

Occasional Paper

The Experience of Cybercrime in Georgia

Awareness, Victimisation and Reporting

Joseph Jarnecki,
Natia Seskuria and
Tatia Chikhladze

192 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, June 2023. ISSN 2397-0286 (Online).



British Embassy
Tbilisi

Royal United Services Institute

for Defence and Security Studies

Whitehall

London SW1A 2ET

United Kingdom

+44 (0)20 7747 2600

www.rusi.org

RUSI is a registered charity (No. 210639)



Contents

Acknowledgements	iii
Executive Summary	1
Introduction	3
Definitions and Terminology	4
Methodology	7
Limitations	9
I. Safety and Confidence	10
Awareness of Cybercrime	10
Knowledge of Cybercrime	16
II. Victimization: Threats and Harms	25
The State of Cybercrime	25
Common Threats Posed by Cybercrime	29
Group-Specific Cyber Vulnerabilities	31
III. Reporting	36
Mechanisms	36
Citizen Reporting	38
Lack of Effective Information-Sharing Systems	40
Trust	41
IV. Findings and Recommendations	44
Conclusion	51
About the Authors	53

Acknowledgements

This research has been commissioned as part of the UK–Georgia Cyber Partnership, a programme funded by the UK’s Conflict, Stability and Security Fund and delivered by the UK Embassy in Georgia to enable Georgia’s cyber ecosystem to be more resilient. The programme is implemented by the consortium of international and local partners in close collaboration with a broad range of Georgian government stakeholders, and supports the implementation of the Georgian National Cyber Security Strategy (NCSS) in three ways:

- Supporting the Information and Cybersecurity Department of Georgia's National Security Council to coordinate the delivery of the NCSS.
- Creating an information management framework to facilitate inter-departmental communication in order to allow faster and more effective responses to cyber incidents.
- Increasing awareness about cyber threats among the Georgian public and equipping them with adequate knowledge and means to protect themselves from the most common forms of attack.

The focus of this paper, on awareness, victimisation and reporting of cybercrime in Georgia, primarily falls on the latter area of activity.

The authors would like to thank Nana Tabagua and colleagues at the Policy and Management Consulting Group for their role in carrying out research activities. Additionally, we would like to thank Sneha Dawda for her contributions across the project.

Thanks also goes to the Ministry of Internal Affairs of Georgia (MIA) for providing an overview of cybercrime data for the years 2020–21. The authors would particularly like to thank the Crime Analysis Unit of the Analytics Division of the Department of Information and Analytics within the MIA for compiling this data.

Executive Summary

This paper establishes an independent evidence base on the experience and perception of cybercrime and online harms in Georgia, with a focus on how and why certain groups are more vulnerable. It aims to inform future policy development and societal understanding of the perception of cybercrime in Georgia, with a focus on awareness, victimisation and reporting. Through its analysis, the paper asserts that a disjuncture currently exists between Georgians' perceptions of what constitutes cybercrime and the provisions found in the Criminal Code of Georgia (CCG). In response to this assertion and additional findings, a series of cyber security capacity-building interventions are recommended to improve awareness, safety and confidence with regard to combating cybercrime.

The paper's findings are based on qualitative primary data-gathering – in-depth interviews with experts from the public, private and civil society sectors, focus group discussions with groups considered most vulnerable, and a consultative workshop – as well as quantitative data provided by Georgia's Ministry of Internal Affairs. The paper does not provide a sufficient evidence base to propose definite amendments to the CCG, and as such this precise consideration is out of its scope.

The paper examines Georgian citizens' sense of safety and security online, and their awareness of what constitute illegal activities in and through cyberspace. It finds that the general perception of cybercrime often conflates cyber-dependent and cyber-enabled crime and online harms and is largely ignorant of what activities the CCG explicitly considers to be cybercrime. It is important to note that the CCG considers cybercrime as solely cyber-dependent crime – i.e., offences carried out, by or against computers or other devices. There are no articles explicitly concerning cyber-enabled crimes or online harms, and prosecutors and victims instead rely on or interpret other existing provisions to demonstrate that an offence has been committed.

The paper also observes that levels of awareness of the threat of cybercrime are low, resulting in understandings of personal risk and risk mitigations being underdeveloped. While these problems are not unique to Georgia, this does not mean that the Georgian government cannot be ambitious in tackling the issue. Recent efforts, including reforms to cybercrime articles under the CCG and increased resourcing to the Cybercrime Division of the Central Criminal Police Department, have been important in addressing cyber-dependent crime, but ample room for improvement, particularly across cyber-enabled crime, remains.

This paper finds that while government is not widely trusted as a recipient of reporting about cyber incidents, it is considered a trustworthy messenger on the threat of cybercrime and cyber hygiene mitigations. The Georgian government should leverage this perception to target interventions at improving general cyber awareness and preparedness.

Increased whole-of-society efforts should be put into raising people's awareness, safety and confidence around cybercrime. A national information campaign is needed to increase baseline awareness, and within this, targeted initiatives focused on vulnerable and influential groups are key. Due to the varying levels of trust that the public affords to government, this campaign should cooperate where possible with civil society voices to achieve the greatest impact. The government should also make efforts to address the mismatch between governmental and popular understandings of what cybercrime is. These initiatives should be coupled with measures to incentivise reporting and strengthen the Georgian cyber security skills ecosystem.

Introduction

Georgia's National Cyber Security Strategy (NCSS) for 2021–24 identifies cybercrime as one of two main cyber-related threats facing the country, alongside state-linked hostile cyber operations.¹ As connectivity across Georgia has grown, the cyber-attack surface has expanded, creating more opportunities for perpetrators.² This has driven an increase in the costs to victims of cybercrime, with total losses for victims jumping 125% over 2020–21, from almost GEL 4 million (£1.3 million) to around GEL 8.9 million (£2.9 million). Moreover, due to the difficulty in tracking cybercrime and measuring impacts, this is likely an underestimation.³ Beyond financial cost, victims of cybercrime have experienced mental and emotional distress, disruption to use of and access to digital services, and public shaming, among other impacts.

Georgia's government has recently enacted legislative and organisational changes to tackle cybercrime. Among these are efforts to improve tracking and monitoring by the Central Criminal Police Department (CCPD), and changes made in 2021 to the Criminal Code of Georgia (CCG) to expand articles covering cybercrime. Following these and other efforts, official government statistics have recorded a 48% drop in reported cybercrimes between 2020 and 2021, and a 6% increase in solved cases.⁴ While improvements by government have likely had an impact, data gathered to inform this research casts doubt on its extent. Participants in the primary research conducted by RUSI and the Regional Institute of Security Studies consistently pointed to a growing threat from cybercrime and highlighted drivers preventing reporting, notably government's inadequate provision of awareness-building, trust and community outreach, or support to local law enforcement. These dynamics were more pronounced among groups on which this research focused and which it argues may be considered vulnerable to digital and cyber threats.⁵

-
1. Government of Georgia, 'Georgian National Cyber Security Strategy', 2021, pp. 11–13.
 2. Sneha Dawda, Joseph Jarnecki and Natia Seskuria, 'RUSI Literature Review: Georgia's Cyber Threat and Policy Landscape', RUSI and Regional Institute of Security Studies, April 2022 (not publicly available), pp. 26–32.
 3. For studies on cybercrime measurement, see Ross Anderson et al., 'Measuring the Cost of Cybercrime', in Rainer Böhme (ed.), *The Economics of Information Security and Privacy* (Berlin: Springer Berlin Heidelberg, 2013), pp. 265–300; Ross Anderson et al., 'Measuring the Changing Cost of Cybercrime', 18th Workshop on the Economics of information Security, Boston, MA, June 2019.
 4. Ministry of Internal Affairs (MIA), 'Overview of Cybercrimes Recorded in 2020–2021', Department of Information and Analytics, 1 September 2022 (not publicly available), p. 3.
 5. The research for this project focused on certain groups: women; ethnic minorities; children; older people; rural residents; journalists; and small to medium-sized enterprises (SMEs). Each has been found to be particularly vulnerable to aspects of cybercrime.

This paper considers the state of cybercrime in Georgia with a focus on the experience of vulnerable groups, addressing: how is cybercrime experienced in Georgia and what vulnerabilities exist across the population? To examine this question, the paper first provides a brief background on Georgian cybercrime, introducing key terms that will be used throughout the study, and explaining the paper's methodology. Chapter I will assess whether people feel safe and their level of confidence in staying secure from cybercrime, addressing the extent of awareness and understanding, and detailing some of the issues in current information provision. Chapter II provides an overview of the state of cybercrime and discusses areas where the law does not adequately consider cyber-enabled crime and online harms; it will also analyse the impacts of cybercrime both on individuals and on organisations. Chapter III will outline cybercrime reporting systems for individuals and organisations, and within government. It will also provide insights into how trust and other factors inhibit reporting. The final part of the paper will set out recommendations for how the Georgian government and other actors can continue to tackle cybercrime.

