, Azerbaijan has signed it in 2000 and ratified in 2002.
[979] See Sub-section 4.3.2., Chapter 4.
[980] Ibid.
[981] Harald Dreßing et al., 'Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact upon Victims' (2014) 17 Cyberpsychology, Behavior, and Social Networking, 61-67.

cyber-stalking do not criminalise free expression, although it would be challenging to achieve in Azerbaijan.

To tackle the growing problem of cyberstalking in the UK a range of laws have been put in place, including Malicious Communications Act 1988, the Protection from Harassment Act 1997, Criminal Justice Act 2003, the Regulation of Investigatory Powers Act 2000, and Investigatory Powers Act 2016. These can be considered when working on the criminalisation of cyberstalking offences in Azerbaijan. Adopting the provisions criminalising the improper use of public electronic communications network for the commission of cyberstalking, contained by the section 127 of the Communications Act 2003, would be especially beneficial. It provides that a person be guilty of an offence 'if he sends using a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or causes any such message or matter to be so sent'.[982] If a message does not create a fear or apprehension in those to whom it was communicated, or who may reasonably be expected to see it, it should not be regarded as cyberstalking, due to the very simple reason that the message lacks menace.[983]

6.4.2 Procedural laws and powers

A comprehensive approach needed to fight against cybercrime necessitates the incorporation of adequate procedural instruments along with substantive criminal laws to enable the effective and efficient prosecution and adjudication as well as cooperation against cybercrime of cybercrime. As concluded in Chapter 5, procedural laws are insufficient in combating cybercrime, and not in line with the relevant Convention on Cybercrime provisions. While, 'the collection of evidence in electronic form of a criminal offence' must be realised through the powers and procedures set out in criminal procedure legislation, which also necessitates the incorporation of the relevant provisions established by the Convention on

[982] Section 127 (1), UK Communications Act 2003.
[983] *Chambers v DPP [2012] EWHC 2157*, para 30.

Cybercrime.[984] Therefore, Azerbaijan needs to bring its criminal procedure laws in line with the Convention on Cybercrime.

Furthermore, the lack of cyber-specific provisions and adequate legal instruments also leaves human rights and liberties at risk of being compromised. Therefore, besides developing cyber-specific powers and instruments, it is vital to ensure that the powers and instruments do not interfere with the internationally as well as regionally accepted the fundamental rights of the suspect.

6.4.2.1 Clarifying the legal status of digital evidence

As provided in Chapter 5, the Code of Criminal Procedure provides general investigative powers and techniques for the investigation of cybercrime. Thus, there is a lack of specific legal provisions about digital evidence, which poses serious challenges to the collection, analysis, authentication and evaluation of digital evidence.[985] Notwithstanding that some of these investigative actions can be achieved through the application of traditional powers, most procedural provisions cannot be translated well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. Therefore, the combination of both traditional and new investigative techniques is required to address these challenges.[986] Consequently, the identification, collection, analysis of digital evidence as well as its presentation and use in court proceedings necessitates the optimisation of legal frameworks for digital evidence, alongside with law enforcement and criminal justice capacity. In addition, proper handling and processing of digital evidence would help to avoid undue invasion of privacy.[987]

Given that neither the national law nor the Convention on Cybercrime contains a definition of digital evidence, a specific definition of digital evidence should be added in the Criminal Procedure Code to implement provisions of the Convention on procedural measures as well as to increase legal clarity. This would also ease the drafting of specific procedural measures. Alternatively, it is recommended by

[984] Article 14, Council of Europe Convention on Cybercrime (2001).
[985] Section 5.2.1. Chapter 5.
[986] Eoghan Casey, *Handbook of Digital Forensics and Investigation (*Academic Press 2009) 27-28.
[987] Ibid. 9.

the Council of Europe that the concept of electronic evidence be included as part of material evidence under Article 128 of the Code, through an amendment which specifically recognises materials in electronic form as part of material evidence.[988]

Introduction of specific norms on digital evidence is also required. For instance, it became evident in Chapter 5 that the position surrounding the admissibility of digital evidence is still contentious in Azerbaijan. According to the Code of Criminal Procedure, there must be no doubt as to the accuracy, source, and the reliability of evidence for it to be admissible in criminal proceedings.[989] However, these conditions have not been clarified by the Code, nor is there a comprehensive national guidance available to be followed when dealing with digital evidence. As Allan states, the introduction of clear and transparent legislation would help to reduce the scope for technical objections to the admissibility of digital evidence.[990] *The Electronic evidence guide - A basic guide for police officers, prosecutors and judges*, [991] developed within the CyberCrime@IPA joint project, for example, can be used as a template document in doing so, that can be adapted and customised in accordance with national legislation, practice and procedure. This guide focuses on a wider audience including judges, prosecutors and others involved in the justice system, as well as private sector investigators. The principles identified by the guide can be considered as a basis for all dealings with digital evidence:

> "Principle 1 – Data Integrity: No action taken should materially change any data, electronic device or media which may subsequently be used as evidence in court.
> Principle 2 – Audit Trail: A record of all actions taken when handling electronic evidence should be created and preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions but also to achieve the same result.

---

[988] Council of Europe, *Suggestions for draft amendments to procedural legislation of Azerbaijan and other recommendations concerning cybercrime and electronic evidence* (Cybercrime@EAP III Project 2017) 4.
[989] Article 125, Criminal Procedure Code (2000).
[990] Gregor Allan, 'Responding to cybercrime: A delicate blend of the orthodox and the alternative.' (2005) 2 *New Zealand Law Review,* 149-178.
[991] Jones, N., George, E., Insa Mérida, F., Rasmussen, U., Völzow, V.*, Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges* (CyberCrime@IPA, EU/COE Joint Project on Regional Cooperation against Cybercrime 2014).

Principle 3 – Specialist Support: If it is expected that electronic evidence may be found in the course of a planned operation, the person in charge of the operation should notify specialists/external advisers in time and to arrange their presence if possible.
Principle 4 – Appropriate Training: First responders must have the necessary and adequate training to be able to search for and seize electronic evidence if no specialists are available at the scene.
Principle 5 – Legality: The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed to the letter."[992]

The Good Practice Guide for Digital Evidence[993] published by the Association of Chief Police Officers (ACPO) in the United Kingdom can also be considered as a suitable set of guidelines when establishing national rules and protocols for dealing with digital evidence. Besides assisting law enforcement, the document is also aimed at providing assistance for all that involves in investigating cyber security incidents and crime. Similar to the approach adopted in Azerbaijan about electronic evidence, the guide stipulates that computer-based electronic evidence be subject to the same rules and laws that apply to documentary evidence, which involves four principles:

'Principle 1: No action taken by LEAs or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

[992] Ibid.
[993] ACPO (Association of Chief Police Officers*), ACPO Good Practice Guide for Digital Evidence*. (2012), available online at: http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

> Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.'[994]

When establishing cyber-specific rules for dealing with digital evidence the *Best Practice Manual for the Forensic Examination of Digital Technology*, issued by the European Network of Forensic Science Institutes (ENFSI) in 2015, can be considered as another helpful document, which particularly aims at providing 'a framework for procedures, quality principles, training processes and approaches to the forensic examination'.[995]

6.4.2.2 Development of cyber-specific investigatory powers

Azerbaijan should next focus on adopting adequate legislative instruments that reflect the specific needs of cybercrime investigation and adjudication to enable LEAs to act more effectively and efficiently, besides ensuring the conformity with the standards of legality. It is also necessary to adopt legislative and other measures as may be imperative for establishing the powers and procedures for specific criminal investigations or proceedings provided for in the Convention on Cybercrime.[996] More precisely, Azerbaijan needs to develop its procedural provisions in a way that enables its competent authorities to order the expedited preservation of computer data, the partial disclosure of preserved computer data, the production of computer data, the lawful collection of traffic data and the lawful interception of content data. Besides, procedural provision should be developed or amended so that it allows effective and efficient utilisation of specific search and seizure instruments related to digital evidence and computer technology.

Based on the analysis of investigatory powers and instruments in Chapter 5, it is suggested that Azerbaijan should consider the following recommendations to develop its procedural law responses to cybercrime:

---

[994] Ibid.
[995] European Network of Forensic Science Institutes (ENFSI), *Best Practice Manual for the Forensic Examination of Digital Technology* (2015) 6.
[996] Article 14, Convention on Cybercrime (2001).

Given that specific definition of data, categories are not provided in national legislation, specifying the definitions of the main concepts, such as 'computer system', 'subscriber information', 'traffic data' and 'content data' in domestic laws would be advisable. These definitions are vital to properly implement procedural powers and provide foreseeability and legal certainty, which would further assist in developing the conditions and safeguards corresponding to those. So, national laws should be amended to include the following definitions:

'computer system' – 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'[997];

'subscriber information' – 'any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;
b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.'[998]

'traffic data' - 'any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service'.[999]

'content data' - the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).[1000]

Expedited preservation of computer data: Introducing specific preservation order provisions would increase the use of less intrusive measures (than the seizure of material objects) by LEAs and trust among stakeholders and thus, foreseeability of law and precision. Alternatively, the combination of general investigative powers

[997] Ibid. Article 1(a).
[998] Ibid. Article 18(3).
[999] Ibid. Article 1(d).
[1000] *Explanatory Report to the Convention on Cybercrime* (2001), para. 209.

with the administrative agreement with service providers, thereby bypassing the necessity of issuing a court order, would enable LEAs to react faster and potentially increase the speed of investigative processes. However, maintaining specific legal provisions would be a better solution also to protect the power from being misused.

It is of particular importance to assess *ex-ante* whether secret interventions might amount to an interference with the right to respect for private life and correspondence as guaranteed by international human rights mechanisms and national laws and whether the exercise of this power is proportional.[1001] An *ex-post* evaluation of proportionality might result in tilting the balance towards allowing the LEAs to resort to more intrusive measures in the face of more grave offences.[1002] Consequently, not only individual rights might be arbitrarily and unlawfully interfered with, but also the evidence collected might become inadmissible at trial, which necessitates a judicial oversight.

Furthermore, given that legal or physical persons cannot be ordered to preserve data expeditiously to enable the competent authorities to seek the disclosure of data,[1003] legislative and other measures should be adopted to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days'.[1004] Therefore, the scope of the Code of Criminal Procedure should be broadened to give effect to Article 16 of the Convention on Cybercrime also about other holders of data (besides ISPs).

Next, as data preservation is primarily a new and innovative power or procedure in national criminal procedure law, Azerbaijan needs to adopt specific legal provisions on the expedited preservation of data to enhance the scope beyond operators and providers, and eliminate legal uncertainty that can lead to breach and misuse of powers by authorities. Articles 16 and 17 of the Convention on Cybercrime should

---

[1001] e.g. Article 8.1, European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Article 17, International Covenant on Civil and Political Rights (ICCPR) UN Doc. A/6316 (1966), Article 32, Constitution of the Republic of Azerbaijan (1995); Article 16, Criminal Procedure Code (2000); see also*, Leander v Sweden,* 9248/81 [1987] 9 EHRR 433.

[1002] Jonida Milaj, 'Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance' (2015) 30 *International Review of Law, Computers & Technology*, 3.

[1003] See Section 5.2., Chapter 5.

[1004] Article 16.2, Council of Europe Convention on Cybercrime (2001) ETS No. 185.

be considered when defining subject matter and the scope of this measure in national legislation.

Production order: It was concluded in Chapter 5 that Azerbaijan has not harmonised its legal provisions regarding cyber-specific production orders with the Convention on Cybercrime. General procedural measures have been implemented to order the submission of the data necessary for investigating cybercrime cases, which has proven to be impractical and onerous.[1005] It is, thus, crucial to develop cyber-specific measures that are effective and efficient in addressing challenges posed by cybercrime before investigations and ensure the foreseeability of law and the legal certainty that can adequately protect against breach and misuse of powers by authorities. In particular, more flexible and quicker responses require specific rules and provisions compelling service providers - without a court decision, but subject to certain legal requirements and limitations - to submit basic 'subscriber information' and contact details, such as the name, IP address, telephone number or e-mail address, or the name of the subscriber associated with the IP address. This can be partly achieved through introducing production order provisions pursuant to Article 18 of the Convention on Cybercrime.

Application of the same fundamental principles for the collection of both digital and non-digital evidence ensures that the LEAs follow the same legal process route and therefore individuals' rights and freedoms are better protected. However, as discussed in Chapter 5,[1006] in practice, the protection of rights and freedoms has not always been a priority in Azerbaijan. Therefore, fair procedural mechanisms, which enable LEAs to investigate cybercrime besides ensuring the protection of the rights successfully, are needed for responding to cybercrime appropriately. So, procedural rules and instruments for collecting digital evidence must be clear and established in a way which 'ensures that cybercrime is not used as a justification to undermine new information security protocols and the right to privacy in

[1005] See Sub-section 5.2. Chapter 5.
[1006] Ibid.

telecommunications'.[1007] So, when establishing national measures for implementing provisions of production orders for computer data or subscriber information, it needs to be ensured that there are 'appropriate safeguards for the fundamental rights of individuals or ...oversight mechanisms to ensure that these powers are not abused' and thus, extensive national surveillance powers are not mandated.[1008]

Search and seizure: Not having specific provisions on search and seizure of stored computer data and extending the legal framework for traditional search and seizure powers to computer data has made the country to face a range of challenges, as discussed in Chapter 5.[1009] It is, therefore, vital to provide explicit provisions with specific powers to search, or access computer systems or data. Procedural legislation should incorporate and clarify specific provisions set out by Article 19 of the Convention on Cybercrime (such as 'search or similarly access a specific computer system'; 'make and retain a copy of those computer data'; 'maintain the integrity of the relevant stored computer data'; and 'to render inaccessible or remove those computer data in the accessed computer'). Besides, criminal justice authorities should be empowered to ensure that they can expeditiously extend the search or similar accessing to linked systems, and order any person who has knowledge and information necessary information to enable the undertaking of the search and seizure measures.[1010]

Furthermore, as discussed in Chapter 2 and Chapter 5, unique technical and organizational challenges raised by cloud computing that render traditional investigative measures and tools widely inapplicable make it difficult to enforce the powers of searches and seizures of digital evidence, and thus, the individuals' right to privacy is put at risk of being invaded. For example, the Convention on Cybercrime provision requires the States parties to enable the authorities to expeditiously extend the search or similar accessing to the other system, if at any

[1007] Ben Hayes et al. (n. 137), 56.
[1008] Ibid. 28.
[1009] See Section 5.2.5. Chapter 5.
[1010] Article 19, Council of Europe Convention on Cybercrime (2001).

time during the investigation they discover that the required evidence is stored in another computer system or network, and such data is lawfully accessible from or available to the initial system.[1011] Meanwhile in the UK, the Criminal Justice and Police Act 2001 grants the LEAs with the right to seize 'both the seizable property and that from which it is not reasonably practicable to separate it', including the material potentially outside the scope of a warrant.[1012] However, implementation of these powers could result in criminal investigations being intrusive and triggering a cause of action on the right to privacy.[1013] Consequently, it is necessary to achieve clarity about the scope of the power, as well as the warrant, with regard to the materials to be searched and seized. For example, in *Weber and Saravia v. Germany,* the Court has developed minimum safeguards that should be set out in statute law to avoid abuses of power. These minimum safeguards include: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[1014]

Next, the Criminal Procedure Code should be amended through adopting clear rules and procedures about the data stored on social and digital media, as well as the preservation of the data seized. Moreover, there should be competent institutions for providing expert assessments of this data.