Definitions and Terminology

Cyber Hygiene

Cyber security best practices and steps which minimise users' risk of exposure to cyber threats fall under the term 'cyber hygiene'. All entities, whether organisations or individuals, can have good or bad cyber hygiene to a lesser or greater degree. For example, good organisational cyber hygiene includes regularly conducting data backups that are stored offline, requiring the use of multi-factor authentication and complex passwords, and regularly updating systems.

Cybercrime and Online Harms

Articles found in Section 9, Chapter 35 ('Cybercrime') of the CCG are listed in Table 1.

Table 1: Cybercrime Articles in the CCG

Article	Title
284	Unauthorised access to a computer system
285	Illegal use of computer data and/or computer systems
286	Interference with computer data and/or computer systems
286 ¹	Interference with computer data and/or computer systems for financial gain
286 ²	Creating fake official computer data

Source: CCG, Document 2287, 22 July 1999 (version 9 February 2023), <<https://matsne.gov.ge/en/document/view/16426?publication=247>>, accessed 18 May 2023.

These are all cyber-dependent crimes – in other words, offences carried out by or against computers or other devices. The CCG has no articles explicitly concerning cyber-enabled crimes, where cyber methods are used to carry out offences that are not cyber-dependent, or online harms, which are broader activities on or using the internet that have negative impacts, such as cyberbullying.⁶ Articles that are regularly invoked to cover cyber-enabled activities or online harms which pass the threshold of criminality are listed in Table 2.

6. For a discussion on online harms, see Ioannis Agrafiotis et al., 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate', *Journal of Cybersecurity* (Vol. 4, No. 1, 2018), pp. 1-15.

Table 2: Articles in the CCG for which Cyber is Regularly an Enabler

Article	Title
151 ¹	Stalking
157	Disclosure of information on private life or of personal data
157 ¹	Disclosure of secrets of personal life
158	Violation of the secrecy of private communication
159	Violation of secrecy of personal correspondence, phone conversations or other kinds of communication
189	Encroachment upon the rights of a holder of copyright or related rights and upon the rights of database manufacturers
210	Manufacturing, sale or use of forged credit cards or charge cards
255	Illegal making or sale of a pornographic work or other items
314	Espionage

Source: CCG, Document 2287, 22 July 1999 (version 9 February 2023).

This list is non-exhaustive and provides a snapshot of articles which relate most closely to how research participants described their understanding and experience of cybercrime – for example, non-consensual sharing or distribution of private images via social media draws on Article 255. It therefore also illustrates how the CCG makes allowance for cyber-enabled activities and online harms to be prosecuted if they are clearly linkable to existing articles, and that cybercrime, as it is perceived by Georgians, is not always covered by Section 9, Chapter 35 of the CCG.

Across primary data-gathering, this research has taken a non-prescriptive approach to engaging with research participants in order to uncover intuitive understandings of cybercrime. As such, researchers did not give participants set definitions of cybercrime and instead allowed participants to express what they understood as cybercrime. Therefore, the report engages with an understanding of cybercrime that is in line with Georgians’ perceptions – one which includes cyber-dependent and cyber-enabled crime as well as online harms. This approach means that foundational to the report are understandings that:

1. The risks that Georgians associate with feeling unsafe or insecure online are not always covered by CCG cybercrime articles.
2. Citizens are often not aware of what constitutes illegal activity online, or the tools and processes available to them to seek support.
3. Citizens rarely, if ever, differentiate between cyber-dependent and cyber-enabled crime and online harms.

An indicative illustration of the differences between citizen understandings of cybercrime and offences included under the CCG are in Table 3.

Table 3: Perceptions and Provisions of Cybercrime: Examples

Activity	Citizens understand as cybercrime	CCG understands as cybercrime
Cyberbullying	X	
Cyberstalking	X	
Non-consensual sharing of private images	X	
Ransomware attacks	X	X
Distributed denial-of-service attack	X	X
Wiperware attack	X	X
Identity theft and extortion	X	

Source: Author generated.

Methodology

Research for this paper was carried out between June 2022 and January 2023 as part of the UK–Georgia Cyber Partnership programme funded by the UK Foreign, Commonwealth & Development Office. It consisted of a mix of primary and secondary qualitative methods, as detailed below.

Semi-Structured Interviews

The research team conducted 11 semi-structured interviews with current or former members of the Georgian government, experts on cyber security and cybercrime, representatives of civil society, journalists and senior members of the private sector. Participants were selected through a purposive sampling strategy among key communities of practice and based on their first-hand experience with cybercrime in Georgia from a governance or civil society perspective. Most interviewees were identified via pre-existing institutional relationships, although a number were identified during the production of the literature review or through a snowballing sampling strategy. Most interviews were conducted in person and in English in Tbilisi. Where this was not possible, interviews took place via video conference and, in one instance, in Georgian. The semi-structured interview format allowed the research team to maintain a broadly consistent line of questioning while leaving space to have spontaneous

in-depth discussions on participants' areas of expertise. Interviews took place between September 2022 and January 2023.

Focus Groups

The research team organised focus group discussions (FGDs) with a total of 41 participants across four groups. Participants were selected based on predetermined identifiers which were expected to increase vulnerability to cybercrime. These 'vulnerable groups', each of which had its own dedicated FGD, included: journalists; parents, guardians⁷ and teachers; ethnic minorities; and women. Other groups, such as children, were also considered more likely to be vulnerable, but for practical reasons the number of FGDs was limited. As part of the FGDs, participant responses were captured on response sheets; additionally, audio recordings were taken from sessions and then transcribed. Participants were selected with a view to ensuring strong engagement from women and representing geographical diversity – as such, 28 of the 41 participants were women and 21 were not urban residents. The FGDs were conducted in Tbilisi, in Georgian, between 3 and 7 October 2022.

Consultative/Data-Verification Workshop

To test and verify the findings from the interviews and FGDs, the research team held a community engagement workshop in Tbilisi, with 49 participants. This was conducted in Georgian and included journalists, civil society organisations (CSOs), parents, and small to medium-sized enterprise (SME) owners and operators, separated into breakout groups according to these stakeholder categories. The session was recorded, and transcripts were generated to analyse the discussions. The workshop was held on 22 December 2022.

Literature Review

The research team conducted a targeted literature review of open source data and research on cybercrime in Georgia. This was informed by a previous systematic literature review, undertaken by project researchers, which contributed to earlier research on the Georgian cyber security ecosystem. In addition, the Department of Information and Analytics of the Georgian Ministry of Internal

7. Across this project, guardians and carers are defined as adults with a regular duty of care for a child of whom they are not the parent. This includes adoptive and foster parents, grandparents and other relatives or other individuals who hold responsibility.

Affairs (MIA) provided in-depth and disaggregated cybercrime statistics for 2020–21.

Across primary data-gathering, participants have been anonymised to protect their identities.

Limitations

One limitation of this research is that the primary data-gathering activities constitute an indicative but not representative sample. While the number of participants is sufficient to accurately test ideas and generate novel findings, it is not sufficient to provide a fully representative reflection of Georgian citizens' sentiments. To mitigate this limitation, FGD participants were selected to ensure that diverse backgrounds were represented and that individuals with a society-wide range of expertise were consulted. Another limitation is that because of the research's focus on the experience and perception of cybercrime, specific regulatory and legislative changes aimed at addressing these perceptions are largely beyond the scope of this paper. Nonetheless, regulatory and legislative measures to address and improve cyber security in Georgia are important and represent key areas of future research.

I. Safety and Confidence

Cybercrime is a relatively novel and rapidly evolving threat. It creates significant anxiety, with all FGD participants reporting that they were ‘worried about being a victim of cybercrime’. Nonetheless, awareness of its scope, impacts and mitigations is underdeveloped. This is a problem internationally, although it is exacerbated in countries like Georgia which have seen rapid digitisation without highly successful large-scale public information campaigns.⁸ This chapter assesses current awareness and understanding of cybercrime in Georgia and proposes how gaps could be filled.

Because this chapter focuses on participants’ experience of safety and confidence, most data referenced is based on a broad conception of cybercrime, which includes cyber-dependent and cyber-enabled crime, in addition to online harms.

Awareness of Cybercrime

Priority Areas

Cybercrime awareness relates to how much is understood about criminal threats faced from or through cyber means. It directly informs the feeling of safety and actors’ motivation to mitigate against cyber security risks and is a priority development area under the NCSS.⁹ All stakeholders have a level of cybercrime awareness, including enterprises, individuals, CSOs and so on.

Research conducted for this paper found that cybercrime and cyber security awareness in Georgia remains low but has improved over recent years. Amendments to the CCG and the expansion of the CCPD’s Cyber Crime Division have helped to raise the profile of cybercrime in Georgia.¹⁰ Moreover, increased connectivity and high-profile cyber attacks on government services and individuals’ private data have brought the threat of cybercrime more into the spotlight.¹¹

-
8. While ‘large-scale awareness campaigns’ are said to have taken place under the NCSS and its Action Plan, no research participants, apart from one government official, could recall such a campaign.
 9. Government of Georgia, ‘Georgian National Cyber Security Strategy’, pp. 8–9.
 10. CCG, Document 2287, 22 July 1999 (version 9 February 2023), Section 9, Chapter 35, ‘Cybercrime’.
 11. Government of Georgia, ‘Georgian National Cyber Security Strategy’, pp. 12–13; Irakli Jgarkava, ‘Georgia’s Cybersecurity Policy: Challenges and Opportunities’, Georgian Center for Strategy and Development, 2021.

Nonetheless, poor awareness remains a general problem. Primary data-gathering for this project highlighted that the groups with the lowest awareness are rural residents, children, older people, and non-Georgian-speaking ethnic minorities.¹²

- **Rural residents.** Low awareness in less urbanised regions, and particularly those with difficult terrain, is driven by relatively poor connectivity, less access to state support, and higher-than-average rates of deprivation.¹³ One FGD participant, who is an IT administrator in a rural school, explained that most residents of her village ask her for help with online activities such as setting or changing passwords, including for online banking. Although she tries to teach them, ‘they do not want to develop these skills, because they do not understand how many risks it contains ... to transfer personal information to anyone else’.
- **Children.** Data gathered from parents, teachers and guardians, as well as experts, showed that children lack basic awareness of cybercrime. However, children do show interest and some knowledge in areas perceived as ‘exciting’, such as hacking.¹⁴ Poor awareness among children is driven by an underestimation of their own risk, assuming everything online is trustworthy, misunderstanding private data protection, and receiving insufficient support from schools and parents.¹⁵
- **Older people.** Based on data from the National Statistics Office of Georgia (Geostat), older Georgians (60+ years) have both a lower-than-average internet use and less varied use cases (see Figure 1). This is supported by FGD and interview data gathered throughout the project which highlights that lower awareness is driven by this low use of technology, as well as a higher likelihood of trusting online information, digital illiteracy, and a gap in provision of CSO and government support.¹⁶ One interviewee, a former senior government employee, stated that older people do not use the internet (or use it to a statistically irrelevant extent) and are therefore almost immune to cybercrime.¹⁷ This is a dangerous assumption that betrays a misunderstanding of cybercriminal rationales by expecting victimisation to correspond with frequency

12. Interviews with former senior members of government and CSO leads, Tbilisi and video conference, 3–18 October 2023.

13. National Statistics Office of Georgia (Geostat), ‘Information and Communication Technologies Usage in Households’, <<https://www.geostat.ge/en/modules/categories/106/information-and-communication-technologies-usage-in-households>>, accessed 20 April 2022; interview with current government official, Tbilisi, 4 October 2022; interview with former senior government official, video conference, 18 October 2022.

14. Interview with senior CSO member, Tbilisi, 6 October 2022.

15. FGDs, Tbilisi, 3–7 October 2022; interview with former senior member of government, video conference, 7 October 2022.

16. FGDs, Tbilisi, 3–7 October 2022; interviews with senior members of CSOs and professional associations, Tbilisi, 3–6 October 2022.

17. Interview with former senior government official, Tbilisi, 5 October 2022.

of use, and it risks isolating older people from digital services and cybercrime support.

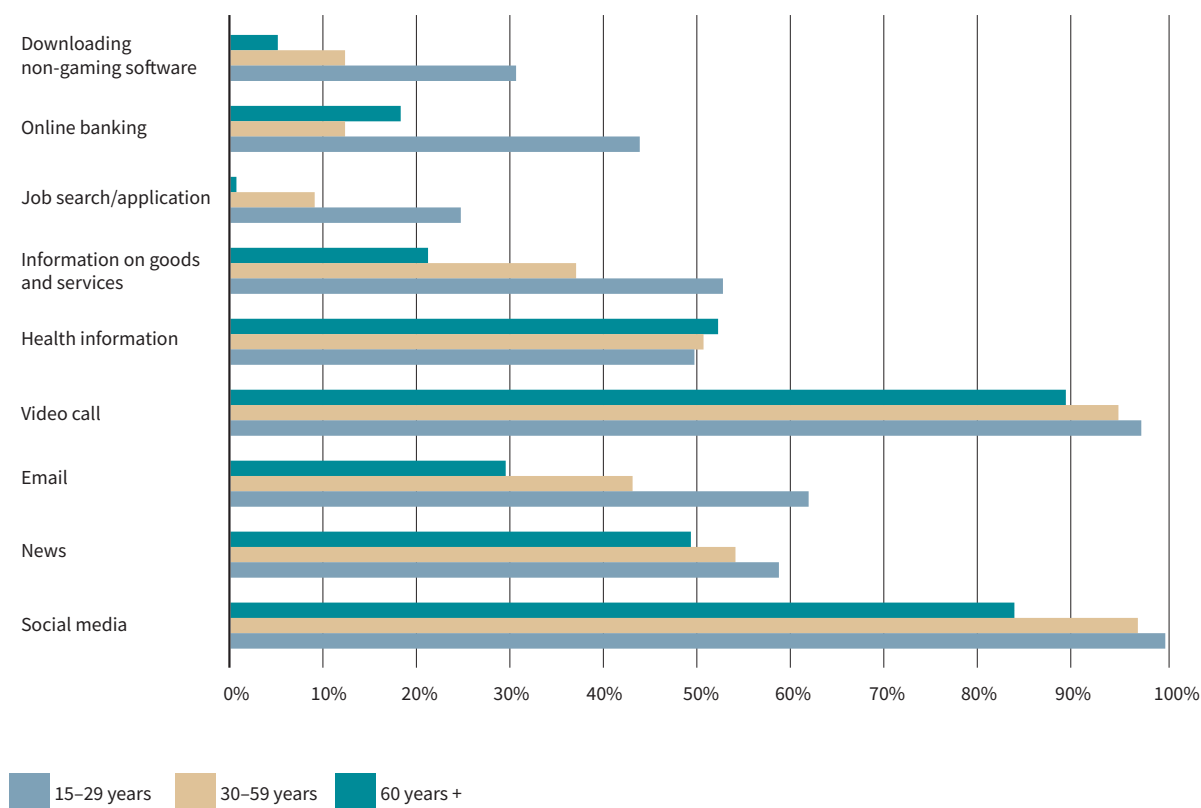
- **Non-Georgian-speaking ethnic minorities.** The primary driver for low awareness among non-Georgian-speaking ethnic minorities is that resources and information available in Georgian are not accessible.¹⁸ Consequently, these groups rely on sources in their first language or, as is more common, they use Russian-language resources. Russian remains a common second language across ethnic minority groups in Georgia.¹⁹ As one former government interviewee emphasised, Russian-language sources are more likely to be leveraged for disinformation and misinformation and as such can create issues in building awareness and present national security risks.²⁰ It is important to nuance this argument, however, as there is insufficient evidence to support it conclusively.

18. FGDs, Tbilisi, 3–7 October 2022; interview with journalist, Tbilisi, 3 October 2022; interview with former senior government official, video conference, 7 October 2022.

19. Rusudan Amirejibi and Kakha Gabunia, 'Georgia's Minorities: Breaking Down Barriers to Integration', Carnegie Europe, 9 June 2021; Tamar Maisuradze, 'Russian Language in Georgia: Not Number One', *JAM News*, 21 December 2016, <<https://jam-news.net/russian-language-in-georgia-not-number-one/>>, accessed 7 February 2023.

20. Interview with former senior government official, video conference, 7 October 2022.

Figure 1: Purposes of Internet Use by Age, July 2021



Source: Geostat, ‘Information and Communication Technologies Usage in Households’, <<https://www.geostat.ge/en/modules/categories/106/information-and-communication-technologies-usage-in-households>>, accessed 20 April 2022.

People within these more vulnerable groups are not limited to one identifier. Identity is multi-faceted, and several vulnerable characteristics can be held simultaneously, with primary data-gathering across the project indicating that this intersectionality often creates a greater likelihood of poor cyber awareness. So, an older person who is a rural resident and does not speak fluent Georgian carries a more substantial risk of poor cybercrime awareness.

Primary data-gathering also found that while instances of low cyber awareness among senior government officials, journalists, police, and SME owners and operators are uncommon, they can have wider societal impacts.