Interception of computer data: It was stated in Chapter 5 that provisions enabling interception of phone and other communications are applied to authorise interception of traffic and content data in Azerbaijan.[1015] However, neither the traffic

[1011] Ibid. Article 19.2.
[1012] Section 50(2), the Criminal Justice and Police Act 2001, UK.
[1013] See for example, *Antonius Cornelis Van Hulst v. Netherlands*, U.N. Doc. CCPR/C/82/D/903/1999 (2004); see also, *Khan v the United Kingdom,* 35394/97, [2001] 31 EHRR 45; *Malone v the United Kingdom,* 8691/79, [1984] ECHR 10; *Liberty and others v United Kingdom,* 58243/00, [2008] ECHR 568.
[1014] *Weber and Saravia v. Germany,* 54934/00, [2006] ECHR 1173.
[1015] Section 5.2.6. Chapter 5.

data nor the content data is defined under the criminal procedure legislation. It is imperative to state about the exact type(s) of communication or information to be intercepted in the decision authorising the interception. Yet, the lack of these definitions does not exclude any of them from being subjected to the interception. In principle, the text provided by the Code of Criminal Procedure 2000 enables the interception of any information sent by communication media and other technical means, and of any other information. In terms of legal prerequisites needed for authorising an interception measure, it is important to make a distinction between the two. This distinction is necessary to ensure legal certainty, to limit the scope of interception and thus, to avoid the misuse of power by LEAs. Also, the real-time collection of content data should attract the imposition of greater limitations than traffic data, as 'the privacy interests in respect of content data are greater due to the nature of the communication content or message'.[1016]

Consequently, it is crucial to review the Code of Criminal Procedure in the light of Articles 20 and 21 of the Convention on Cybercrime, with the aim of amending provisions of Article 259, and including specific provisions on interception of information sent by communication media and other technical means, and of other information. Development of cyber-specific rules would also ensure a better balance between individual rights and freedoms, and investigative measures, which does not compromise any of them. In addition, reviewing the limitations and safeguards for the implementation of interception provisions pursuant Articles 20 and 21 of the Convention would be advisable.

6.5 Conclusion

This Chapter has provided recommendations to enhance the legal and policy responses of Azerbaijan to cybercrime based on the analysis of laws, policy papers, documents and academic literature on cybercrime control and prevention, as well as interviews conducted with experts in Azerbaijan and lessons drawn from the UK.

[1016] *Explanatory Report to the Convention on Cybercrime* (2001), para. 210.

At the start, specific recommendations were made with special reference to the UK that would help to achieve a better understanding of the nature and scale of threats and vulnerabilities caused by cybercrime to Azerbaijan. The importance of accurate quantification, as well as the mapping and measurement of cybercrimes were emphasised and potential solutions to address those issues were presented.

Based on the UK expertise, the Chapter next tried to propose solutions for the introduction and development of an explicit cybercrime strategy, or specific cybercrime policies to ensure an effective criminal justice response. The central idea was that the combination of relevant strategy, policies, and legislation would ease the cooperation of different actors with overlapping competences, and decrease the time spent for the establishment of legal foundation and increase effectiveness and efficiency of laws.

Having identified the overlapping competences among different stakeholders in the preceding Chapters, this Chapter then proposed specific recommendations to address this problem. These recommendations related to systems and laws. On the systems, the low levels of personnel and organisational cybercrime specialization for the investigation, prosecution and adjudication in Azerbaijan were the subject of explicit solutions. Specific ideas aimed at enhancing the role of the private sector, academia and civil society in controlling and preventing cybercrime were also offered. It was recommended that the holistic approach adopted in the UK, which brings all sectors together and requires a collective effort, would prove effective and efficient in Azerbaijani context.

The state-centric governance approach pursued in Azerbaijan was criticised. Establishment of efficient platforms and arrangements for inter-agency cooperation and operational partnerships with the private sector to share information on threats in cyberspace was regarded as a better tactic for Azerbaijan. Joint industry and government initiatives established in the UK to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on businesses were given as examples. Furthermore, the country needs to be more oriented towards the harmonisation of the relevant laws, and development and implementation of formal

mechanisms in accordance with these laws besides developing informal cooperation mechanisms to foster more effective and efficient international cooperation against cybercrime. Notwithstanding that the legal system of Azerbaijan is based on civil law, the author was able to draw some lessons from the relevant UK laws, as well as from international guidelines, including crucially the Convention on Cybercrime. In general, it was recommended that sanctions imposed for cybercrime offences should be stricter in Azerbaijan, in line with the UK. Moreover, Azerbaijan should introduce cyber-specific provisions to deal with computer-related fraud, identity theft, and cyberstalking. Given that many content-related acts have been criminalised in Azerbaijan, the principle of proportionality in relation to individual rights requires a higher threshold for criminalising offences relating to defamation, obscene material, and insult. Finally, many detailed recommendations for the development of cyber-specific investigatory powers and optimisation of legal frameworks for digital evidence were also devised in the light of lessons drawn from the relevant UK laws and experience and international guides and developments.

In conclusion, given the importance of ICT to the economic and social development of the country, reforms are vital in Azerbaijan, although these reforms could be difficult to realise due to political, social, economic and technical issues. The recommendations and blueprints presented in this Chapter could potentially assist in conducting these reforms with relative ease, cost and speed.

CHAPTER 7: Conclusion

This Chapter offers critical reflection on the thesis, including a summary of the main findings and analysis presented in the preceding chapters as well as limitations in the research. It sets out the main research findings based on the primary research questions of the project.

Despite the scarcity of the national sources and inconsistencies in the approaches to cybercrime in Azerbaijan, the researcher analysed different laws, policy papers, documents and academic literature and conducted interviews with relevant experts in Azerbaijan to explore his arguments and to ensure the completeness of this study, the results of which are outlined in this chapter. Furthermore, possible avenues and recommendations for future research are proposed.

7.1 Primary Research Findings

This thesis has sought to provide an in-depth explanation and analysis of policy and legal responses of Azerbaijan to cybercrime. As part of this project, it offers recommendations to enhance the effectiveness, efficiency and legality of the responses. In addition, it was also an objective to identify selective lessons to be drawn from the UK, which can contribute to developing further Azerbaijan's capacity to prevent and control cybercrime.

To accomplish the abovementioned objectives, this study was designed to answer five principal research questions, as set out in Chapter 1, through considering each of them in a separate chapter.

7.1.1 The reality and perception of cybercrime: how much of a problem is cybercrime in Azerbaijan?

Chapter 2 elaborated what is meant by cybercrime and how cybercrime is experienced and perceived in Azerbaijan. Based on the literature review and the analysis of semi-structured interviews, there is still substantial ambiguity around the term 'cybercrime' and the extent of its harmfulness. The lack of an adequate definition for cybercrime has also produced the significant undercounting of cybercrimes. To address the overlap between the international and national

approaches to defining the term ‘cybercrime’ as well as to establish a basis for consistent analysis throughout the research, a working definition of cybercrime and a speculative set of acts that may be embraced by this term have been explained in Chapter 2.

It was revealed that as the concepts of online risk assessment and risk mitigation have not been given adequately high priority at all levels in Azerbaijan, potential and actual victims of cybercrime, especially non-corporate persons, have not been sufficiently acknowledged, nor have they been adequately informed about how to report cyber incidents. The problem of under-reporting and under-counting of cybercrime have distorted the understanding of the current cyber threat landscape and obscured its full impact on the country. Since businesses and the public have not been sufficiently informed about the existing and potential threats, it is still difficult to measure the true extent and scale of cybercrime in Azerbaijan. Nor are there methodologically sound national surveys to map and measure cybercrimes in the country accurately.[1017]

To illuminate the scale and impact of cybercrime on Azerbaijan, the researcher considered relevant international and security network reports as well as the interviews along with considerably limited and incomplete information provided by the national sources. Both the interviewees and the reports supported the view that cybercrime is a real and growing threat to the country. Interviewees have underlined several factors linked to the increasing impact and scale of online threats and cybercrime in the country. These factors include globalisation, the complex geopolitical position of the country, possible and ongoing conflicts with neighbouring countries, lack of control and monitoring mechanisms covering the information space, increasing dependence on the Internet and digitisation of services, low levels of ICT education and awareness, and changing socio-economic conditions.

Chapter 2 also provided a summary of the main features of the challenges and opportunities in combatting cybercrime to ensure an early understanding of the

[1017] See Section 2.5, Chapter 2 for further discussion.

problem.[1018] Automated digital forensics and traceability of online activities were identified as opportunities for pursuing cyber offenders. However, it was argued that Azerbaijan had not grasped these opportunities successfully, due to the complexity of modern tools and the lack of both specific laws and powers and properly trained personnel with relevant knowledge and expertise. In general, there is an imbalance between the general ICT development and application, which is currently above the global average, and the level of ensuring cybersecurity in Azerbaijan.

In addition to the legal challenges, which were later analysed by chapters 3, 4 and 5 in the light of policy and legal responses to cybercrimes, the country has to face design challenges. It was argued that the number of suitable targets and motivated offenders would increase due to the growing proportion of people connected to the networked environment. More importantly, an increasing number of users and the greater access to, and spread of, the networked environment will enable offenders to easily multiply the scale of offending and consequently, it will become more challenging to combat these acts and automate the investigation processes. The country has also been challenged by the major disjunction between the speed of traditional methods practised by LEAs in responding to cybercrimes, which is far too slow, and the speed of processes in cyberspace. Besides the borderless nature of the Internet, anonymity has been identified as another feature making the precise attribution of harm challenging for Azerbaijani LEAs.

What was also initially revealed in Chapter 2, as later confirmed throughout the analysis in later chapters and during the fieldwork, was that combatting cybercrimes has become onerous due to the absence of control mechanisms.

In summary, it became evident that cybercrime is a real and growing threat to the country, although there is a substantial ambiguity around the term ‘cybercrime’, and the extent of its harmfulness. Neither the state nor the public has fully perceived the risks and threats posed by cybercrime to the country, and it has not been properly measured and mapped.

[1018] See Section 2.3, Chapter 2.

7.1.2 Cybercrime Policies and Strategies: what are the developments in Azerbaijan?

Chapter 3 focused on providing a detailed analysis of official policy responses in the country to cybercrimes. It was highlighted that dedicated cybercrime strategies and policies had not been introduced in Azerbaijan. Given that it is difficult to ascertain and delineate the full scope of a cybercrime strategy and policies, the chapter concentrated on the measures that could be considered as potentially suitable parts of the country's anti-cybercrime policy responses, and its translation into a national strategy.

Initially, the chapter tried to shed light on the national cybersecurity context of the country. It was revealed that Azerbaijan has not maintained a systematic and comprehensive approach in ensuring an adequate level of cybersecurity and thus, has failed to adopt a dedicated cybersecurity strategy and policies. The country has also been lacking the interest and capacity to develop a national cybersecurity strategy and policies. In addition to the shortage of a sufficient level of sectorial capacity, the country has also been missing management at the strategic level. Following the comparative analysis of international studies and measurements focused on Azerbaijan's commitment to cybersecurity, it was concluded that the cybersecurity level in Azerbaijan could not be considered as being fully satisfactory.

Chapter 3 also briefly elaborated the role of the law and legal measures in controlling and preventing cybercrime and tried to identify various components of the legislative elements needed in a comprehensive approach and key areas to be addressed by legislation. It was argued that the dynamics of the law are still slow when compared to the dynamics of cyberspace and criminal conduct in this environment. However, laws have been viewed as having a central role in responding to cybercrime and being required in distinct areas, including criminalisation, jurisdictional coverage, procedural powers, international cooperation, and fixing the responsibility and liability of internet service providers. It was argued that the lack of a dedicated strategy and policies would lead to the

inadequacy of implementation and coordination of legal efforts, which was later revealed to be true following the extensive analysis of legal responses in Chapters 4 and 5.

Chapter 3 also reviewed the overlapping competencies in the roles and responsibilities of authorities in securing the national cyberspace.[1019] Although a state-centric approach has been pursued in protecting citizens from cyber-attacks and cybercrime, there are still difficulties in clarifying the roles and responsibilities, as well as ensuring that government authorities are provided with necessary resources in Azerbaijan.

It was also identified in Chapter 3, as well as during the fieldwork, that there is a lack of qualified specialists and sufficient resources within the government authorities to deal with cybersecurity and cybercrime.[1020] While some levels of organisational and personnel cybercrime specialisation have been ensured for the investigation of cybercrime cases, minimal levels of specialisation for cybercrime have been observed by prosecution and adjudication institutions. It was also argued that it would still be hard for LEAs to carry out successful investigations unless they are provided with the necessary intelligence, and are competent, well organised and fully equipped.

Furthermore, it was determined in Chapter 3 that the role of the businesses, the private sector, academia and civil society in Azerbaijan's cybersecurity alongside with government sector has been undermined due to the state-centric approach adopted in the country. This was also confirmed during the interviews. Following the analysis of the role of each of these sectors, it is contended that the country should recognise the fact that tackling cybercrime and making the Internet less attractive to criminals requires a holistic public-private approach.

Next, Chapter 3 considered the importance of cooperation in controlling and preventing cybercrime and analysed the current situation and developments in Azerbaijan in the light of both intra-state and international cooperation measures

[1019] See Section 3.5, Chapter 3.
[1020] Ibid.

taken.[1021] The core argument was that in Azerbaijan the way of managing risks in cyberspace does not match the complex and dynamic environment of the country's information space, albeit that measures have been taken at both internal inter-agency and external international levels to foster cooperation against cybercrimes. First, the country has not treated the threat posed by cybercrime as a strategic priority and thus, has not established a strong public-private partnership for mitigating threats and identifying and disrupting criminals more appropriately. Little has been done by the government to improve the situation or to avoid exercising a single-industry agency jurisdiction. Second, Azerbaijan is still in the early phases of the development of multilateral and mutually productive working relationships with other countries, and thus, has not developed a sufficient number of operational channels for both formal and informal cross-border cooperation.

In the last section of Chapter 3, it was provided that Azerbaijan does not have a cybercrime prevention plan with clear priorities and objectives, nor is there a general crime prevention plan encompassing such priorities and objectives in a clear way, even though it should be an integral part of the organisational aspect of crime prevention.[1022] Although not specifically and directly pertaining to cybercrime prevention, LEAs and other governmental institutions, academia and private sector entities have taken prevention and awareness-raising initiatives to foster better protection against cyber-attacks. However, it can be argued that the country can not be regarded as being successful in preventing cybercrime, a view also supported by interviewees during the fieldwork.

In summary, because of the lack of a dedicated strategy and policies there persists the inadequacy of implementation and coordination of legal efforts. More precisely, the country has broadly relied on multiple documents and uncoordinated measures, which have led to a potential gap of compatibility and inconsistency within these measures and resulted in significant reduction of legality, effectiveness and efficiency of responses to cybercrime.

[1021] See Section 3.5, Chapter 3.
[1022] See Section 3.6, Chapter 3.

7.1.3 To what extent are regulatory and substantive criminal laws equipped to handle cybercrimes?

Chapter 4 provided a detailed study of relevant constitutional rights, liberties and laws, and the criminalisation approach from the theoretical/doctrinal and critical perspectives. It started the discussion through reflecting upon the role of the law, in particular, the criminal law, in controlling and preventing cybercrime.[1023] Laws were regarded as being one of the main instruments used for regulatory purposes and thus play a major role in combatting cybercrimes. At the same time, inconsistencies between laws and requirements, which ought to be satisfied to address the specific challenges of cyberspace properly, were also noted.

Before embarking upon the analysis of substantive criminal laws, constitutional provisions were analysed to ensure the coherence of the critical elements of this study.[1024] It was also acknowledged that constitutional provisions are not specific enough to serve as concrete legal orders and do not provide the clarity required for criminal norms. Rather, lower tier regulatory laws, which could provide the clarity in understanding the underlying standards and values, were also considered in the light of relevant constitutional provisions, conditions and safeguards. To assist in further understanding of the core values to be protected in the fight against cybercrimes, fundamental rights and liberties specified by the Constitution. It was also highlighted that when examining the legality of responses to cybercrimes, it is necessary to scrutinise the compatibility of national laws and standards with provisions determined by principles and norms of international law, as the international treaties to which Azerbaijan is a party are an integral part of the legislative system.

Chapter 4 continued the discussion by reflecting on the criminalisation of specific offences, as well as general provisions and principles of the criminal statute, which shape the criminalisation approach.[1025] It was argued that viewing cybercrime offences among ‘crimes not representing great social danger’ or ‘minor crimes’ may

[1023] See Section 4.1, Chapter 4.
[1024] See Section 4.2, Chapter 4.
[1025] See Section 5.3, Chapter 5.

result in the full array of responses of the country to cybercrime being rendered inadequate.

It was also argued in Chapter 4 that Azerbaijan has fixed the minimum age of criminal responsibility (MACR) at a relatively high age level, which might become problematic when dealing with cybercrime.[1026] Furthermore, it was determined that the Criminal Code had not attached criminal liability against legal entities for the commission of offences related to infringements of copyright and related rights. It was also revealed that sanctions determined by the Criminal Code to be imposed on the acts studied are also inconsistent and relatively lenient.

Analysis of specific cybercrime offences in Chapter 4 with special reference to the Convention on Cybercrime and comparatively with the pre-harmonised version of the current Criminal Code revealed few gaps and inconsistencies.

In summary, having a physical component as the primary focus, ignoring the societal structure of cyberspace, reflecting the slow dynamics of development and enforcement, and thus, becoming easily outdated are among the features which compromise the role of criminal law in virtual worlds. Notwithstanding these limitations, the national criminal law is effective to some extent, both symbolically and practically. In addition, sufficient degree of conditions and safeguards are provided for under domestic laws, the full implementation of which would ensure the adequate protection of human rights and liberties. There are, however, several criminalization gaps and inconsistencies resulting in the potential to affect both Azerbaijan and cooperation with other countries.

7.1.4 Which procedural instruments and powers are in place in Azerbaijan to investigate and adjudicate cybercrime? Do they provide an effective and efficient response?

Chapter 5 critically analysed domestic procedural instruments and powers applied in responding to cybercrime with reference to the procedural aspects of the Convention on Cybercrime. Besides, the chapter focused on scrutinizing national

[1026] See Section 4.3, Chapter 4.

laws and practices adopted in Azerbaijan regarding jurisdictional issues and international cooperation provisions, as well as the provisions on the collection and admissibility of digital evidence.

The chapter started the discussion by examining the legal status of digital evidence.[1027] It became obvious that specific legal provisions regulating digital/electronic evidence were missing, albeit the possibility to use digital or electronic information as evidence before a court in criminal proceedings has been provided by general legal powers and procedures. As also identified during the fieldwork, digital evidence has been neither widely scrutinised and analysed nor thoroughly understood in the country since it has been relatively alien to the national legal system. It was also revealed that lawmakers had not shown a willingness to effectively address the admissibility of digital evidence or clearly distinguish between digital and physical evidence. Comprehensive national guidance available to be followed when dealing with digital evidence has also been missing. It was, thus, suggested that clear and transparent legislation should be introduced for the purposes of reducing the scope of technical objections to the admissibility of digital evidence.

Chapter 5 also focused on conditions and safeguards to be ensured during the establishment, implementation and application of the powers and procedures when dealing with cybercrime cases to guarantee the adequate protection of human rights and liberties, including international law human rights.[1028] In theory, the protection of human rights and liberties has been given a priority when balanced against the requirements of law enforcement. In addition, it was also revealed that the principle of proportionality has not been directly incorporated into national powers and procedures. However, explicit provisions ensuring that relevant powers or procedures are not excessive compared to the nature and circumstances of the offence have been consolidated within the legislation on criminal procedure.

[1027] See Section 5.2., Chapter 5.
[1028] See Section 6.2.2., Chapter 6.

The key concern of the chapter was the analysis of procedural rules implemented during the investigation, prosecution and adjudication of cybercrime. The analysis of these powers and laws, as well as interviews with experts, made it evident that the procedures are insufficient in dealing with the increasing number of cybercrime cases. The country has not developed specific procedural rules to respond to cybercrime and heavily relies on extending its general procedural powers to the prosecution and adjudication of cybercrime cases. Although relevant to some extent, these 'offline' procedural powers have not been appropriate for the virtual environment and therefore, posed significant problems for enforcement. Moreover, the Convention provisions on evidence and procedures have not been implemented. It was argued that even though the Convention itself does not seem to be sufficient in dealing with cybercrime, it provides minimum settings necessary for the investigation and prosecution of criminal offences committed via computer systems. So, Azerbaijan should bring its criminal procedure laws in line with the Convention to ensure the consistency of its responses to cybercrime and enable the LEAs to carry out effective and efficient investigations.

Since cybercrime has given rise to complex jurisdictional issues and caused an increase in concurring or competing jurisdiction claims, Chapter 5 also elaborated on what is the established jurisdiction over the cybercrimes.[1029] Similar to the Convention's jurisdictional clauses, the principle of territoriality and the principle of nationality have been contained by the national laws. However, it was identified that both the national laws and the Convention have largely neglected the issue of jurisdictional concurrency. It was argued that in the realm of cybercrime, jurisdictional disputes would arise at a faster pace in the near future, as cyberspace and the internet architecture have provided countries with the ability to conduct investigation extraterritorially and thus, claim jurisdiction over a wide range of offences. Even if a full legal harmonisation of national laws with the Convention were achieved, concurrent jurisdiction in the context of cybercrime would still be challenging and problematic.

[1029] See Section 6.3., Chapter 6.

The last section of Chapter 5 was devoted to the analysis of provisions and mechanisms regarding international cooperation.[1030] It became evident that the country still primarily relies on applying general investigative and cooperation related powers in the fight against cybercrime. This situation does not mean that general MLA and extradition related national legal instruments have been completely irrelevant for cybercrime cases. A 24/7 point of contact has been created to provide specialised assistance, to order the expeditious preservation of computer data or traffic data, after getting a court decision to seize objects containing data, and to perform or facilitate the execution of procedural documents. However, this study also revealed that these mechanisms have been underutilised, notwithstanding the LEAs have been enabled to receive and execute requests both from legal and technical perspectives.

Next, it became apparent that Azerbaijan has been encountering problems arising from discrepancies between the underlying nature of different legal systems and time delays (because of multi-layered steps and duration of the procedures), which make it difficult to deliver extensive co-operation and to achieve smooth and rapid flow of information and evidence internationally.[1031] This problem was also confirmed during the interviews.

In summary, Azerbaijan has not adopted adequate legislative instruments reflecting the specific needs of cybercrime investigation and adjudication. In addition, specific international cooperation instruments or partnerships designed to address cybercrime related issues are also missing. The lack of cyber-specific provisions and adequate legal instruments enabling competent authorities to carry out effective and efficient investigation and adjudication of, and cooperation against, cybercrime have also left human rights at risk. Therefore, it is also necessary to ensure that procedural powers and instruments do not interfere with the internationally as well as regionally recognised fundamental rights and freedoms of the suspect, nor those in the national constitution.

[1030] See Section 6.3., Chapter 6.
[1031] See Section 6.3., Chapter 6.

7.1.5 What can be done to augment the strength of Azerbaijan in preventing and controlling cybercrime? What lessons can be drawn from the UK?

Based on the analysis of policy and legal responses provided by the preceding chapters, Chapter 6 concentrated on devising recommendations to ensure that the responses given are more effective and efficient and are based on fair laws and procedures. The Chapter also drew lessons from relevant UK legislation and practice to make further recommendations for enhancing the responses of the country to cybercrime.

The chapter initially elaborated the importance of achieving a better understanding of the nature and scale of threats and vulnerabilities caused by cybercrime in Azerbaijan.[1032] In consideration of the UK Cyber Security Strategy (2011) and the UK National Cyber Security Strategy 2016-2021, it was recommended that Azerbaijan should also treat achievement of a clear and shared understanding of the scale of the threat as an indicative success measure of the country's capability to control and prevent cybercrime. The cybercrime response should, therefore, ensure that a higher proportion of incidents reported to the authorities through specifying more transparent processes for reporting cyber incidents and via increasing awareness about the existence of such a mechanism among businesses and public.

Next, acknowledging the fact that Azerbaijan has not developed methodologically sound national surveys measuring cybercrime, the adoption of the methodology applied by the Crime Survey for England and Wales (CSEW) was offered as a potential solution to overcome the limitations of police recorded crime.[1033] It covers a broad range of victim-based crimes, not just those that have been reported to, and recorded by, the police. In addition, a higher level of objectivity can be achieved if the survey is conducted by an independent (from the government or the police) survey research organisation using trained interviewers who have no vested interest in the results of the survey.

[1032] See Section 6.2. Chapter 6.
[1033] See Section 6.2. Chapter 6.

The chapter also demonstrated again the need for cybercrime strategy and policies.[1034] It was argued that the country should place greater value and effort in enhancing security, resilience, reliability and trust in ICT by pursuing comprehensive strategies and thoroughly coordinated policies. Introduction of a dedicated strategy would enhance cybersecurity and the anti-cybercrime capacity of the country. This would assist the country to initiate a systematic national programme to secure cyberspace, and prioritise threats and risks, allocate roles and responsibilities more efficiently, as well as help mobilise technical assistance for capacity building. Developing an anti-cybercrime strategy would help to ensure that legal and criminal justice responses mirror the special challenges of cybercrime and assist in determining operational and strategic priorities prior to shaping legislative reform processes. The advantages of having stated policies were identified as enabling the government to comprehensively define its response to a specified problem, and to incorporate a wide range of responses to achieve specific goals, and at the same time, can ensure that legal and strategy objectives do not cause conflicts. In addition, the establishment of dedicated policies can also be utilised to identify the areas where legal development and harmonisation needs to take place as well as to determine the regional/international standards that should be enforced in the particular national circumstances of Azerbaijan. It was concluded that failure to devise a comprehensive strategy and policies could cause the legislation to be fragmented, partial and ill-directed, as had also became apparent from the analysis of legal responses to cybercrime in Chapters 4 and 5.

It was recommended in Chapter 6 that the country should adopt a comprehensive approach in responding to cybercrime, more precisely, by means of combining relevant policies, strategy and legislation.[1035] This combination could also ease the collaboration of different government authorities with overlapping competences in the same field, and increase the efficiency in establishing a legal basis, which is crucial for the Azerbaijani context.

[1034] See Section 4.2, Chapter 4.
[1035] See Section 6.3, Chapter 6.

Based on the UK expertise, the Chapter also proposed solutions for the allocation of roles and responsibilities between different stakeholders in controlling and preventing cybercrime in Azerbaijan.[1036] However, the government has not adequately clarified the roles and responsibilities in the fight against cybercrime, as well as failed to ensure that government authorities are provided with necessary resources. Shortcomings and gaps are present at both prevention and the detection, investigation, prosecution and adjudication levels. Thus, the lessons drawn from the UK helped with each of these levels.

As Azerbaijan has established neither a specific cybercrime prevention plan, nor a general crime prevention plan encompassing priorities and objectives in a clear way, the importance of prevention was also raised in the light of the UK Cybersecurity Strategy (2011), and the UK National Cyber Security Strategy 2016-2021.[1037] Furthermore, besides personnel specialisation, sufficient degree of organisational cybercrime specialisation for the prosecution and adjudication should also be ensured. As a model for making further improvements in prosecution, the UK Crown Prosecution Service Cybercrime Strategy (2016) was considered. Furthermore, reflecting the growing cyber threat and minimal levels of specialisation for cybercrime shown by courts in Azerbaijan, two types of solutions were proposed based on the UK experience. Either judges, as well as prosecutors, should be equipped with necessary knowledge and capabilities to handle cybercrime cases and digital evidence, and courtrooms should be fitted with the modern multimedia technology necessary to effectively present digital evidence during proceedings. Alternatively, if a surge in cybercrime case load is experienced in the future, designation of a new centralised court complex with a focus on cybercrime, such as the one to be opened in the City of London,[1038] can help to fast-track process of delivering justice.

Furthermore, since the role of businesses, the private sector, academia and civil society in preventing and controlling cybercrime have been undermined by

[1036] See Section 6.3, Chapter 6.
[1037] See Section 6.3, Chapter 6.
[1038] The UK government, for example, has announced in July 2018 that a £170m flagship court to deal with cybercrime is to be set up in the City of London. See Section 6.3. Chapter 6.

excessive centralisation in Azerbaijan, it was recommended that the more holistic approach adopted in the UK, which brings all segments together and requires a collective effort, would prove more effective and efficient in Azerbaijani context. Each sector's potential role, as well as the cooperation between those sectors, have been discussed with reference to the UK experience and relevant solutions. Collaborative arrangements, partnerships and initiatives existing in the UK between the government, industry and academia have been given emphasis and offer blueprints to enhance intrastate cooperation in Azerbaijan.