- **Senior government officials.** While senior government managers and ministers were not criticised at length for low awareness of cybercrime, there was a general sentiment among research participants that their decisions led cybercrime to be under-prioritised.²¹ One interviewee, with senior government

21. FGDs, Tbilisi, 3–7 October 2022; interview with former senior government official, video conference, 7 October 2022.

experience, argued that this was due to a specific lack of awareness of the cross-governmental challenge posed by cybercrime. This interviewee suggested running ministerial-level cyber exercises to build cross-governmental understanding and capabilities.²²

- **Journalists.** Journalists who participated in interviews and FGDs stated that their own awareness was lower than it should be, and that media does not sufficiently cover cybercrime.²³ One journalist who participated in an FGD also highlighted that media organisations do not provide training in cyber hygiene or threats. This, they argued, leads to insufficient analysis of, and attention to, cybercrime. Both expert and non-expert research participants across FGDs, interviews and the verification workshop stated that media reporting on cybercrime is not detailed enough.²⁴
- **Police.** People regularly go directly to the police to report cybercrime. An interviewee within government highlighted that police have received extensive training to build awareness and support victims when they report.²⁵ However, no former government officials or FGD participants pointed to an increased capability to facilitate reporting by police at any stage, and CSO interviewees highlighted this as an area particularly in need of improvement.²⁶ Indeed, many research participants highlighted issues and concerns with reporting to the police (see ‘Reporting Processes’).
- **SME owners and operators.** Globally, cyber-dependent criminal activity is predominantly financially motivated. While there is a lack of wider data to fully justify this assertion in Georgia, recorded cybercrime incidents do support this conclusion (see Chapter II). Businesses are key targets of cybercrime, and where owners and operators, particularly of SMEs, have low awareness of the threat of cybercrime, they are put at greater risk.²⁷ This carries a concurrent individual threat to their livelihoods but also, if pervasive, to national economic security.

A lack of awareness among the above groups can have a negative impact on how well society understands the risk of cybercrime, reducing national preparedness to tackle the threat, as people and organisations fail to take proper precautions. Consequently, these influential groups should be considered a high priority for awareness campaigns.

22. Interview with former senior government official, video conference, 7 October 2022.

23. FGDs, Tbilisi, 3–7 October 2022; interview with journalist, Tbilisi, 3 October 2022.

24. *Ibid.*; interview with member of CSO, video conference, 20 October 2022.

25. Interview with senior government official, Tbilisi, 4 October 2022.

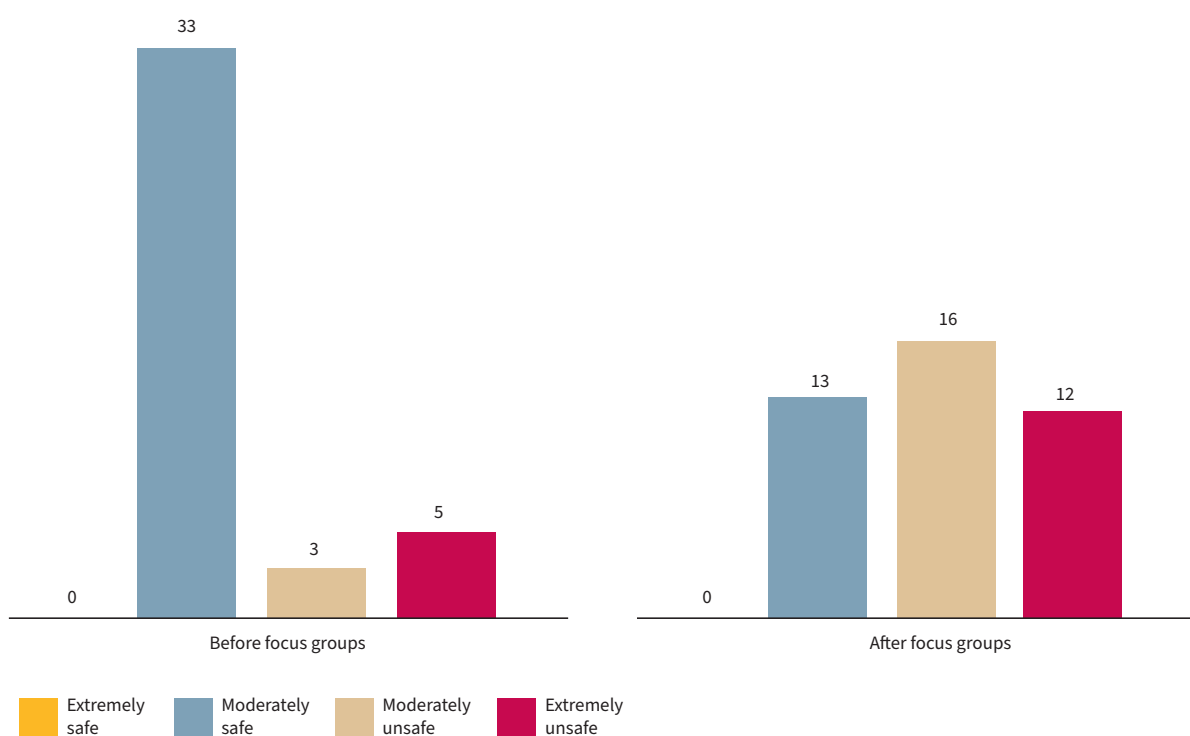
26. Interviews with members of CSOs, Tbilisi, 3–4 October 2022.

27. Interview with senior government official, Tbilisi, 4 October 2022; interview with former senior member of government, video conference, 18 October 2022.

Feelings of Safety and Confidence

When asked to rate their feelings of safety when using the internet and digital services, 33 of the 41 participants at the beginning of the FGDs said they felt moderately safe, while eight felt either moderately or extremely unsafe. Following the FGDs this shifted, with 28 reporting that they felt either moderately or extremely unsafe (see Figure 2).

Figure 2: Feelings of Safety, Focus Group Data



Source: Author generated from FGD data.

FGDs included participants sharing their experiences of what they perceive as cybercrime and providing real-life examples and details. As outlined above, participants were not given a prescriptive definition of cybercrime to orient their engagement with the FGDs, instead, researchers provided light-touch guidance to keep discussions on topic, and participants independently focused on cyber-dependent and cyber-enabled crime as well as online harms. The fact that 20 of the participants left feeling less safe than before (see Figure 2) indicates that they had low awareness of the threat picture coming into the FGDs. This is supported by comments made by attendees. For example, one participant who is also a journalist remarked that they were more worried afterwards because ‘perhaps I don’t fully understand how much damage cyber-criminals can cause’.²⁸

28. Journalists’ FGD, Tbilisi, 6 October 2022.

Moreover, all expert interviewees consistently mentioned that Georgians underestimate the threat from cybercrime.

Feelings of safety are not homogeneous. In advance of the FGDs, women reported feeling much safer than men, with 25 women feeling moderately or extremely safe compared with eight men.²⁹ However, after the FGDs this figure was lower for both men and women, with 17 women and three men lowering their feeling of safety to either moderately unsafe or extremely unsafe. Meanwhile, in a women-only focus group, nine of the 12 participants responded that they thought they were more likely to be victimised than men.³⁰ This data may indicate that women feel more threatened by cybercrime in Georgia, as discussed below. Moreover, it may indicate that some of this sentiment comes from a lack of cyber awareness, although further research is needed to support this assertion.

Knowledge of Cybercrime

Cyber Hygiene

As noted earlier, cyber security best practices that minimise the risk of exposure to cyber threats fall under the term ‘cyber hygiene’. For example, an organisation practices good cyber hygiene if it backs up its data, requires the use of multi-factor authentication and complex passwords, and regularly updates its systems. Improving cyber hygiene is an important step to creating a more resilient national cyber ecosystem. The conventional argument is that as more individuals and organisations begin to practise good cyber hygiene, fewer of them are likely to be victimised by cyber-criminals.

Although cyber hygiene is an important mechanism for improving general cyber resilience, it is important to note that it is only one area of activity in this regard. Other measures to secure products and services by design, thereby removing cyber security risk or decision-making from the end user and reducing reliance on individual choices, have also been developed internationally.³¹ Nonetheless,

29. The total number of 41 FGD participants was divided into 28 women and 13 men. These were split between FGDs dedicated to ethnic minorities (9); women (12); journalists (10); and parents, guardians and teachers (10).

30. Women’s FGD, Tbilisi, 4 October 2022.

31. See, for example, the UK National Cyber Security Centre’s (NCSC) Active Cyber Defence programme, in NCSC, ‘NCSC Annual Review 2022’, 1 November 2022, p. 17, <<https://www.ncsc.gov.uk/collection/annual-review-2022/resilience/active-cyber-defence>>, accessed 5 May 2023. See also the recently published US National Cybersecurity Strategy, which has been credited with taking a novel approach to national cyber security risk management, The White House, ‘National Cybersecurity Strategy’, March 2023, <<https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>>, accessed 5 May 2023.

improving cyber hygiene remains an important step to strengthening national cyber resilience.

Cyber hygiene tends to have a positive correlation with cyber awareness; as such, low levels of awareness result in similarly poor cyber hygiene. Most expert interviewees argued that this is a decisive factor in the success or failure of cybercrime activities, with one stating that it is ‘the main problem across society driving cybercrime’.³² Equally, FGD attendees frequently referenced uncertainty around ‘what they were meant to do’ in certain situations where they were victimised by cybercrime, including issues like the preservation of cyber evidence. Research found that cyber hygiene concerns fall into three areas for Georgians: behaviours, tools and trusted sources.

Behaviours

Cyber hygiene informs the way people prepare for and react to cyber threats. Good behaviours include questioning untrustworthy links and not sharing private data. Research indicated that bad behaviours, particularly sharing private information such as passwords, not taking proactive security measures, such as using multi-factor authentication, and uncritically trusting online information, are common in Georgia. An expert interviewee described cultural attitudes to proactive cyber security as poor, arguing that people ‘only start caring about it when ... [their] account gets hacked’.³³ Similarly, among representatives from SMEs at the verification workshop, participants whose businesses had not invested in cyber security explained that this was because they had not faced major attacks and so did not think the cost was merited.