Next, notwithstanding that the legal system of Azerbaijan is based on civil law, the author drew some lessons from the relevant UK laws. As regards substantive criminal laws, it was recommended that sanctions imposed for cybercrime offences should be stricter in Azerbaijan as in the UK. Moreover, by referring to UK laws, Azerbaijan should, in turn, introduce cyber-specific provisions to deal with computer-related fraud, identity theft, and cyberstalking. Also, it was recommended that 'procuring child pornography through a computer system for oneself'[1039] and 'possessing child pornography in a computer system or on a computer-data storage medium'[1040] should also be criminalised, and the criminalisation of illegal interception should be expanded to cover the 'confidentiality of private communications' as well.

As regards procedural powers and instruments, it was recommended that the country should develop its procedural provisions in a way that will enable its competent authorities to order the expedited preservation of computer data; the partial disclosure of preserved computer data; the production of computer data; the lawful collection of traffic data and the lawful interception of content data; as well as to effectively and efficiently use specific search and seizure instruments related to digital evidence and computer technology. Recommendations for the development of cyber-specific investigatory powers has also incorporated some lessons drawn from the relevant UK laws and experience.

[1039] Article 9.1 (d), Convention on Cybercrime, ETS 185
[1040] Ibid. Article 9.1 (e).

7.2 Central thesis

The thesis for this study is that the Republic of Azerbaijan has not responded appropriately to cybercrimes. It was contended that although the application of ICTs had been significantly encouraged by the State of Azerbaijan effective and efficient control and prevention of cybercriminal activities had not been adequately assured. This thesis has, therefore, focused on finding out whether necessary institutions are in place, and whether national policies and laws are sufficient to address the challenges of cybercrimes and are being implemented in accordance with constitutional or international law, standards and principles.

As one of the countries having encountered an increasing impact of threats from cybercrimes, Azerbaijan needs to enhance its capacity to control and prevent these threats more effectively and efficiently. Notwithstanding the country has taken multiple measures to address the problem of cybercrime, these measures are not effectively coordinated and remain fragmented and incomplete.

In summary, having considered all the research findings it can now be asserted that Azerbaijan has failed to respond appropriately to cybercrime due to the lack of both policy and legal frameworks as well as insufficient human, institutional and technological capacity and resources, and low levels of cooperation at the national and international levels. However, it has also become apparent that there is not a single solution to the problems posed by cybercrime, which Azerbaijan has failed to adopt. Cybercrime requires a holistic response: a combination of a strategy, policies and laws, extra-legal measures, sufficient human, institutional and technological capacity and resources, as well as effective and efficient cooperation at the national and international levels. Specific recommendations and solutions proposed by this study would significantly enhance the capacity of the country against cybercrime if fully applied in Azerbaijan.

7.3 Limitations and Future Research Directions

This study has presented a critical review of the policy and legal responses of Azerbaijan to cybercrime within the limits of time and resources associated with this research. To date, there has been little attention to the problem and minimal in-

depth research on the topic of cybercrime in Azerbaijan. Although Azerbaijani authorities recognise the necessity to deepen and broaden the research into the issue of cybercrime, insufficient research has been conducted to address the cybercrime problem. This thesis can also serve as a basis for structuring cybercrime measures since no other systematic and comprehensive project has been previously undertaken to investigate cybercrime problems.

Evidently, cybercrime studies in Azerbaijan are still in their infancy with the consequence that there have been very limited discussions, academic literature and secondary sources to be reviewed for the purposes of this study. The researcher has, therefore, primarily concentrated on the theoretical and doctrinal analysis of primary sources of Azerbaijan, plus with reference to the Western literature. So, the research was also bound to draw on debates and theoretical perspectives that were primarily introduced based on the political, social and cultural domains of the European countries, in particular, the UK perspectives. In these ways, this study has contributed to the expansion of very limited academic knowledge in the country. Besides, it has produced a substantial amount of analysis and revealed gaps and shortcomings in the responses of the country to cybercrime that can be further considered for improvements. The research has also paved the way for more detailed exploration on each of the findings and can be used for comparative studies in the future.

As mentioned, due to the presence of limited resources in Azerbaijan the study has also involved an empirical component. It was predicted that access and collection of the statistical data, which is crucial for a quantitative approach, would be highly challenging and problematic. Insufficiency of the relevant statistics supplied by the official government data sources limited any quantitative approach. Therefore, preference was given to qualitative interviews to gain an insight into socio-legal issues influencing the capacity of the country through understanding the views and the experience of people who have relevant information, who directly or indirectly participate in the country`s information security life. However, the fieldwork component involved a small number of participants. Although limited than planned, fieldwork in Azerbaijan has further revealed the lack of expertise and interest on

the topic, and the prevalence of the state security mentality and culture, which implies that officials are not open to discussions and would not actively engage with non-state stakeholders on cybersecurity and cybercrime-related topics.

Whilst the fieldwork was highly original and illuminating, it would be beneficial to engage with more participants in terms of the investigation and adjudication of cybercrime offences. Moreover, engaging with the public through surveys and questionnaires might help to analyse the perception and attitudes of publicity on preventing and controlling cybercrime. This would also help to determine the responsiveness of the government to societal needs and concerns regarding cybersecurity and their expectations from the government on controlling and preventing cybercrime.

In general, drawing lessons from the UK allowed the considerable benefit to be drawn from existing experience and insights in a more developed and transparent jurisdiction. Nevertheless, it is challenging to predict the success of future implementation of the optimal solutions that might be adopted based on policy transfer, as there are significant differences regarding resources and capabilities, as well as the political environment and legal contexts, between the two countries. Moreover, Azerbaijan cannot be considered as capable as the UK in mobilising international cooperation. Thus, differences between countries in the political, social and cultural domains have been considered to the widest extent possible to ensure the applicability of UK developed crime control perspectives in Azerbaijani context.

As well as drawing on debates and theoretical perspectives of the Western societies, in particular, the UK context, it would also be interesting to comparatively study other states' legal and policy responses, especially, the Commonwealth of Independent States (CIS), with which Azerbaijan shares similar legal systems and comparable socio-demographic and economic factors. Investigating more deeply the roles of business, the private sector, academia and civil society in these countries and transferring the most relevant and innovative cooperation tactics between the public and private sector would also be beneficial. Furthermore, a

comparative study of criminalization approaches to cybercrime can be suggested as another promising area. Analysis of underlying social, economic and criminological factors of cybercrimes in Azerbaijan, as well as the criminological aspects of the cyber-deviant behaviour the ‘normalised’ behaviour in cyberspace among the people in Azerbaijani context would help to establish more specific and relevant cybercrime control and prevention plan.

BIBLIOGRAPHY

Table of Legislation

Azerbaijan Legislation

Constitution of the Republic of Azerbaijan (1995)

Constitutional Law on the Regulation of the Realization of Human Rights and Freedoms in the Republic of Azerbaijan (2002), № 404-IIKQ

Civil Code (1999)

Criminal Code (1999)

Criminal Code of the Republic of Azerbaijan SSR (1960)

Criminal Procedure Code (2000)

Decree of the President on 'Measures in the field of improvement of the activities of the information security' (2012) № 708

Law on Copyright and Related Rights (1996) № 115-IQ

Law on Electronic Signature and Electronic Document (2004) № 602-IIQ

Law on Enforcement of the Intellectual Property Rights and Fight against Piracy (2012), № 365-IVQ

Law on Extradition (2001) № 132-IIQ

Law on Freedom of Information (1998) № 505-IQ

Law on Information, Informatisation and Protection of Information, (1998) №460-IQ

Law on Intelligence and Counter-Intelligence Activities (2004) № 711-IIQ

Law on Legal Assistance in Criminal Matters (2001) № 163-IIQ

Law on Legal Protection of Azerbaijani Folklore Expressions (2003) No. 460-IIQ

Law on Legal Protection of Compilations of Data (2004) № 755-IIQ

Law on Legal Protection of Topographies of Integrated Circuits (2002)

Law on Mass Media (1999) №769-IQ

Law on Mutual Legal Assistance on Criminal Matters (2001), № 163-IIQ

Law on National Security (2004) № 712-IIQ

Law on Operative-Investigative Activity (1999) № 728-IQ

Law on Patents (2009) № 312-IQ

Law on Personal Data (2010) № 998-IIIQ

Law on Telecommunication (2005) № 927-IIQ

Law on the Right to Access to Information, (2005) No 1024-IIQ

Law on Trademarks and Geographical Indications (2010) № 504-IQ

Law on Amendments to the Criminal Code of the Republic of Azerbaijan (2012) № 408-IVQD

Law on Amendments to the Criminal Code of the Republic of Azerbaijan (2012) № 314-IVQD

Law on Amendments to the Criminal Code of the Republic of Azerbaijan (2013) № 650-IVQD

Law on Approval, Entry into force of the Criminal Code and the Legal Regulation Issues Connected With it (1999), № 787-IQ

UK Legislation

Communications Act 2003

Computer Misuse Act 1990

Copyright Designs and Patent Act 1988

Criminal Justice Act 2003

Criminal Justice and Police Act 2001

Data Retention and Investigatory Powers Act 2014

Forgery and Counterfeiting Act 1981

Fraud Act 2006

Investigatory Powers Act 2016

Malicious Communications Act 1988

Protection from Harassment Act 1997

Regulation of Investigatory Powers Act 2000

Trade Marks Act 1994

Table of Cases

Antonius Cornelis Van Hulst v Netherlands, U.N. Doc. CCPR/C/82/D/903/1999 (2004)

British Telecommunications Plc and Others v One in a Million, [1999] 1 WLR 903

Chambers v DPP, [2012] EWHC 2157

Coleman v Australia, U.N. Doc. CCPR/C/87/D/1157/2003

Dudgeon v UK, 7525/76, [1981] 4 EHRR 149

Evans v UK, 6339/05, [2007] ECHR 264

Fatullayev v Azerbaijan, 40984/07, [2010] ECHR 623

Guerra v Italy, 14967/89, [1998] ECHR 7

Handyside v United Kingdom, 5493/72, [1976] ECHR 5

K.U. v Finland, 2872/02, [2008] ECHR

Khan v the United Kingdom, 35394/97, [2001] 31 EHRR 45

Leander v Sweden, 9248/81, [1987] 9 EHRR 433

Liberty and others v United Kingdom, 58243/00, [2008] ECHR 568

Mahmudov and Agazade v Azerbaijan, 35877/04, 18 December 2008

Malone v the United Kingdom, 8691/79, [1984] ECHR 10

Marques v Angola, U.N. Doc. CCPR/C/83/D/1128/2002

Otto Preminger Institut v Austria, 13470/87 [1994] 19 EHRR 34

Schalk & Kopf v Austria, 30141/04 [2011] 2 FCR650

SS Lotus (France v Turkey) [1927] PCIL Reports, Series A No. 10 [55]

Társaság a Szabadságjogokért (TASZ) v. Hungary, 37374/05 [2009] ECHR 618

Twentieth Century Fox Film Corp v Newzbin Ltd [2010] EWHC 608 (Ch)

Weber and Saravia v. Germany, 54934/00, [2006] ECHR 1173

Secondary sources

Abbasova F, *Criminal Process: The General Part (Cinayət Prosesi: Ümumi Hissə)* (Baku, Zardabi, 2015)

Ablon L and Libicki M, 'Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data' (2015) 82 *Defense Counsel Journal*

ACPO (Association of Chief Police Officers*), ACPO Good Practice Guide for Digital Evidence* (2012) http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf

Adam N J, 'An Integrated Approach to Policy Transfer and Diffusion.' (2002) 19 Review of Policy Research

Aghayev I, *Corpus delicti: its concepts, elements, significance* (Moscow, 2008)

Aghayev I, *Criminal Law: The Special Part (Cinayət hüququ: xüsusi hissə)* (Baku: Nurlar, 2018)

Aghayev I, *Criminal Law: The General Part* (Leipziger Universitätsverlag, 2015)

Akdeniz Y, *Internet child pornography and the law: national and international responses* (Routledge, 2016)

Akdeniz Y, Walker C and Wall D S, *The Internet, Law and Society* (Longman 2000)

Alguliyev RM, İmamverdiyev YN and Mahmudov RS. 'Multidisciplinary scientific and theoretical problems of information security' (2017) 2 *Journal of Problems of Information Society*

Alkaabi A, Mohay G, McCullagh A and Chantler N, 'Dealing with the Problem of Cybercrime', in Baggili I (eds) Digital Forensics and Cyber Crime. ICDF2C 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 53. (Springer, Berlin, Heidelberg)

Allan G, 'Responding to cybercrime: A delicate blend of the orthodox and the alternative' (2005) 2 New Zealand Law Review

Amnesty International, *Amnesty International Report 2015/16: The State of The World's Human Rights (*2016)

Arden L J, 'Proportionality: the way ahead?' (2013) Public Law 498

Arnell P, 'The Case for Nationality Based Jurisdiction' (2001) 50 International & Comparative Law Quarterly

Auger C P, *Information Sources in Grey Literature* (Bowker-Saur, 4th edn, 1998)

Ayres I, Braithwaite J*, Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, Oxford, 1992)

Balajanov E, 'Setting the Minimum Age of Criminal Responsibility for Cybercrime' (2017) 32 *International Review of Law, Computers & Technology*

Baller S, Dutta S and Lanvin B, *The Global Information Technology Report 2016* (World Economic Forum 2016)

Banakar R and Travers, M. *Theory and Method in Socio-Legal Research* (Hart Pub 2005)

Barak A, *Proportionality – Constitutional Rights and their Limitations* (Cambridge: Cambridge University Press 2012)

Basu S, 'Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis' (2012) 3 *European Journal for Law and Technology*

''Bockel B, *The Ne Bis In Idem Principle in EU Law* (Austin: Wolters Kluwer Law & Business, 1st edn, 2010)

Boister N and Currie R J, *Routledge Handbook of Transnational Criminal Law* (Routledge, Taylor & Francis Group 2014)

Boister N, 'Transnational Criminal Law?' (2003), 14 *European Journal of International Law*

Brenner S W and Koops B J, 'Approaches to Cybercrime Jurisdiction' (2004) 4 *Journal of High Technology Law*

Brenner S W, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' (2001), 8 *E-Law: Murdoch University Electronic Journal of Law* https://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html

Brenner S W, 'Cybercrime jurisdiction' (2006) 46 *Crime, Law and Social Change*

Brenner S W, ‘Cybercrime: rethinking crime control strategies’ in Jewkes Y (Eds) *Crime online* (Cullompton, Devon: Willan, 2007)

Brenner S W, *Cybercrime and the Law* (Boston: Northeastern University Press 2012)

Brenner S W, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, Calif.: Praeger 2010)

Brenner S W, *Cyberthreats and the Decline of the Nation-State* (Routledge, Taylor & Francis Group 2014)

Bridy A, ‘Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement (2010) 89 *Oregon Law Review*

Brown C, ‘Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice’ (2015) 9 *International Journal of Cyber Criminology*

Brown I, Edwards L and Marsden C T, ‘Information Security and Cybercrime’ in Edwards L, Waelde C (Edn) *Law and the Internet*, (Oxford: Hart, 3rd Ed 2009)