Among non-expert research participants, many explained that people are not sufficiently conscious of privacy considerations, and pointed to examples of people sharing password details or of they themselves doing so. One FGD participant, however, highlighted instances of women they know living in rural areas who are compelled by their partners to share this information, so that their partners ‘have control over their online activities’.³⁴ For any cyber awareness campaign, cyber hygiene behaviours should not be over-simplified, and individuals must not be shamed for a lack of best practice.

32. Interview with head of CSO, Tbilisi, 3 October 2022; interview with member of CSO, Tbilisi, 3 October 2022; interview with member of women’s CSO, video conference, 20 October 2022; interview with senior government official, Tbilisi, 4 October 2022.

33. Interview with journalist, Tbilisi, 3 October 2022.

34. Women’s FGD, Tbilisi, 4 October 2022.

Tools

Use and understanding of everyday cyber hygiene tools among individuals is poor. In the FGDs, when participants were presented with a list of cyber hygiene measures to prioritise by efficacy, all participants required explanations for at least one measure, and in most sessions, researchers needed to walk the group collectively through each measure.³⁵ It is notable also that the distribution across what participants selected as more or less efficient measures was relatively regular, indicating that there was little consensus around what represented a particularly strong or weak security measure.³⁶ As none of the measures put forward were inherently bad, this does not necessarily reflect that people's average cyber hygiene is low, but it does highlight that participants did not have a reference point for a key cyber security concept. This aligns with FGD participants' explanation that they had encountered little communication about cyber hygiene best practices previously and is supported by arguments made by expert interviewees that low levels of awareness and confidence in using basic tools, such as password managers, are pervasive.³⁷

Organisations also struggle with prioritising cyber security measures. For example, one journalist from the FGDs highlighted that their employer, a media company, does not provide or recommend specific cyber security tools for its employees, and nor does it conduct any cyber hygiene or awareness trainings despite the specific cyber risk experienced by journalists (see 'Common Threats Posed by Cybercrime'). Other FGD participants broadly supported this point, arguing that their organisations under-invest in or under-prioritise cyber security; similarly, expert interviewees consistently mentioned this as an endemic issue and emphasised that organisations have a responsibility to do more.








In contrast to this view, some SME representatives at the verification workshop noted that their companies have recently increased expenditure on cyber security to around 5–10% of gross income. This spending has funded technical measures, including training and 24/7 IT response capabilities, as well as non-technical provisions such as ad hoc threat communication and non-disclosure agreements. Nonetheless, while these initiatives are encouraging, primary data-gathering conducted for this paper indicates that they remain uncommon.

-
35. Cyber hygiene measures listed were: different passwords for every account; password manager; multi-factor authentication; checking the sender's email address; avoiding sharing passwords or personally identifiable information online; using end-to-end encrypted communications; using antivirus software; updating software/devices automatically; and changing router name and password.
 36. Measures that did not have a regular distribution – where there was a larger-than-average share of participants thinking that a measure was particularly effective or ineffective – were 'different passwords for every account' and 'multi-factor authentication', which were considered effective, and 'update software/devices automatically' and 'change router name/password', which were considered ineffective.
 37. Interview with senior member of CSO, Tbilisi, 6 October 2022; interview with former senior member of government, video conference, 18 October 2022.

Trusted Sources

When asked ‘Which source of information on cyber hygiene would you be most likely to trust?’, FGD participants indicated government information campaigns (49%), law enforcement agency (LEA) websites (41%) and news/media (41%) as the most trustworthy sources (see Figure 3).³⁸ In contrast to low levels of trust when reporting cybercrime (see the section below on ‘Citizen Reporting’), participants believed government to be a trustworthy source on cyber hygiene, because they considered that its priorities aligned with their own. Participants consistently expressed that government would not want them to be victimised, as it presents a cost and security risk, and therefore would provide the best information possible. This sentiment carried across to law enforcement websites. Participants’ selection of news/media was often because people believed it to be a good source for information generally, though several FGD attendees complained about the lack of coverage of cybercrime issues.

Figure 3: Cyber Hygiene Information Sources

	Government information campaigns	49%	0%
	LEA websites	41%	2%
	News/media	41%	20%
	Social media	37%	49%
	Government websites	37%	0%
	Friends or family	24%	54%
	NGOs	22%	27%

Source: Author generated from FGD data.

38. Percentages as a number of FGD participants: 49%=20; 41%=17.

In contrast to what sources people think they can trust, FGD participants responding to the question ‘Where do you get information on cyber hygiene from?’ most often selected friends and family (54%) and social media (49%).³⁹ While neither are necessarily problematic, generally low levels of cyber awareness are likely to mean that personal networks also do not have a strong knowledge of cyber hygiene. Moreover, the danger associated with social media as a lever for spreading misinformation and disinformation was mentioned several times by expert interviewees.⁴⁰ This is not to say that all aspects of social media are negative – for example, one female FGD participant highlighted Facebook groups where women provide support to encourage reporting of online harms caused by ex-partners.⁴¹

Although it was not a listed option, 11 FGD participants highlighted NGOs as one of their sources of cyber hygiene information. Across focus groups this finding was selected by six out of nine ethnic minorities’ FGD participants, four out of 10 journalists’ FGD participants and one out of 12 women’s FGD participants. No parents, guardians or teachers raised NGOs as a source of information. From follow-on discussions, participants explained this skew through two factors. First, on the supply side, ethnic minority FGD participants emphasised that there are substantial amounts of cyber hygiene information that they can access from NGOs, with one interviewee providing context for this by outlining NGOs’ focus on ethnic minorities and journalists, as they are considered to be at higher risk.⁴² Second, on the demand side, journalists and ethnic minorities say they are less likely to trust government support in contrast to support from NGOs (see ‘Citizen Reporting’).

Professional and Educational Ecosystem

Research conducted for this paper found that the professional and educational ecosystem focused on cybercrime and cyber security in Georgia lacks capacity. As a result, there are a limited number of skilled and qualified experts who have professional-level cyber awareness. This situation, however, is evolving rapidly following Russia’s invasion of Ukraine, as many Russian cyber professionals are emigrating to Georgia – it remains to be seen, though, whether émigrés are working in Georgian companies or contributing to national cyber security.⁴³

39. Percentages as a number of FGD participants: 54%=22; 49%=20. Some participants may have selected both ‘friends and family’ and ‘social media’.

40. Interview with journalist, Tbilisi, 3 October 2022; interview with head of CSO, 3 October 2022; interview with member of CSO, Tbilisi, 3 October 2022.

41. Women’s FGD, Tbilisi, 4 October 2022.

42. Interview with journalist, Tbilisi, 3 October 2022.

43. *The Bell*, ‘Russia’s IT Exodus and the Kremlin’s Futile Efforts to Reverse It’, 24 January 2023, <<https://en.thebell.io/russia-s-it-exodus-and-the-kremlin-s-futile-efforts-to-reverse-it/>>, accessed 25 April 2023.

Although most countries are facing similar challenges across cyber professional and educational development, there are key areas that Georgia can target to help scale up its capabilities at pace.

Education

Multiple expert interviewees expressed frustration at the lack of university-level cyber security courses in Georgia.⁴⁴ Two interviewees noted, for example, that there is only a single undergraduate cyber security degree in Georgia, run jointly between Caucasus University and New Jersey University.⁴⁵ One said, however, that the more pressing issue is the small quantity of Georgia-based postgraduate education. He argued that having few Master's-level courses creates a 'bottleneck' of skilled individuals in the country.⁴⁶ A clear mitigation, the same interviewee suggested, would be to launch more of these programmes or provide comparable courses at the National Defence Academy to build internal government cyber skills development capacity.⁴⁷

Across data-gathering, interviewees and FGD participants highlighted the broader education system as an important mechanism for advancing positive cybercrime safety and confidence outcomes. Moreover, many stressed that it is currently under-used. Impacts which participants argued could be achieved through better leveraging of the education system include:

- **Mainstreaming cyber awareness and hygiene among students.**⁴⁸ Including cyber issues on the curriculum or in special sessions for students would support a group which this report has found to be uniquely at risk from cybercrime and online harms (see 'Common Threats Posed by Cybercrime'). It would also provide an understanding to children and young people of how they should report to law enforcement (see Chapter III).
- **Building trust-based cooperation between parents/guardians and children on cyber security.**⁴⁹ Schools can provide or host mediated sessions so that parents/guardians and children can jointly improve their understanding of cybercrime threats and mitigations. This will improve awareness generally

44. Interview with senior CSO member, Tbilisi, 6 October 2022; interview with former government adviser, Tbilisi, 4 October 2022; interview with senior member of CSO, Tbilisi, 4 October 2022.

45. Interview with former government adviser, Tbilisi, 4 October 2022 ; interview with senior CSO member, Tbilisi, 6 October 2022.

46. Interview with former government adviser, Tbilisi, 4 October 2022.

47. *Ibid.*

48. *Ibid.*; interview with former senior member of government, video conference, 7 October 2022; interview with former government adviser, Tbilisi, 4 October 2022.

49. Interview with senior member of CSO, Tbilisi, 3 October 2022; interview with head of CSO, Tbilisi, 6 October 2022.

but will also help to offset parents'/guardians' concerns that if they implement cyber security measures, their children will see it as a sign of distrust.⁵⁰

- **Awareness multiplier effect.**⁵¹ Schools are important community hubs, particularly in rural areas.⁵² Hosting external awareness-raising activities within schools will likely attract other members of the community, increasing the impact of interventions. Moreover, several interviewees pointed out that as schools intersect with many different social networks, there would be a multiplying effect from interventions.

Certifications and Qualifications

Interviewees, especially those with technical or private sector backgrounds, highlighted a gap in certification and qualification pathways for cyber security professionals.⁵³ This is partly a problem of private sector investment, though it may also be due to risk-averse cyber capacity-building interventions by partner countries. One participant stated that many cyber capacity-building initiatives take a risk-averse approach to funding certifications/qualifications and are reluctant to support schemes with high average failure rates or on sensitive topics, such as penetration testing. This results in a significant supply shortage in key areas and limits overall national capacity.⁵⁴ Certification and qualification schemes could also be used as an incentive to support public sector retention. Multiple interviewees with experience in government argued that if the technical training offer is improved, government will retain people in technical roles for longer.⁵⁵ This aligns with Task 3.2 of the NCSS, which is to strengthen national cyber capabilities across key government agencies.⁵⁶

Georgia is not unique in requiring additional capacities to support its national cyber capabilities and awareness. Most if not all countries are struggling on this issue. Compared with global leaders such as the US and China, Georgia is behind. Although one expert interviewee argued that Georgia is in a strong position within its region, this assertion requires further research.⁵⁷

50. Verification workshop, Tbilisi, 22 December 2022.

51. *Ibid.*; interview with senior government official, Tbilisi, 4 October 2022; interview with former senior government official, video conference, 7 October 2022.

52. Interview with senior government official, Tbilisi, 4 October 2022.

53. Interview with head of CSO, Tbilisi, 6 October 2022; interview with former government adviser, Tbilisi, 4 October 2022.

54. Interview with head of CSO, Tbilisi, 6 October 2022.

55. *Ibid.*; interview with former senior member of government, video conference, 18 October 2022.

56. Government of Georgia, 'Georgian National Cyber Security Strategy', p. 20.

57. Interview with former senior government official, Tbilisi, 5 October 2022.

Guidelines for Cybercrime Awareness-Raising Campaigns

Across primary data-gathering, most participants emphasised the need for further cybercrime awareness-raising interventions. The following points detail common recommendations from these participants about how such interventions should be structured. These directly inform the recommendations in Chapter IV.

- **Easily understandable content.** Participants consistently emphasised that content should be accessible and structured as clear, short and memorable messages targeting specific issues, such as the nature of threats, password hygiene or privacy rights. Campaigns should forefront practical examples, demonstrations and stories as the most impactful, with one academic interviewee emphasising that ‘real stories alongside expertise are crucial for communication’. Types of communication should be intuitive to understand; for example, using visualisations and video publications is important. Diverse language options should also be available to ensure accessibility for non-Georgian-speaking minorities.
- **Audience-centric communications.** Campaigns should be audience-centric. Although there are overarching messages, some information is better suited to specific groups. One participant in the verification workshop illustrated this point by arguing that it is ineffective, for instance, to speak about licensed software with a segment of the population that is close to the poverty line. An expert interviewee who works in a women’s group also strongly advocated for this point, outlining the importance of awareness-raising around privacy issues for women and girls, who are disproportionately targeted by online harms, such as threats to leak personal images.
- **Activities focused on high-vulnerability and high-impact groups.** Certain groups are more vulnerable to cybercrime or play a key role in its prevention or mitigation (see the above section on ‘Priority Areas’). Awareness-building interventions should make extra provision for these groups – for example, additional support should be targeted on rural non-Georgian-speaking populations. Target group selection should be sensitive to average levels of cybercrime awareness, and messages which are most likely to improve people’s lives should be prioritised, such as secure SME digitisation.

- Cross-government coordination.** Under the NCSS, the Digital Governance Agency is the principal agency responsible for awareness-raising, with the MIA taking the lead on cybercrime issues. Both therefore have equity in messaging about cybercrime threats and cyber hygiene. Interviewees emphasised that to achieve the most impactful cybercrime awareness campaigns, both agencies should collaborate closely and coordinate with other parts of government. Other parts of the public sector most frequently mentioned as important to a successful campaign were the National Bank of Georgia and the Ministry of Education, Science, Culture and Sport.
- Leverage diverse platforms.** Almost all FGD participants and interviewees who spoke about cybercrime awareness campaigns stressed the need to use multiple platforms, not just social media, for communication. While there is significant scope to leverage online platforms, traditional media is still widely used, particularly among more vulnerable groups such as older people. Without platform diversity, awareness-raising efforts risk being unable to access key constituencies.
- Whole-of-society planning and delivery.** Awareness-building campaigns should be multi-stakeholder and should thus include actors from across the public and private sector, NGOs, CSOs, media and international partners. Private gambling companies, for instance, have a key role given the high incidence of illicit online bank transfers due to compromised online gambling accounts (see section below on ‘Common Threats Posed by Cybercrime’). Commercial banks also have unique opportunities to spread awareness, with one ex-government interviewee raising the example of a ‘What is Phishing?’ guide on one online banking login portal. Finally, another ex-government interviewee highlighted the high rate of phishing attacks on accountants in 2021 and recommended that professional associations be supported to improve awareness within their field.

II. Victimization: Threats and Harms

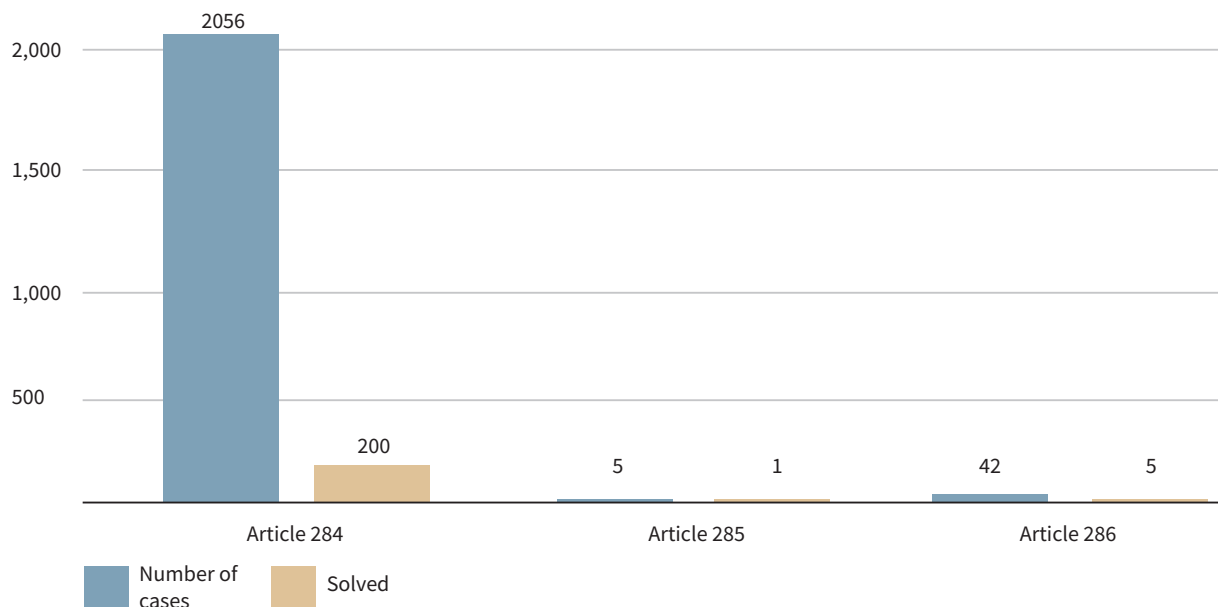
This chapter analyses the state of cybercrime victimisation in Georgia. It references data from across the semi-structured interviews, FGDs and verification workshop, as well as statistical data provided by the MIA, to assess the tools and tactics employed by cyber-criminals to target victims. The first section examines MIA reporting on the state of cybercrime and compares it with primary data generated from this project. The second and third sub-sections outline cybercrime vulnerabilities with a specific focus on groups found to be more vulnerable, namely women, children, journalists, ethnic minorities and SMEs.