Brownlie I, *Principles of Public International Law* (Oxford: Oxford University Press, 6th edition, 2003)

Bryman A, *Social Research Methods* (Oxford University Press 2008)

Buchan R and Tsagourias N, ‘Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence’, (2016) 21 *Journal of Conflict and Security Law*

Business Software Alliance, BSA Position on Appropriate Measures to Deter Online Piracy of Content (2010)

Cabinet Office, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world (London 2011)

Cabinet Office, The UK National Cyber Security Strategy 2016 to 2021 (London 2016)

Cargan L, *Doing Social Research* (Rowman & Littlefield Publishers 2007)

Casey E, *Digital Evidence and Computer Crime* (Academic Press, 3rd edn, 2011)

Casey E, *Handbook of Digital Forensics and Investigation (*Academic Press 2009)

Chehtman A, *The Philosophical Foundations of Extraterritorial Punishment*, (Oxford: Oxford University Press, 1st edition, 2010)

Chiesa R, Ducci S and Ciappi S, *Profiling Hackers* (Boca Raton: Auerbach Publications, 2009)

Clough J, *Principles of Cybercrime* (Cambridge University Press 2010)

Cohen L E and Felson M, ‘Social Change and Crime Rate Trends: A Routine Activity Approach’ (1979) 44 *American Sociological Review*

Coleman C, Moynihan J, *Understanding Crime Data* (Buckingham: Open University Press, 1996)

Constitutional Court of Azerbaijan, the Decision of the Plenum of the Constitutional Court of the Republic of Azerbaijan) on Interpretation of Article 177.2.3-1 of the Criminal Code of the Republic of Azerbaijan (22 June 2015)

EU Council Framework Decision 2005/222/JHA on attacks against information systems (24 February 2005)

Council of Europe Convention on Cybercrime (2001) ETS No. 185

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) CETS No.201

Council of Europe Parliamentary Assembly, *Towards decriminalisation of defamation*, Resolution 1577 (2007)

Council of Europe, *Action Plan for Azerbaijan 2014-2016* (ODGProg/Inf (2014) 2revE)

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 (2003) ETS No.189,

Council of Europe*,* Additional Protocol to the Convention on Cybercrime (2003) ETS - No. 189

Council of Europe, Additional Protocol to the European Convention on Extradition (1975) ETS 086

Council of Europe, *Article 15 - Conditions and Safeguards under the Budapest Convention on Cybercrime* (CyberCrime@IPA 2012)

Council of Europe, *Capacity building on cybercrime – discussion paper* (Global Project on Cybercrime 2013)

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) ETS No.108

Council of Europe, *Cybercrime and cybersecurity strategies in the Eastern Partnership region* (Cybercrime@EAP 2014)

Council of Europe, Cybercrime Convention Committee (T-CY), *Assessment Report. Implementation of the preservation provisions of the Budapest Convention on Cybercrime*. *Follow up given by Parties* (2015)

Council of Europe, Cybercrime Convention Committee (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime* (2014)

Council of Europe, Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #2 Provisions of the Budapest Convention covering botnets* (Adopted by the 9th Plenary of the T-CY (June 2013))

Council of Europe, Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #4 Identity theft and phishing in relation to fraud* (Adopted by the 9th Plenary of the T-CY (June 2013))

Council of Europe, Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #5 DDOS attacks (Adopted by the 9th Plenary of the T-CY* (June 2013))

Council of Europe, Cybercrime Programme Office, *Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play* (2017)

Council of Europe, *Cybercrime training for judges and prosecutors: a concept* (Strasbourg, France 2009)

Council of Europe, *Declaration on Strategic Priorities for Cooperation against Cybercrime in the Eastern Partnership Region* (CyberCrime@EAP project, 2013)

Council of Europe, European Convention on Extradition (1957) ETS No.024

Council of Europe, European Convention on Mutual Assistance in Criminal Matters (1959) CETS No.030

Council of Europe*, Explanatory Report to the Additional Protocol to the Convention on Cybercrime* (2003) ETS - No. 189

Council of Europe*, Explanatory Report to the Convention on Cybercrime* (2001) ETS No. 185

Council of Europe, *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime* (2008)

Council of Europe, *Progress Report* (*covering the period of 1 June 2011 – 31 March 2012)* (Data Protection and Cybercrime Division, Directorate General of Human Rights and Rule of Law, 2012)

Council of Europe, *Revised Assessment Report (2018) on International cooperation on cybercrime in the Eastern Partnership region* (Cybercrime Programme Office, Cybercrime@EAP 2018 Project, 2018)

Council of Europe, *Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region,* (CyberCrime@EAP project, 2013)

Council of Europe, *Suggestions for draft amendments to procedural legislation of Azerbaijan and other recommendations concerning cybercrime and electronic evidence* (Cybercrime@EAP III Project 2017)

Council of Europe, 'Workshop on reform of legislation to ensure compliance with Articles 16 and 17 of the Budapest Convention on Cybercrime' (CyberCrime@EAP II, Baku, Azerbaijan, 13 – 15 February 2017) https://www.coe.int/en/web/cybercrime/-/eap-ii-workshop-on-reform-of-legislation-to-ensure-compliance-with-articles-16-and-17-of-the-budapest-convention-on-cybercrime

CPS Cybercrime Strategy (2016), http://www.cps.gov.uk/publications/docs/cps_cybercrime_strategy_2016.pdf

Cross M and Shinder D L, *Scene of the Cybercrime* (Burlington, MA: Syngress Pub, 2008)

Crow I and Semmens N, *Researching Criminology* (Open University Press, Maidenhead 2006)

Dantzker M and Hunter R, *Research Methods for Criminology and Criminal Justice,* (Jones&Bartlett Learning, 3rd edn 2012)

Davis L S and Sener M F, 'Intellectual Property Rights, Institutional Quality and Economic Growth' (2012) *SSRN Electronic Journal*

Deibert R J and Rohozinski R, 'Risking Security: Policies and Paradoxes of Cyberspace Security' (2010) 4 *International Political Sociology*

Dent C, 'Confusion in a Legal Regime Built on Deception: The Case of Trade Marks' (2015) 5 *Queen Mary Journal of Intellectual Property*

Development Concept 'Azerbaijan 2020: The Vision of the Future' (2012)

Devlin P, *The Enforcement of Morals* (Oxford: Oxford University Press 1965)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems (NIS Directive)

Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Dolowitz D P and Marsh D, 'Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making' (2000) 13 *Governance*

Dolowitz D P and Marsh D, 'Who Learns What from Whom, A Review of Policy Transfer Literature' (1996) XLIV *Political Studies*

Draft International Convention to Enhance Protection from Cyber Crime and Terrorism *(*Stanford Draft 1999)

Dreßing H, Bailer J, Anders A, Wagner H and Gallas C, 'Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact upon Victims' (2014) 17 *Cyberpsychology, Behavior, and Social Networking*

Duit A and Galaz V, 'Governance and Complexity Emerging Issues for Governance Theory' (2008) 21 *Governance*

Dutta S, Geiger T and Lanvin B, *Global Information Technology Report 2015* (WEF 2015)

Dworkin R, 'Do We Have a Right to Pornography?' in *A Matter of Principle*, (Cambridge, MA: Harvard University Press, 1985)

EC-Council, *Computer Forensics: Investigating Network Intrusions and Cybercrime* (EC-Council Press, Cengage Learning, 2017)

E-Governance Academy Foundation (Estonia), *National Cyber Security Index*, 2018 http://ncsi.ega.ee/

European Commission (EC), 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', JOIN (2013) 1 final

European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (1953) ETS No.5

European Network of Forensic Science Institutes (ENFSI), *Best Practice Manual for the Forensic Examination of Digital Technology* (2015)

Evans M, 'Teenager Who Hacked Governments Worldwide Is Spared Jail' (The Telegraph, 2016) http://www.telegraph.co.uk/news/2016/07/20/teenage-hacker/

Evans M, *New Directions in the Study of Policy Transfer* (Routledge 2010)

Expression Online Initiative, *Searching for Freedom: Online Expression in Azerbaijan* (2012)

Fafinski S and Minassian N, *UK Cybercrime Report 2009*

Fafinski S, *Computer Misuse* (Willan Pub 2009)

Fafinski S, Dutton W H and Margetts H, 'Mapping and Measuring Cybercrime' (2010) 18 OII Forum Discussion Paper

Feeley M M, 'Three Voices of Socio-Legal Studies' (2001) 35 *Israel Law Review*

Fenwick H, Civil Liberties and Human Rights (Routledge-Cavendish; 4th edn, 2007)

Fidler D P, 'Cyberspace, Terrorism and International Law' (2016) 21 *Journal of Conflict and Security Law*

Finklea K M, *Identity theft: Trends and issues* (CRS Report for Members and Committees of Congress, 2014)

Foster J S, Gjelde E, Graham W R and Hermann R J, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (Washington D.C.: EMP Commission, 2008)

Freedom House, *Freedom on the Net Report 2014*

Freedom House, *Freedom on the Net Report 2015*

Freedom House, *Freedom on the Net Report 2016*

Freedom House, *Freedom on the Net Report 2017*

Garfinkel S, "Automated Digital Forensics" (2015), *Crcs.seas.harvard.edu*, http://crcs.seas.harvard.edu/event/simson-garfinkel-automated-digital-forensics.

Garland D, *The Culture of Control: Crime and Social Order in Contemporary Society* (OUP Oxford, 2001)

Gercke M, 'Legal Approaches to Criminalise Identity Theft' in UNODC, *Handbook on Identity- related Crime* (United Nations, 2011)

Gercke M, *Project on cybercrime: Internet-related identity theft* (Discussion paper Economic Crime Division Directorate General of Human Rights and Legal Affairs, 2007)

Gercke M, 'Strategy, Policy, Legislation, Prevention and Enforcement' in Duyan A (Edn), *Analyzing Different Dimensions and New Threats in Defence against Terrorism (104 NATO Science for Peace and Security. Series E: Human and Societal Dynamics*) (IOS Press, 2012)

Gercke M, 'The Slow Wake of a Global Approach against Cybercrime' (2006) 7 *Computer Law Review International*

Gercke M, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU 2014)

Ghazaleh S A, 'Fighting Cybersquatting: Nominet Disputes Resolution Service Policy' (2011) *32 Business Law Review*

Ghosh S and Turrini E, *Cybercrimes: A Multidisciplinary Analysis* (Springer Berlin 2014)

Gillespie A, *Cybercrime: Key Issues and Debates* (Routledge 2015)

Gordon S and Ford R, 'On the Definition and Classification of Cybercrime' (2006) 2 *Journal in Computer Virology*

Grabosky P, 'The Global Dimension of Cybercrime' (2004) 6 Glo*bal Crime*

Grabosky P, *Electronic Crime* (Pearson Prentice Hall 2007)

Gragido W and Pirc J, *Cybercrime and Espionage* (Syngress 2011)

Guinchard A, 'Crime in virtual worlds: The limits of criminal law' (2010) 24 (2) *International Review of Law, Computers & Technology*

Guinchard A, 'Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime.' (2018) 2 (2) *Journal of Information Rights, Policy and Practice*

Guliyev R and Imanov M, *Criminal Law: The Special Part* (Digesta, Baku 2001)

Hallevy G, *A Modern Treatise on the Principle of Legality in Criminal Law* (Springer Berlin 2014)

Harašta J, 'Cyber Security in Young Democracies', (2013) 20.4 *Jurisprudence*

Hawkins G J and Zimring F E, *Pornography in a Free Society* (Cambridge: Cambridge University Press, 2011)

Hayes B, Jeandesboz J, Ragazzi F, Simon S and Mitsilegas V, *The law enforcement challenges of cybercrime: are we really playing catch-up?* (European Union, Brussels, 2015)

Hert P, Fuster G G and Koops B J, 'Fighting Cybercrime in the Two Europes.*'* (2006) 77 *Revue internationale de droit pénal*

Higgins G E and Makin D A, 'Does social learning theory condition the effects of low self-control on college students' software piracy?' (2004) 2 *Journal of Economic Crime Management*

Hinduja S, 'Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams' (2004) 27 *Policing: An International Journal of Police Strategies & Management*

Hirst P, Thompson G, 'Globalization and the future of the nation state' (1995) 24 *Economy and Society*

HM Government, 'Developing our capability in cyber security' (2015)

Hoeren T, Westkamp G, *Study on voluntary collaboration practices in addressing online infringements of trademark rights, design rights, copyright and rights related to copyright* (EUIPO 2016)

Holt T J and Bossler A M, 'An Assessment of the Current State of Cybercrime Scholarship' (2013) 35 *Deviant Behavior*

Holt T J and Bossler A M, *Cybercrime in Progress: Theory and prevention of technology-enabled offenses* (Routledge 2016)

Holt T J, Bossler A M and Seigfried-Spellar K C, *Cybercrime and Digital Forensics* (Routledge 2015)

Holt T J, *Crime On-Line* (Durham, N.C.: Carolina Academic Press, 2nd edn. 2013) 8

Home Office*,* Serious and Organised Crime Strategy (London: Home Office, 2013)

Home Office, UK Cyber Crime Strategy (2010)

Hough M, 'Thinking about Effectiveness' (1987) 27 *British Justice Criminology Journal*

Human Rights Watch, *World Report 2018*, https://www.hrw.org/sites/default/files/world_report_download/201801world_report_web.pdf

Hutchinson T, 'Doctrinal research' in Watkins, D., Burton, M. *Research Methods in Law* (Routledge 2013)

ICB4PAC - Electronic Crimes: Knowledge-based Report (Assessment) (2013)

Imamverdiyev Y N, 'Coordination problems in information security of e-government', (2014) 2 *Journal of Problems of Information Society*

Imamverdiyev Y N, 'Next generation national cyber security strategies' (2013) 2 *Journal of Problems of Information Society*

Implementation of the European Neighbourhood Policy in Azerbaijan, Brussels, SWD (2015) 64 final, http://eeas.europa.eu/enp/pdf/2015/azerbaijan-enp-report-2015_en.pd

Infringements of Intellectual Property Rights on the Internet (2014), (A conference co-chaired and hosted by the Office for Harmonization in the Internal Market (OHIM), Europol and Eurojust)

Intellectual Property Office, 'A consultation on changes to the penalties for offences under sections 107(2A) and 198(1A) of the Copyright, Designs and Patents Act 1988 (Penalties for Online Copyright Infringement)' (2015)

Intellectual Property Office, 'Criminal Sanctions for Online Copyright Infringement: Government Consultation Response' (2016)

International Bar Association's Human Rights Institute (IBAHRI), *Azerbaijan: Freedom of Expression on trial* (2014)

International Covenant on Civil and Political Rights (ICCPR) UN Doc. A/6316 (1966)

ISO copyright office, ISO/IEC 27032:2012, *'Information technology – Security techniques – Guidelines for cybersecurity,* (Geneva, Switzerland 2012)

ISO copyright office, ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition and preservation of digital evidence,* (Geneva, Switzerland 2012*)*

ITU, *Cybercrime/e-crimes: Model policy guidelines and legislative texts* (HIPCAR. BDT, Geneva, 2012)

ITU, *Global Cybersecurity Index 2017*

ITU*, Measuring the Information Society Report 2014*

ITU, *Measuring the Information Society Report 2017*

ITU, *National Cybersecurity Strategy Guide*. (Geneva, 2012) 21.