The State of Cybercrime

According to MIA data, there were 3,257 recorded cybercrimes in Georgia over 2020–21, 2,143 in 2020 and 1,114 in 2021. From 2020 to 2021, there was therefore an almost 50% drop in the number of reported cybercrimes. In parallel with this, the rate of solved cases doubled from 9.6% in 2020 to 19.7% in 2021 – although this represented a numerical increase of just 13, from 206 to 219 solved cases.⁵⁸

58. MIA, 'Overview of Cybercrimes Recorded in 2020–2021', p. 3.

Figure 4: MIA Cybercrime Statistics by Article, 2020

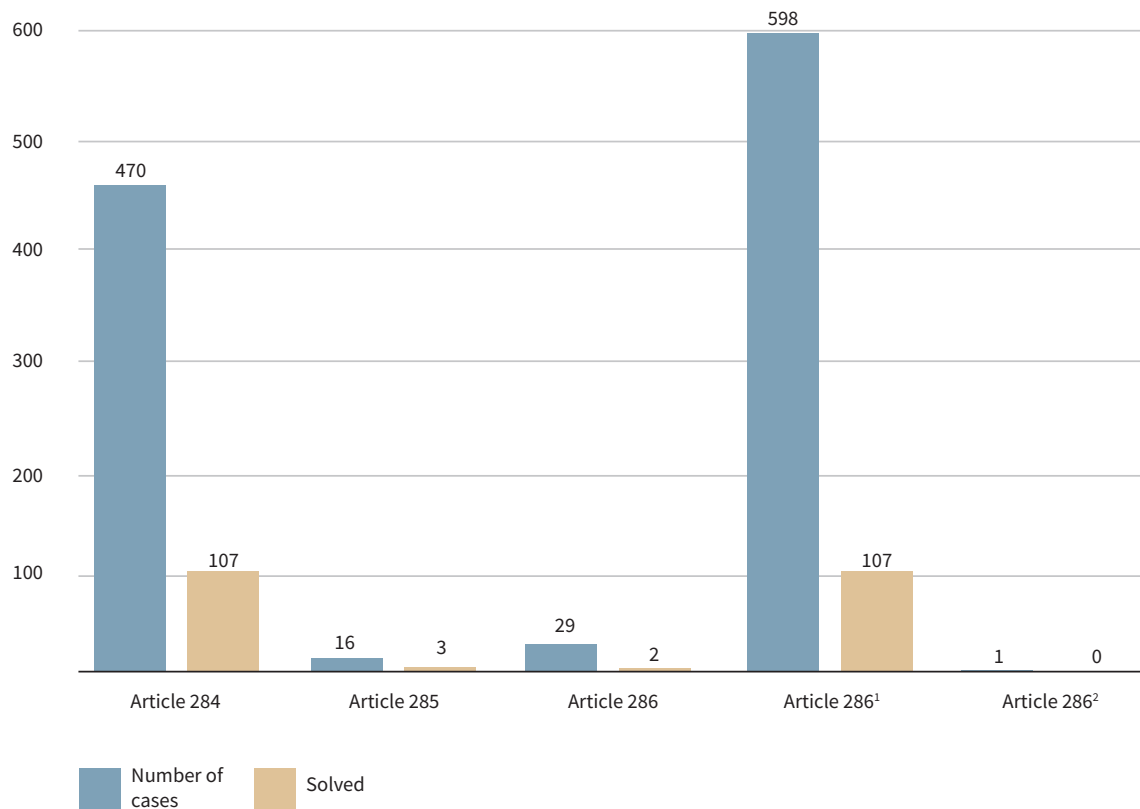


Source: MIA, 'Overview of Cybercrimes Recorded in 2020–2021', Department of Information and Analytics, 1 September 2022 (not publicly available), p. 3.

The 2020 data shows cases under Article 284, 'Unauthorised Access to a Computer System', as constituting the most cybercrimes (98%) recorded by the MIA. Cases falling under the two other articles (285 and 286), relating to illegal use of and interference with a computer or system, accounted for only 0.2% and 1.9% of total cases respectively.⁵⁹

59. *Ibid.*, pp. 3–4.

Figure 5: MIA Cybercrime Statistics by Article, 2021



Source: MIA, ‘Overview of Cybercrimes Recorded in 2020–2021’.

Before 2021, offences covering financially motivated misuse of computer data or systems fell jointly under Articles 284 and 177 (‘Theft’) of the CCG. Reforms in 2021 created a dedicated offence – Article 286¹, ‘Interference with Computer Data and/or Computer Systems for Financial Gain’ – which has since accounted for the highest number of annual cybercrime cases (54%). This has also meant that cases covered under Article 284 have fallen from 96% to 42% as a share of total recorded cybercrimes.⁶⁰ These data points indicate that profit is a key motivation in most cyber-criminal activity targeting Georgia.

MIA cybercrime data disaggregates victims by age, gender, education level, employment status and region of residence. It indicates that the highest concentration of reported cybercrimes is in Tbilisi (55.8% in 2020, 46% in 2021). It is likely that this is due to higher average awareness of cybercrimes across victims and police (see ‘Awareness of Cybercrime’). Regions with large ethnic minority populations – Kvemo Kartli and Samtskhe-Javakheti – which were identified by participants in the ethnic minorities’ FGD as areas with high cybercrime vulnerabilities (see below) do not appear in the MIA data as regions with a high rate of victimisation. In 2020, only 4.5% of individual victims were recorded as being in Kvemo Kartli and 1.9% in Samtskhe-Javakheti. The regional

60. *Ibid.*

distribution of cybercrime looks quite similar in 2021: out of a total of 1,214 individuals who were victims of cybercrime, 3.2% were reported in Kvemo Kartli and 2.1% in Samtskhe-Javakheti.⁶¹

Disaggregating MIA data by gender, in both 2020 and 2021 more men than women reported victimisation by cybercrime. As for the age distribution of victims, the most targeted age category was 25–35, followed by 35–45. The fewest number of cybercrime cases were reported in the age categories of 0–14 and 14–17.⁶² Based on this data, it appears that children and women do not have a higher risk of being targeted by cybercrime. The key reason for this is that cybercrimes recorded by the MIA are limited to those defined as such under the CCG. As outlined earlier, all articles falling under ‘cybercrime’ within the CCG are cyber-dependent; cyber-enabled crimes and online harms, which the research found disproportionately target women and minors, fall outside the cybercrime umbrella. Therefore, issues that research participants intuitively associated with cybercrime, such as cyber harassment, cyberstalking, cyber fraud and personal data leaks, do not factor into official statistics.

Comparative analysis of the data provided by the MIA and primary data-gathering activities shows that understandings of cybercrime differ between the MIA and broader society, the latter having a wider view on cybercrime compared to the existing legislative definition. In all focus group and workshop discussions, participants assumed that cyber-enabled crimes and online harms fell within scope when discussing cybercrime. When summarising cyber risks that children and their parents face, one parent who participated in the verification workshop provided the following typology of threats: ‘Dangerous relationships, cyberbullying, financial machinations and disinformation’.⁶³ This response includes both cyber-dependent crimes, and cyber-enabled crimes and online harms, particularly cyberbullying. Similar attitudes were shared by other parents who were research participants.

Similarly, in response to the question ‘What are your key concerns when it comes to cybercrime?’, teachers who participated in the verification workshop raised cyber-dependent financial fraud alongside cyber risks to children, particularly cyberstalking and cyberbullying.⁶⁴ Participants who are members of CSOs or journalists also did not make a distinction between online harms, cyber-enabled crimes and cyber-dependent crimes, instead considering them a single threat to which women and children are particularly vulnerable. Women FGD members

61. *Ibid.*, pp. 3–7.

62. *Ibid.*, pp. 6, 9.

63. Verification workshop, Tbilisi, 22 December 2022.

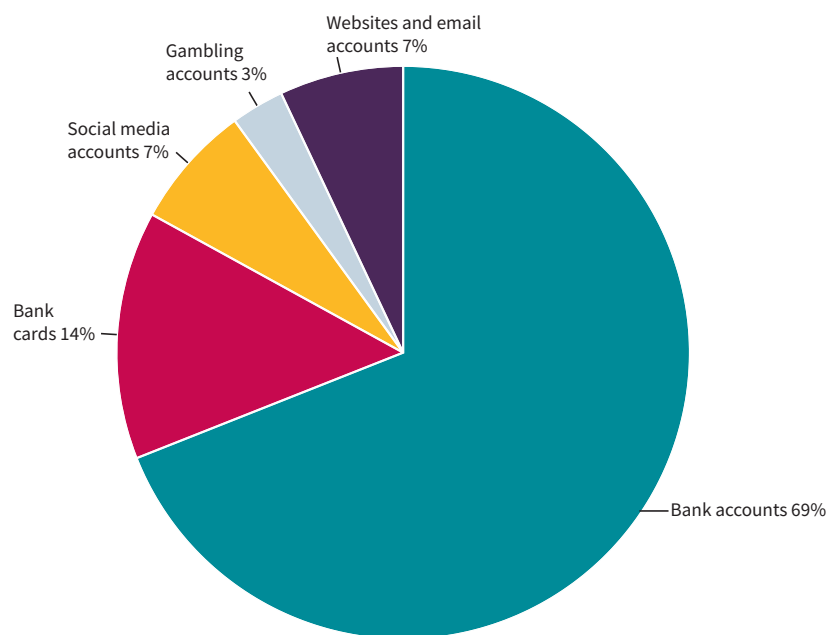
64. *Ibid.*

emphasised online bullying, leaking of personal data and blackmailing by former romantic partners as key concerns when it comes to cybercrime.