ITU, *Recommendation ITU-T X.1205 "Overview of Cybersecurity"* (2008)

ITU, *The ITU National Cybersecurity Strategy Guide* (Geneva, 2012)

Jafarguliyev M, *Criminal Procedure of the Republic of Azerbaijan (Azərbaycan Respublikası Cinayət prosesi)* (Baku, Ganun, 2008)

James J I and Gladyshev P, 'A Survey of Mutual Legal Assistance Involving Digital Evidence' (2016) 18 *Digital Investigation*

James J J and Gladyshev J, 'Challenges with Automation in Digital Forensic Investigations' (2013) *Computers and Society*

Jewkes Y and Yar M (Eds) *Handbook of Internet Crime* (Willan, 2009)

Jones N, George E, Mérida I, Rasmussen U and Völzow V, *Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges* (CyberCrime@IPA, 2014) Version 2.0

Jones T and Newburn T, *Policy Transfer and Criminal Justice* (Open University Press 2007)

Kaspersen H, *Cybercrime and Internet Jurisdiction* (Council of Europe, 2009)

Kaspersky, *Kaspersky Security Bulletin* 2014 Europe overtakes US' Kaspersky, *Kaspersky Security Bulletin* 2016 (Kaspersky Lab 2016)

Kaspersky, *Kaspersky Security Bulletin* 2017 (Kaspersky Lab 2017)

Kent G, 'Sharing Investigation Specific Data with Law Enforcement - An International Approach' (Stanford Public Law Working Paper 2014) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413#

Kerr O, 'Criminal Law in Virtual Worlds' (2008) *University of Chicago Legal Forum*

Kerr O, 'Searches and Seizures in a Digital World' (2005) 119 *Harvard Law Review*

Kirwan G and Power A, *Psychology of Cyber Crime* (IGI Global 2014)

Kohl U, *Jurisdiction and the Internet* (Cambridge: CUP 1st edn, 2007)

Koops B J, 'Technology and the Crime Society: Rethinking Legal Protection' (2009) 1 *Law, Innovation and Technology*

Koops B J, Leenes R E, Meints M, Meulen N and Jaquet-Chiffelle D J, 'A Typology of Identity-Related Crime' (2009) 12 *Information, Communication & Society*

Kosachenko A (Edn), Criminal law: General Part (4th edn, Moscow: Norma Publisher, 2009)

KPMG International Cooperative, *Cyber threat intelligence and the lessons from law enforcement* (2013)

Lab S P, *Crime Prevention: Approaches, Practices, and Evaluations* (Routledge; 9th edition, 2016)

Lavorgna A, 'Cyber-Organised Crime. A Case of Moral Panic?' (2018) *Trends in Organized Crime*

Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics*, LAW COM No. 245 (1997)

Lessig L, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

Levi M and Williams M L, 'Multi-Agency Partnerships in Cybercrime Reduction' (2013) 21 *Information Management & Computer Security*

Levi M, 'Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues' (2016) 67 *Crime, Law and Social Change*

Levi M, Doig A, Gundur R, Wall D S and Williams M. *The Implications of Economic Cybercrime for Policing* (London: City of London Corporation, 2015)

Madsen F G, *Transnational Organized Crime* (London: Routledge, 2010)

Mahmudov R S, 'Actual problems of regulation of the Internet', (2010) 8 *Journal of Problems of Information Society*

Makili-Aliyev K and Attiq-ur-Rehman, 'Cyber-Security Objective: Azerbaijan in the Digitalized World' (2013) 11 *SAM Review*

Mammadov B N and Asgarova A N, 'Necessity of global cybersecurity convention or the opportunities for Budapest Convention to become a global standard' (2014) 1 *Journal of Problems of Information Society*

Mansell R, Ang P H and Ballon P, *International Encyclopedia of Digital Communication and Society* (1st edn. John Wiley & Sons 2015)

Marchuk I, *The Fundamental Concept of Crime in International Criminal Law: A Comparative Law Analysis* (Heidelberg: Springer, 2014)

Masferrer A and Walker C, Countering Terrorism and Crossing Legal Boundaries in Masferrer A and Walker C, *Counter-Terrorism, Human Rights and The Rule of Law* (Cheltenham: Ed. elgar, 2013)

Maskus K, 'The New Globalisation of Intellectual Property Rights: What's New This Time?' (2014) 54 *Australian Economic History Review*

Mason J, *Qualitative Researching* (London: Sage, 2nd edition 2002)

McGuire M and Dowling S, 'Cybercrime: A review of the evidence' - Chapter 1: Cyber-dependent crimes (2013) *Home Office Research Report* 75

McKemmish R, 'What is Forensic Computing?' (1999) 118 *Australian Institute of Criminology*

McQuade S C, *Encyclopedia of Cybercrime* (Westport, Conn.: Greenwood Press, 2009)

McQuade S C, *Understanding and Managing Cybercrime* (Pearson/Allyn and Bacon 2006)

Media Rights Institute, *Execution of Judgments of The European Court of Human Rights in Azerbaijan, Status Quo Upon Azerbaijan's Chairmanship of the Committee of Ministers of The Council of Europe* (2014)

Mehtiyev M, 'Fighting transnational organized crimes is the priority duty' (Transmilli mütəşəkkil cinayətkarlığa qarşı mübarizə prioritet vəzifədir) Respublika qəzeti (newspaper), Baku 19 March 2013, http://www.mns.gov.az/az/pages/144-367.html

Merriam S B, *Qualitative Research: A Guide to Design and Implementation* (Jossey-Bass 2009)

Meulen N V and Koops B J, 'The Challenge of Identity Theft in Multi-Level Governance' in Rianne Letschert, Jan van Dijk, *The New Faces of Victimhood* (Springer 2011)

Milaj J, 'Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance' (2015) 30 *International Review of Law, Computers & Technology*

Mill J S, *On Liberty* (London: John W. Parker & Son 1859)

Mueller G, ‘Transnational crime: Definitions and Concepts’, in Williams, P. and Vlassis, D. (eds), *Combating Transnational Crime* (Portland, Oregon: Frank Cass publishers, 2001)

Mueller M, *Networks and States* (MIT Press 2010)

Murray A, *Information Technology Law: The Law and Society* (Oxford University Press, 2016)

National Audit Office, *The UK cyber security strategy: Landscape review, cross government* (House of Commons Papers 2013)

National Crime Agency (UK) Strategic Cyber Industry Group, *Cyber Crime Assessment (2016)*

National Information and Communication Technologies Strategy for the Development of the Republic of Azerbaijan (2003-2012) 2003

National Security Concept of Estonia (2010)

National Security Concept of Georgia (2012)

National Security Concept of the Republic of Azerbaijan (2007) No. 2198

National Strategy on the Development of the Information Society for the years 2014-2020 (2014)

NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/strategies-policies.html

Newman R C, *Computer Forensics: Evidence Collection and Management* (Auerbach Publications 2007)

Noaks L and Wincup E, *Criminological Research* (London: SAGE 2004)

O’Neill M E, ‘Old Crimes in New Bottles: Sanctioning Cybercrime’ (2000) 9 *George Mason Law Review*

Odagiri H, *Intellectual Property Rights, Development, and Catch Up* (Oxford: Oxford University Press, 2012)

Office for National Statistics, *Crime in England and Wales: year ending Sept 2016* (Ons.gov.uk, 2016)

Office for National Statistics, *Crime in England and Wales: year ending March 2018* (Ons.gov.uk, 2018)

Office for National Statistics, *Improving Crime Statistics for England and Wales – Progress Update- Office for National Statistics* (Ons.gov.uk, 2017)

Office for National Statistics*, Improving Crime Statistics for England and Wales – progress update July 2018* (Ons.gov.uk, 2018)

Office for National Statistics, *Methodological note: Work to extend the Crime Survey for England and Wales to include fraud and cyber-crime (*Ons.gov.uk*, 2014)*

Organisation for Economic Co-operation and Development, *Non-governmental perspectives on a new generation of national cybersecurity strategies* (Paris: OECD Publishing, 2012)

Orthmann C H and Hess K M, *Criminal Investigation* (Delmar Cengage Learning 2013)

Osborne D and Gaebler T, *Reinventing Government* (Addison-Wesley Pub Co 1992)

Ouimet M, 'Internet and crime trends' in Schmalleger M and Pittaro M, *Crimes of the Internet* (Prentice Hall 2009)

Oxman B H, 'Jurisdiction of States', in Bernhardt R. *Encyclopedia of Public International Law*, vol. 3 (Amsterdam: Elsevier Science Publishers, 1997)

Packer M J, *The Science of Qualitative Research* (New York: Cambridge University Press 2011)

Parliament Street Policy Paper, 'Policing and Cybercrime' (Parliament Street 2018)

Patton M Q, *Qualitative Research and Evaluation Methods* (Sage Publications 2002)

Picotti L and Salvadori I, *National legislation implementing the Convention on Cybercrime - Comparative analysis and good practices (*Council of Europe, Project on Cybercrime, Discussion Paper 2008)

Police Executive Research Forum, 'The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime' (2014) *Critical Issues in Policing Series*

PricewaterhouseCoopers LLP, *Global Economic Crime Survey* (2014)

PricewaterhouseCoopers LLP, *Global Economic Crime Survey (*2018)

Property Rights Alliance, *International Property Rights Index (2017)* https://internationalpropertyrightsindex.org/country/azerbaijan

Proposal for a Council framework decision to strengthen the criminal law framework to combat intellectual property offences Brussels, COM (2005)276 final, 2005/0127(COD) 2005/0128(CNS)

Qasimov V, *Information security: computer crimes and cyberterrorism* (*İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq)* (Baku: Elm 2007)

Quick D, Martini B and Choo K R, *Cloud Storage Forensics* (Syngress, 1st edition, 2014)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Reinsalu K, Rikk R, Krenjova J and Pernik P, *Situation Review: Safety and Security of Cyberspace and E-Democracy in the Eastern Partnership Countries* (e-Governance Academy 2017)

Resolution of the Plenum of the Supreme Court of the Republic of Azerbaijan 'On the judicial practice on considering complaints in private criminal prosecutions' (February 21, 2014 No 03)

Reyes A, *Cyber Crime Investigations* (Syngress Pub 2007)

Roach Anleu S L, *Law and Social Change* (London: SAGE, 2nd edn, 2010)

Rogers M and Seifried-Spellar K, *Digital Forensics and Cyber Crime* (Springer 2013*)*

Romero Moreno F, 'The Three Strikes and You Are Out Challenge', (2012) 3 *European Journal for Law and Technology*

Roscini M, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014)

Rose R R, 'What Is Lesson-Drawing?' (1991) 11 *Journal of Public Policy*

Ruan K, *Cybercrime and Cloud Forensics: Applications for Investigation Processes* (IGI Global, 2013)

Ryngaert C, *Jurisdiction in International Law* (Oxford: Oxford University Press, 2nd edition, 2015)

Samandarov F, *Commentary on the Criminal Code of the Republic of Azerbaijan, Second part (Azərbaycan Respublikası Cinayət Məcəlləsinin kommentariyası, İkinci hissə) (*Baku, Hüquq Yayın Evi, 2016)

Samandarov F, *Criminal law: General Part (Cinayət hüququ: Ümumi hissə)* (Baku: Hüquq ədəbiyyatı, 2002)

Schiff D N, 'Socio-Legal Theory: Social Structure and Law' (1976) *Modern Law Review*

Schjolberg S, *The History of Cybercrime: 1976-2014* (Books on Demand, 2014)

Science & Technology Committee, *Malware and cyber crime* (House of Commons London: The Stationery Office Limited 2011)

Scott C, 'Analysing Regulatory Space: Fragmented Resources and Institutional Design' (2001) *Public Law*

Second Additional Protocol to the European Convention on Extradition (1978) ETS 098

Seger A, *Cybercrime strategies - Discussion paper* (Global Project on Cybercrime, Council of Europe 2011)

Seidman I, *Interviewing as Qualitative Research* (New York: Teachers College Press 4th edition, 2013)

Shinder D L and Tittel E, *Scene of the Cybercrime* (Syngress Pub 2002)

Sieber U, 'Mastering Complexity in the Global Cyberspace: The Harmonisation of Computer-related Criminal Law' in Mireille D, Pieth M and Sieber U, *Les Chemins De L'harmonisation Pénale/ Harmonising Criminal Law* (Paris, France: Société de législation comparée, 2008)

Silverman D, *Doing Qualitative Research: A Practical Handbook* (London: Sage 2000)

Sir Robert Peel's Principles of Law Enforcement (1829) https://www.durham.police.uk/About-Us/Documents/Peels_Principles_Of_Law_Enforcement.pdf

Smith C J, Zhang S and Barberet R. *Routledge Handbook of International Criminology* (Routledge 2011)

Smith R G, Grabosky P and Urbas G, *Cyber Criminals on Trial* (Cambridge University Press 2004)

Smolaks M, 'Data Center Fire Kills Internet in Azerbaijan' (*DatacenterDynamics,* 2015) http://www.datacenterdynamics.com/power-cooling/data-center-fire-kills-internet-in-azerbaijan/95227.fullarticle

Sommer P, 'Forensic Science Standards in Fast-Changing Environments' (2010) 50 *Science & Justice*

Stewart H, 'The Limits of the Harm Principle' (2009) 4 *Criminal Law and Philosophy*

Strategic road maps for the national economy and main economic sectors (Azerbaijan) 2016

Swiss Institute of Comparative Law*, Comparative Study on blocking, filtering and take-down of illegal Internet content* (2015)

Taylor N, 'Policing, Privacy and Proportionality', *European Human Rights Law Review* (Special issue: privacy 2003)

TechUK, 'Partners against crime- How can industry help the police to fight cyber-crime?' (2015)

Terrill R J, *World Criminal Justice Systems* (Routledge, 9th edition 2015)

The Commonwealth, Model Law on Computer and Computer Related Crime (LMM (02)17) (Oct. 2002)

The Digital Defenders Partnership (DDP), Insights into Internet freedom in Central Asia: Azerbaijan (2013) https://www.digitaldefenders.org/azerbaijan/

The National Strategy for Information Society Development in Azerbaijan for 2014-2020 (2014)

The Software Aliance, *The Compliance Gap: BSA Global Software Survey 2016,* http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_InBrief_A4.pdf

The UK Cyber Security Strategy 2011-2016, Annual Report (2016)

Thomas D and Loader B, *Cybercrime Law Enforcement, Security and Surveillance in the Information Age* (Routledge 2000)

TNS BMRB, *CSEW Fraud and Cyber-crime Development: Field Trial – October 2015*

Towse R, 'The Quest for Evidence on the Economic Effects of Copyright Law' (2013) 37 *Cambridge Journal of Economics*

UK National Security Strategy 2010

UK National Security Strategy and Strategic Defence and Security Review (2015)

UN General Assembly, Creation of a global culture of cybersecurity and the protection of critical information infrastructures (2004) A/RES/58/199

UN General Assembly, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (2009), A/RES/64/211

UN General Assembly, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2001) A/RES/54/263

UN General Assembly, United Nations Convention against Transnational Organized Crime: resolution / adopted by the General Assembly (2001) A/RES/55/25

UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (8 April 1988).

UNDP, *Modernization of Sustainability and Efficiency of ICT infrastructure and ICT services in the Republic of Azerbaijan* (UNDP 2013)

United Nations Economic and Social Council (UNESC), United Nations Guidelines for the Prevention of Crime, Economic and Social Council resolution (Council resolution 2002/13 - Annex).

United Nations Human Rights Committee, *General Comment No. 34. Article 19: Freedoms of opinion and expression.* (2011) CCPR/C/GC/34

United Nations Human Rights Council, *Concluding observations* (2016) CCPR/C/AZE/CO/4

United Nations Office on Drugs and Crime, *Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies* (UNODC, Vienna, Austria, 2014)

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (United Nations 2013)

United Nations Office on Drugs and Crime, *Mutual Legal Assistance Request Writer Tool* (2016)

United Nations Office on Drugs and Crime, *The Globalisation of Crime. A Transnational Organized Crime Threat Assessment*. (United Nations Publications 2010)

United Nations Report of the International Law Commission, 58th session, General Assembly Official Records, Supplement No. 10 (A/61/10)

US Department of Justice, *The National Information Infrastructure Protection Act of 1996* (Legislative Analysis 1996)

Walden I, *Computer Crimes and Digital Investigations* (Oxford University Press 2007)

Wall D S and Williams M, 'Policing Diversity in the Digital Age' (2007) 7 *Criminology & Criminal Justice*

Wall D S, 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', in Brownsword R, Scotford E and Yeung K (Edn.), The Oxford Handbook of the Law and Regulation of Technology (Oxford: Oxford University Press 2017)

Wall D S, 'Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime', (2008) 22 *International Review of Law Computers and Technology*

Wall D S, 'Cybercrimes and the Internet' in Wall D S (Edn.) *Crime and the Internet*, (New York: Routledge 2001)

Wall D S, 'Locking up hackers could do more harm than good' (*The Conversation*, 2013) http://theconversation.com/locking-up-hackers-could-do-more-harm-than-good-15889

Wall D S, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' (2007) 8 *Police Practice and Research*

Wall D S, 'Policing identity crimes' (2013) 23 *Policing and Society*

Wall D S, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge: Polity 2007)

Walport M, *Annual Report of the Government Chief Scientific Adviser 2015: Forensic Science and Beyond: Authenticity, Provenance and Assurance*, vol. 1 (Government Office for Science: London, 2015)

Weatherley M, 'Follow the Money': Financial Options to Assist in the Battle against Online IP Piracy' (A Discussion Paper, 2014)

Welsh W N and Harris P W, *Criminal Justice Policy and Planning: Planned Change* (Routledge, 5th edition 2016)

Wilkinson D and Birmingham P, *Using Research Instruments: A Guide for Researchers* (Routledge Falmer 2003)

Williams B (ed.), *Obscenity and Film Censorship* (Cambridge: Cambridge University Press, 1981)

Williams K S, 'Transnational developments in Internet Law' in Jewkes Y. and Yar M (Ed.) *Handbook of Internet Crime* (London: Willan Publishing 2010)

Wincup E, *Criminological Research: Understanding Qualitative Methods* (2nd edn, London: Sage 2017)

World Economic Forum, *Recommendations for Public-Private Partnership against Cybercrime* (2016)

WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (1994) (TRIPS Agreement)

Yar M, *Cybercrime and Society* (London: SAGE Publications 2013)

Yin R K, *Qualitative Research from Start to Finish* (New York: The Guilford Press, 2011)

Young R, Zhang L and Prybutok V R, 'Hacking into the Minds of Hackers' (2007) 24 *Information Systems Management*

Online sources

'Academic Centres of Excellence in Cyber Security Research - NCSC Site' (*Ncsc.gov.uk*, 2018) https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research

'Armenian Hackers Leak ID Cards, Passports of 5K Azerbaijani Citizens' (*HackRead,* 2015) https://www.hackread.com/armenian-azerbaijani-cyberwar/

'Azerbaijan Airline Websites, hit by Cyber Attack', (*The Daily Star,* 2012) http://www.dailystar.com.lb/News/Middle-East/2012/Feb-24/164417-azerbaijan-airline-websites-tv-hit-bycyber-attack.ashx#axzz2TRrsILKJ

'Azerbaijan IP Investigation | Copyright Patent Infringement' (*IP Investigator,* 2016, http://www.iprightsinvestigators.com/azerbaijan-ip-investigation.php

'Azerbaijan to accomplish e-government project by 2020', (*AzerNews.az,* 2014) http://www.azernews.az/business/74290.html

'Azerbaijan: Cyber Attacks on Rise, Warns Microsoft-UNPAN - United Nations Public Administration Network' (*Unpan.org.*, 2016). http://www.unpan.org/PublicAdministrationNews/tabid/115/mctl/ArticleView/ModuleID/1467/articleId/49409

'Azerbaijani business faces cyber threat' (*AzerNews,* 2016), https://www.azernews.az/business/99644.html

'Azerbaijani Hackers Deface NATO-Armenia, Embassy Websites In 40 Countries' (*HackRead*, 2016) https://www.hackread.com/azerbaijani-hackers-defac-nato-armenia-embassy-sites/

'Azerbaijani Official Websites Victimized by Cyberattack', (*Radio Free Europe/Radio Liberty*, (2012), https://www.rferl.org/a/azerbaijani_websites_hacked/24454171.html

‘Brief History of the Internet - Internet Timeline | Internet Society’ (Internetsociety.org, 2015) http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Origins accessed 26 May 2018

‘Can Hackers steal money from Azerbaijani banks? – The number of attacks have been increased’ (*Publika.Az*, 2016), http://publika.az/news/tehlil/178593.html

‘CERT Warns of Cyber Attack by Armenian Hackers’ (*AzerNews,* 2015), http://www.azernews.az/azerbaijan/80903.html

‘Changes to Penalties for Online Copyright Infringement’ (*GOV.UK*, 2015) https://www.gov.uk/government/consultations/changes-to-penalties-for-online-copyright-infringement

‘Civilians to Help Police Investigate Cybercrimes, Says Theresa May’, (*BBC News,* 2016) http://www.bbc.com/news/uk-35354139

‘Crime Analysis for 2017’ (mia.gov.az 2018) http://www.mia.gov.az/index.php?/az/content/29958/

‘Cyber Aware’ (*Cyberaware.gov.uk,* 2018) https://www.cyberaware.gov.uk/

‘Cyber Crime is No Longer the Preserve of Bedroom Hackers’ (*GOV.UK*, 2013) https://www.gov.uk/government/news/cyber-crime-is-no-longer-the-preserve-of-bedroom-hackers

‘Cyber Schools Programme’ (*GOV.UK,* 2018) https://www.gov.uk/guidance/cyber-schools-programme;

‘Cyber Security Information Sharing Partnership (CISP) - NCSC Site’ (*Ncsc.gov.uk*, 2018) https://www.ncsc.gov.uk/cisp

‘Cyber Security Lessons Offered to Schools in England’ (*BBC News,* 2017) https://www.bbc.co.uk/news/education-38938519

‘Defence Cyber Protection Partnership’ (*GOV.UK*, 2016) https://www.gov.uk/government/collections/defence-cyber-protection-partnership.

‘Digital and Cyber Crime | College Of Policing’ (*College.police.uk,* 2018) http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx

‘Europe overtakes US’ as the largest perpetrator of global cybercrime’ (*Information Age,* 2017) http://www.information-age.com/europe-overtakes-us-largest-perpetrator-global-cybercrime-123466109/

‘Extracurricular Cyber Clubs to Inspire and Identify Tomorrow’s Cyber Security Professionals’ (*GOV.UK*, 2018) https://www.gov.uk/government/news/extracurricular-cyber-clubs-to-inspire-and-identify-tomorrows-cyber-security-professionals;

‘Fifth Arrest in Talktalk Investigation’, (*Metropolitan Police,* 2015) http://news.met.police.uk/news/fifth-arrest-in-talktalk-investigation-139221

‘Fighting over Nagorno Karabakh Takes to Cyber Space’ (*Eurasianet.org*, 2016) https://eurasianet.org/fighting-over-nagorno-karabakh-takes-to-cyber-space

‘How Copyright Infringements are Punished in Azerbaijan’ (‘Azərbaycanda piratçılıq edənlər necə cəzalandırılır.’), (*Copag.gov.az,* 2018) http://copag.gov.az/copag/az/content/news/972

‘How to Remain 100% Anonymous on the Internet?’ (*Security.stackexchange.com,* 2015) http://security.stackexchange.com/questions/29196/how-to-remain-100-anonymous-on-the-internet accessed 25 May 2018

‘Information Security Management Policy on Safeguarding Data – Storage, Backup and Encryption’, (*It.leeds.ac.uk,* 2018) http://it.leeds.ac.uk/info/116/policies/255/policy_on_safeguarding_data-storage_backup_and_encryption

‘Information Warfare: Armenia-Azerbaijan Cyber War Intensifies Amid Karabakh Clashes - Karabakh | Armenianow.Com’ (*Armenianow.com*, 2016) https://www.armenianow.com/karabakh/71214/armenia_karabakh_azerbaijan_information_warfare

‘Iran Cyber Army’ Hits Azerbaijan State TV Site’ (*Phys.org*, 2012) https://phys.org/news/2012-02-iran-cyber-army-azerbaijan-state.html

‘Kaspersky Lab: Azerbaijan could come under increasing cyber-attacks in connection with geopolitical risks’ (*En.apa.az*, 2016) http://en.apa.az/azerbaijan-economy/infrastructure/kaspersky-lab-nagorno-karabakh-conflict-increases-risk-of-cyber-attack-on-azerbaijan.html

‘Mass Cyber-Attack Hits Government Websites’ (*AzerNews.az*, 2012) https://www.azernews.az/nation/40349.html

‘Metadata on indicators’ (‘Göstəricilərə Dair Məlumat Sistemi’) (*Azstat.org,* 2017) http://www.azstat.org/MetaDataG/bchapgos.jsp?prkod=90001&prskod=36

‘“Microsoft” has warned Azerbaijan’ ("Microsoft" şirkəti Azərbaycana xəbərdarlıq edib) (*Report Information Agency,* 2016) https://report.az/i-kt/microsoft-sirketi-azerbaycana-xeberdarliq-edib/

‘“Monte Melkonian Cyber Army” Hacks 47 Azerbaijani Websites’ (*armenpress.am,* 2015) http://armenpress.am/eng/news/810768/%E2%80%9Cmonte-melkonian-cyber-army%E2%80%9D-hacks-47-azerbaijani-websites.html

‘Number of cyber-attacks in Azerbaijan increases annually by 30%’ (*Report News Agency*, 2015) https://report.az/en/ict/the-number-of-cyber-attacks-in-azerbaijan-increases-annually-by-30/

'OSCE Trains Cybercrime Investigators from Georgia and Azerbaijan | OSCE' (Osce.org, 2017) https://www.osce.org/secretariat/307621

‘Patriotic Hackers’ in Armenia and Azerbaijan Escalate Crisis with Cyber Attacks’ (*Atlantic Council*, 2012) <https://www.atlanticcouncil.org/blogs/natosource/patriotic-hackers-in-armenia-and-azerbaijan-escalate-crisis-with-cyber-attacks>;

‘Platform to Match Volunteer Skills to Cybercrime Investigations | Office of Northamptonshire Police and Crime Commissioner’ (*Office of Northamptonshire Police and Crime Commissioner*, 2018) https://www.northantspcc.org.uk/platform-to-match-volunteer-skills-to-cybercrime-investigations/

‘Police will fight cybercriminals’, (‘Kibercinayətkarlarla Polis Mübarizə Aparacaq’), (*Sputnik.az*, 2015) http://sputnik.az/radio/20151216/403058771.html

'Project Co-Ordinator in Baku Organised a Training Course on Basic Digital Forensic | OSCE POLIS' (*Polis.osce.org*, 2015) https://polis.osce.org/node/644

'Regional Conference on Cybercrime Kicks Off in Baku' (*Aztv.az*, 2017) http://www.aztv.az/readnews.php?lang=en&id=4910

‘State Security Service reveals international cybercrime group stealing 3.7m AZN from Azerbaijani bank’ *(Report.az,* 2017) https://report.az/en/incident/state-security-service-reveals-members-of-international-cybercrime-group-stealing-3-7-million-azn-fr/

‘The Regulation of the Electronic Security Center should be prepared through public engagement’, (‘Elektron Təhlükəsizlik Mərkəzinin ƏSASNAMƏSİ İCTİMAİYYƏTİN İŞTİRAKI İLƏ HAZIRLANMALIDIR’) | AIF", (*Aif.az,* 2012) http://aif.az/etm-nin-%C9%99sasnam%C9%99si-ictimaiyy%C9%99tin-istiraki-il%C9%99-hazirlanmalidir/

‘Three Strikes and You’re out? Delays are Costing the UK’s Piracy Laws - Intellectual Property Magazine’ (*Intellectualpropertymagazine.com*, 2018) https://www.intellectualpropertymagazine.com/incoming/three-strikes-and-youre-out-delays-are-costing-the-uk-s-piracy-laws-87365.htm

‘UK Domain Dispute Resolution Service’ (*Nominet,* 2017) https://www.nominet.uk/domains/resolving-uk-domain-disputes-and-complaints/

'UK to Establish Court for Cybercrime in London' (*Bankinfosecurity.com*, 2018) https://www.bankinfosecurity.com/uk-to-establish-court-for-cybercrime-in-london-a-11174

‘What does the empowerment of the Ministry of Internal Affairs with further investigation powers promise?’ (‘DİN-In Istintaq Səlahiyyətlərinin Genişləndirilməsi Nə Vəd Edir?’) (*Azinforum.az* 2015) http://azinforum.az/din-in-istintaq-s%C9%99lahiyy%C9%99tl%C9%99rinin-genisl%C9%99ndirilm%C9%99si-n%C9%99-v%C9%99d-edir/

‘World-Class Fraud and Cybercrime Court Approved for London’s Fleetbank House Site’ (*GOV.UK*, 2018) https://www.gov.uk/government/news/worldclass-fraud-and-cybercrime-court-approved-for-londons-fleetbank-house-site

‘WTO | Accession Status: Azerbaijan’, (*Wto.org,* 2016) https://www.wto.org/english/thewto_e/acc_e/a1_azerbaidjan_e.htm

'1.7GB Documents Leaked from Special State Protection Service of Azerbaijan' (Cyber War News, 2013) https://www.cyberwarnews.info/2013/01/20/1-7gb-documents-leaked-from-special-state-protection-service-of-azerbaijan/

Academy of the State Security Service of the Republic of Azerbaijan named after Heydar Aliyev http://dtx.gov.az/en/articles4.php

Apple http://www.apple.com/privacy/transparency-reports/

APWG https://www.antiphishing.org/about-APWG/

Azerbaijan Internet Forum http://aif.az/

CERT.AZ description as per RfC 2350, http://www.cert.az/s/u/document/rfc_2350.pdf

Computer Emergency Response Centre https://cert.gov.az/az

Educational video resources (Ministry of Education), www.video.edu.az

E-Government Portal (Ministry of Education), www.e-gov.az

E-health (Ministry of Health), http://e-health.gov.az/-

Electronic learning resources (Ministry of Education), www.e-derslik.edu.az

Electronic learning resources (Ministry of Education), www.e-resurs.edu.az

Electron Security Service http://www.cert.az/

Facebook https://transparency.facebook.com/government-data-requests/country/AZ;

Faculty of Law, Baku State University, http://law.bsu.edu.az/az/content/cnayt_hququ_v_krmnologya_kafedrasi__312

FIRST https://www.first.org/

Google https://transparencyreport.google.com/user-data/overview?hl=en

Internet Watch Foundation https://www.iwf.org.uk/

Internet World Stats http://www.internetworldstats.com/stats.htm

Lexis Library, https://www.lexisnexis.com/uk/legal/

Microsoft https://www.microsoft.com/en-us/about/corporate-responsibility/lerr;

Ministry of Internal Affairs http://mia.gov.az/

Ministry of Justice of the Republic of Azerbaijan, http://www.justice.gov.az/images/toplu-2014.pdf

OpenNet Initiative https://opennet.net/research/profiles/azerbaijan

State Fund for Development of Information Technologies, http://ictfund.gov.az/?page_id=1373&lang=en

State Security Service http://dtx.gov.az/en/haqqimizda2.php

State Statistical Committee of the Republic of Azerbaijan https://www.stat.gov.az/source/information_society/?lang=en

Statistics on the Implementation of the 'State Program on education of Azerbaijani Youth abroad in 2007-2015', http://xaricdetehsil.edu.gov.az/uploads/Statistika4.pdf

The Dispute Resolution Service Policy – Nominet, https://s3-eu-west-1.amazonaws.com/nominet-prod/wp-content/uploads/2017/10/17150434/final-proposed-DRS-policy.pdf

The Trusted Introducer Service https://www.trusted-introducer.org/index.html

Twitter https://transparency.twitter.com/

Westlaw UK http://legalresearch.westlaw.co.uk/

World Development Indicators of the World Bank https://fred.stlouisfed.org/series/ITNETSECRP6AE

Yahoo https://transparency.oath.com/

Appendix 1

Fieldwork

Interview Guide

Section One: Demographics and Background

At the beginning, I would like to start by asking you some personal questions about your background, the nature of your job, and qualifications; the purpose is to set your answer in the context of your professional profile.

A1. Could you specify your age band? Is it (20-29/30-39/40-49/50+)?

A2. What is your job title?

A3. How long have you been working in your present job?

A4. What are your responsibilities?

A4.1. What are your responsibilities in terms of cybercrime fighting?

A5. What qualifications/expertise do you have pertaining to this field?

Section Two: Phenomenon of Cybercrime in Azerbaijan

This section is to identify the nature and scale of cybercrime, underlying factors linked to changes in its extent and impact. Thus, I would like to ask you questions about the following issues.

A6. What, if any, is the formal/working definition of cybercrime that has been adopted by your organization?

A6.1. What activities do you think the term ‘cybercrime’ incorporates?

A6.2. What activities do you think this term does not or should not incorporate?

A7. What are the common types of cybercrime you are dealing with in your organization?

A8. What do you think about the current threats or risks of cybercrime either to the country or to your organization? Is any severe or not? Which is the worst? Are there any risks or threats which are novel or new?

A9. Which underlying factors are linked to changes in the impact and scale of cybercrime in the country?

A10. Which mechanisms are in place for the detection and reporting of cybercrime? Do you think the current detection and reporting mechanisms are effective in responding to cybercrime? Why?

Section Three: Policy Responses of Azerbaijan to Cybercrime

This section focuses on the relevant policy and strategy of the country, as well as actions undertaken against cybercrimes.

A11. Is there a dedicated cybercrime policy and strategy established in your organization?

A11.1. Is it adequate or should there be something different?

A11.2. How are the outputs and impacts measured?

A12. Do you think the state as a whole has developed an adequate cybercrime policy and strategy? What could be done to make improvements in this regard?

A13. Do you think there is a sufficient institutional apparatus for fighting cybercrime? Are the institutions dealing with cybercrime effective?

A14. What are the capabilities, roles and responsibilities of the organization you are working for in terms of fighting cybercrime?

A14.1. Do you think fighting cybercrime has given suitably high priority within your organization?

A14.2. Are there enough staff?

A14.3. Are there enough financial and technical resources?

A14.4. Within present personnel, are they the sufficiently qualified and trained?

A14.5. With regard to your involvement in fighting against cybercrime, what do think about the training you received?

A14.6. Does your organization have enough knowledge to evaluate the intended consequences of actions undertaken against cybercrime?

A14.6. Countermeasures of your institution ever overcome/breached by cybercriminals?

A15. Who are the stakeholders you are working with in terms of cybercrime-control and prevention?

A15.1. How frequently do you cooperate with other governmental authorities? On what issues do you cooperate? Do they ask you to help more than you ask them? With what outcome, is it successful?

A15.2. How frequent do you cooperate with the private sector? On what issue do you cooperate? Do they ask you to help more than you ask them? With what outcome, is it successful?

A15.3. Do you think the roles and resources are effectively and efficiently allocated among stakeholders? What needs to be done differently in this regard? Why?

A15.4. Is there a need for more resources and more intensive and efficient cooperation to respond appropriately to cybercrime? Why?

A16. What level of resources does it take to disrupt cybercrime?

A16.1. What level of resources would it take to prevent cybercrime? Which prevention measures exists? What extra measures of prevention are needed, if any?

Section Four: Regulatory and Criminal Law Responses to Cybercrime

This section will ask about the appropriateness of national legislation and frameworks.

A17. Do you think Azerbaijan has established a sufficient legal framework to respond to cybercrime? Is there a need to pass extra laws to deal with cyberspace? Why?

A18. Do you think legal measures undertaken in fighting cybercrime are appropriate in protecting and respecting individual rights and freedoms?

A19. What are the challenges in observing them?

A20. What do you think of the adequacy, effectiveness and efficiency of the Criminal Code on combatting cybercrime?

A20.1. Do you think the Code appropriately defines and regulates cybercrime acts that threaten the country?

A20.2. Which, if any, acts should be criminalized or decriminalized? Why?

A20.3. To what extent are the sanctions imposed for cybercrime effective and fair? Why?

Section Five: Investigatory Powers and International Cooperation Responses to Cybercrime

The evaluation of procedural measures and instruments, as well as the appropriateness of criminal procedural laws and investigative techniques will be the main focus of questions in this section.

A21. What do you think about 1) legal 2) regulatory 3) technical powers applied to investigate/adjudicate cybercrime?

A21.1. Are they adequate and specific enough? What needs to be changed in each respect?

A21.2. How about fairness, effectiveness and efficiency?

A21.3. Is there any need or pressure (national and international) to change the law? Do you think more or less procedural powers and instruments are needed?

A21.4. Which relationship exists between three techniques; and which one(s) have been prioritized? Is prosecution always the best approach? What technique can be applied as an alternative?

A22. How often do you need to obtain a court warrant in order to proceed with an investigation? Do you think it is necessary and important to issue a court warrant in order to implement procedural powers for the investigation of

cybercrime? Do you think that procedural provisions appropriately regulate this issue? What factors do you consider before applying for a court warrant?

A22. Do you think that legal regulations provide an appropriate balance between the effective use of investigatory powers and the protection of national interest and the respect of human rights and citizens' rights of people? Why?

A23. To what extent are procedural laws adequate in addressing challenges of collecting and using digital evidence? What, if anything, needs to be improved in this regard?

A24. Is the necessary capacity for collecting and using digital evidence available? Do you have access to up-to-date tools and expertise?

A25. Do you think the current level of international cooperation against cybercrime, and for the collection of digital evidence located outside the country is effective?

A25.1. Is international cooperation used in many cases? Do reported cybercrimes actually cross borders? What percentage of cybercrime acts reported/ investigated/adjudicated involve transnational dimensions?

A25.2. How many MLA requests are sent and received on average per year? What is the average time for response to requests sent and received?

A25.3. How much and how difficult it is when Azerbaijan asks for cooperation? How about when Azerbaijan is asked for cooperation?

A25.4. How often do you send or receive information without any request having been made and on your own initiative? In your experience, how relevant is such information and what follow up do you give to such information?

A25.5. Is cooperation with foreign service providers (such as Google, Facebook, Twitter, etc) common? What challenges are there in this regard?

A25.5. What help do you think you may expect to receive from your foreign partners when cooperating with them to investigate/adjudicate cybercrimes? Does it depend on the partner? How so?

Section Six: Concluding Questions

A26. Is there any way that you feel the policy, laws, procedures, or cooperation measures could be changed in Azerbaijan in order to enhance the capacity of the country in responding to cybercrime, or to make the situation fairer and safer for the public?

A27. Do you have any documents or guides published by your organisation or authority that might be helpful for my research? Could you provide me, if possible?

A28. Is there anything you would like to add?

Thank you!

INFORMATION SHEET

You are being invited to take part in a PhD research project conducted at the University of Leeds, School of Law. Please take time to read the following information carefully and discuss it with others if you wish. Ask us/me if there is anything that is not clear or if you would like more information. I would be grateful if you let me know within 2 weeks your decision whether you wish to participate in the research or not.

Thank you for thinking about taking part in my project!

The title of the research project:

Responses to cybercrime in Azerbaijan with special reference to the United Kingdom.

What is the purpose of the project?

The ultimate aim of this socio-legal research is to examine, assess and make suggestions to further enhancing the effectiveness, efficiency and legality of responses of the Republic of Azerbaijan to cybercrime. Investigating the growing problem of cybercrime, analysing the appropriateness of legal and policy responses of the country to cybercrime, bringing anti-cybercrime legislation and strategy into line with international standards and principles with reference to the UK's corresponding knowledge and experience can serve to achieve the purpose of this study.

Why have you been chosen? / What do you have to do?

You have been chosen for the interview because it is considered that you have the relevant expertise which can be benefitted for the purposes of this study. In pursuit of the fieldwork, 30 interviews will be conducted with the most relevant experts and personnel of both public and private sector institutions in Azerbaijan.

You will be asked only to take part in an individual interview - approximately one hour depending on the topic being discussed - at neutral, secure/safe venue convenient for you. You will be interviewed once, and it is not likely that follow-up interviews will be needed. Interview questions will enable open answers to be given in relation to the policy and legal responses of the Republic of Azerbaijan to cybercrime.

No expenses will be incurred by you (other than the time spent for the interview).

What are the possible benefits of taking part?

It is hoped that this work will give the participants the opportunity to share their knowledge and to take part indirectly in evaluating and making suggestions to further enhancing the capacity of the country in the fight against cybercrime. I would, therefore, be grateful if you share with me your ideas, opinions and experiences, which is also crucial to achieve the ultimate purpose of this study.

What are the possible disadvantages and risks of taking part? / What measures will be taken in order to protect the participants from potential negative repercussions?

This study has no significant personal risks to the participants of a physical, emotional or financial nature. In order to protect the participants from potential negative repercussions, the participants will be warned about the risks of their answers before proceeding further. Moreover, utmost care will be given to privacy, confidentiality and data protection issues. The information collected about the participant during the course of the research will be kept confidential. Inclusion of the information leading to identify the respondent will be avoided, and the final research outputs will not include any such information.

Audio recording devices will be used only with your consent during the interview. I will take notes regarding your answers if the audio recording device is not used. Notes taken/audio recordings will be transcribed within three days and sent to you for your consideration and further comments. After the transcription of the interview, notes/audio recordings of the interview will be destroyed. Anonymity of transcripts will also be ensured, by not including any personal data of the participant. The transcripts will be stored in separate secure files (protected with passwords) at the University of Leeds for a period of 2 years after the degree has been awarded, before being securely and irreversibly deleted from the devices on which they are stored.

It is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep (and be asked to sign a consent form)

and you can still withdraw at any time (up until two weeks passes from the interview as it will not be possible to withdraw responses once the results have been anonymized and analysis has begun). You do not have to give a reason for your decision to withdraw.

What will happen to the results of the research project?

The data collected during interviews will only be used for the purposes of this research and will not be disclosed to a third party. The collected data will be stored with the project's main documents in a secure location (and in a safe computer system) at the University of Leeds.

Contact for further information	**Principal investigator**	**Other members of the research team**	
Name	Mr Elvin Balajanov	Dr Subhajit Basu	Professor Clive Walker
Position	PhD student	Main supervisor	Co-supervisor
Department/ Faculty	School of Law / Education, Social Sciences and Law (ESSL)		
Work address	The Liberty Building, University of Leeds, Leeds, LS2 9JT, UK		
Phone number	+994 70 911 11 77 +44 77 801 27305	+44 113 343 5031	+44 113 343 5022
Email address	lw11eb@leeds.ac.uk	s.basu@leeds.ac.uk	c.p.walker@leeds.ac.uk

CONSENT FORM

Consent to take part in “Responses to cybercrime in Azerbaijan with special reference to the United Kingdom”	Add your initials next to the statement if you agree
I confirm that I have read and understand the information sheet/ letter explaining the above research project and I have had the opportunity to ask questions about the project.	
I understand that my participation is voluntary and that I am free to withdraw from the participation without giving any reason and without there being any negative consequences. In addition, should I not wish to answer any particular question or questions, I am free to decline. I also understand that I will be able to withdraw from the study during the first two weeks after the interview without giving any justification or explanation and without repercussion for me. Contact number of the researcher: +447780127305 UK; +994709111177 Azerbaijan.	
I understand that my responses will be kept strictly confidential and will be used only for the purposes of this study.	
I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in reports or other publications arising from the research.	
I understand that relevant sections of the data collected during the study, may be looked at in confidence by supervisors from the University of Leeds where it is relevant to my taking part in this research. I give permission for these individuals to have access to my records.	
I agree to take part in the above research project and will inform the lead researcher should my contact details change.	

Name of participant	
Participant’s signature	
Date	
Name of lead researcher	
Signature	
Date*	