Common Threats Posed by Cybercrime

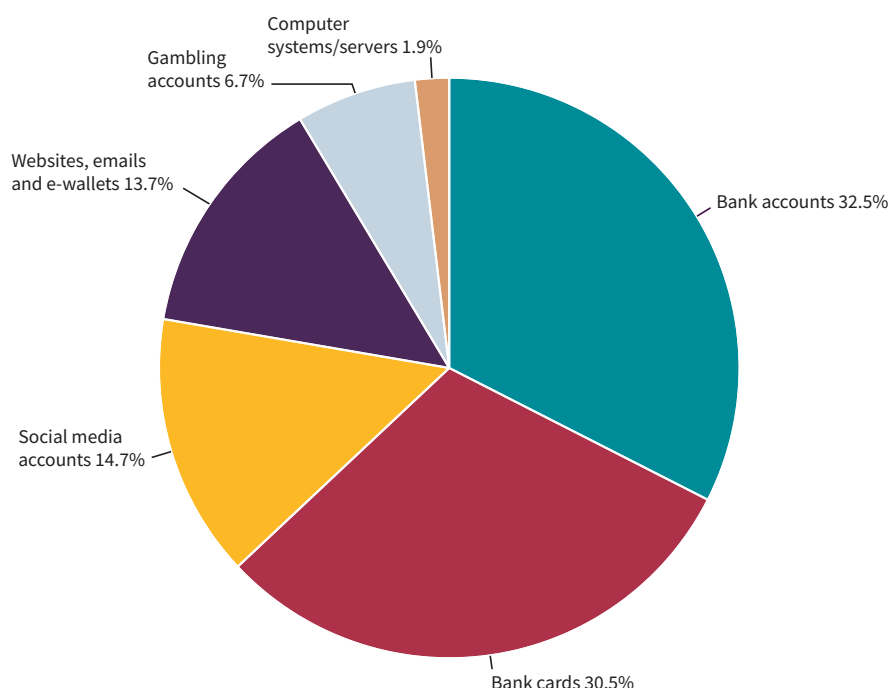
In 2020–21, the MIA identified bank accounts, bank cards, and social media and gambling website accounts as key targets of cybercrime (see Figures 6 and 7).

Figure 6: Targets of Cybercrime, 2020



Source: MIA, 'Overview of Cybercrimes Recorded in 2020–2021', p. 4.

Figure 7: Targets of Cybercrime, 2021



Source: MIA, ‘Overview of Cybercrimes Recorded in 2020–2021’, p. 4.

In 2020, unauthorised access to bank accounts accounted for the highest number of cybercrime cases, with access largely resulting from gambling account exposures (76%).⁶⁵ In these cases, victims had linked their bank cards to gambling websites, which cyber-criminals then compromised in order to steal the victims’ details and conduct unauthorised transactions. Phishing cases were also frequent, mostly driven by the sharing of links over social networks (Facebook, Instagram), and there were many instances of stolen/found bank cards being used for payment in shops. Furthermore, there was an increase in cases of unauthorised withdrawal of funds from contactless ATMs. Across social networks, it was common for perpetrators to gain unauthorised access to private Facebook accounts. Once compromised, accounts were leveraged to collect and share victims’ personal details and private materials, and to fraudulently obtain funds or bank details from the victims’ friends and family.

In 2021, cases of unauthorised access to bank accounts through gambling accounts decreased significantly. According to MIA representatives this was a result of cooperation between the MIA and the private sector which improved mechanisms for protecting bank and gambling accounts. Common cybercrimes across 2021 included fraudulent use of Facebook accounts, when perpetrators contacted the friends of the victims and obtained their bank details or asked for financial assistance; phishing, which involved the use of fake loan offers or

65. MIA, ‘Overview of Cybercrimes Recorded in 2020–2021’, p. 4.

fake shop websites to trick victims into providing their bank details; and unauthorised use of bank cards. Despite significantly decreased numbers of reported cybercrime cases in 2021, victims suffered substantially increased costs, at GEL 8.9 million in 2021 compared to GEL 3.9 million in 2020.⁶⁶

In addition to the common cybercrime threats outlined above, a general challenge mentioned across data-gathering was the under-prioritisation of cybercrime in the broader population, driven by a lack of awareness about potential cyber threats. This point was emphasised by one interviewee, who described the general level of cybercrime awareness as ‘very, very low’, especially across security basics such as password management.⁶⁷ This problem was well illustrated by one participant in the women’s FGD, who stated that since she is known in her village as a person who has some IT skills, she is asked for help in setting or resetting neighbours’ social media and even online banking account passwords.

Low levels of awareness and cyber hygiene among participants in FGDs and the verification workshop were illustrated by expressed sentiments such as ‘This does not concern me’ or ‘I will not be targeted’. One of the participants in the parents’, guardians’ and teachers’ FGD mentioned that since his own financial condition is not very favourable, he is less likely to be targeted by cyber-criminals. Another participant, from the SME community engagement workshop, made a similar point, arguing that his medium-sized local company is too small to interest cyber-criminals, who would instead focus on high-value targets. One expert interviewee said that it is quite common for people to start caring about cyber security measures only after being targeted by cyber-criminals.⁶⁸

Group-Specific Cyber Vulnerabilities

Primary data analysis shows that cybercrime reporting, outlined above, does not fully capture diverse cyber-enabled crimes or online harms. Moreover, this is particularly apparent when looking at the experience of certain groups, namely women, children and journalists. The frequency with which cyber-enabled crimes featured in discussions with these participants emphasises again the discrepancy between how cybercrime is understood by broader society and how it is viewed by government.

66. *Ibid*, p. 5.

67. Interview with senior member of CSO, Tbilisi, 6 October 2022.

68. Interview with former senior government official, video conference, 18 October 2022.

Women

Nine out of 12 women FGD participants stated that women are more likely to be victimised by cybercrime as broadly understood – including cyber-enabled crime and online harms. Women are especially vulnerable to specific cyber-enabled crimes and online harms such as personal data leaks, cyber harassment by current or former romantic partners, and cyberbullying.⁶⁹ CSOs and journalists attending the verification workshop argued that this stems from social and cultural factors – Georgia remains a conservative society where women face substantial shame from, for example, the illegal sharing of their personal data.⁷⁰ As a result, perpetrators more often use this tactic to victimise women. One verification workshop participant illustrated this point by stating that cases of personal data leakage against men are rare and that even when such incidents do occur, the victims are less likely than women are to be shamed by the exposure of their private material.⁷¹

Women are also frequently victimised by cyberbullying. One interviewee noted that this is an issue significantly affecting women politicians.⁷² Women representing both the ruling and opposition parties are targeted by cyberbullying, although the frequency of attacks on women opposition leaders is higher. One participant in the women’s FGD said that the most worrying part of cyberbullying is that she feels that victims in ‘99% of cases are women or children’.

CSO and journalist participants in the verification workshop mentioned specific challenges that women face when becoming victims of cybercrime and online harms:

- **Lack of awareness about their rights.** Victims often blame themselves and are not aware that their rights have been violated or that they can report incidents to LEAs.
- **Lack of information on whom to address for help.** In most cases, women do not know that they should address the Special Investigation Service, an independent investigative body, if they are victims of personal data leakage.
- **Lack of knowledge on cyber violence evidence preservation.** Victims often are not aware of how to preserve evidence proving that their personal data

69. Women’s FGD, Tbilisi, 4 October 2022.

70. It is important to note, however, that Georgia is not unique in this. The literature points clearly to these sentiments existing across many countries. See, for example, Tim Owen, Wayne Noble and Faye Christabel Speed, *New Perspectives on Cybercrime* (London: Palgrave Macmillan, 2017), pp. 141–58; Nicola Henry and Anastasia Powell, ‘Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence’, *Violence Against Women* (Vol. 21, No. 6, 2015), pp. 758–79.

71. Verification workshop, Tbilisi, 22 December 2022.

72. Interview with journalist, Tbilisi, 3 October 2022.

has been leaked. If perpetrators delete personal information that they have shared illegally, investigating the crime becomes significantly more difficult.⁷³

Children

Seven out of 10 participants in the parents', guardians' and teachers' FGD said that children are extremely unsafe in online spaces, with the remainder saying that they are moderately unsafe. Interview participants similarly shared this opinion, with one stressing that children are one of the most vulnerable groups because their 'online activity level is high, while [their] awareness is low'.⁷⁴ According to other interviewees, children often have a perception that everything they see online is true.⁷⁵

In contrast, some other research participants stated that children are more cyber aware than either their parents or their teachers, with one interviewee arguing that awareness among children is higher than generally presumed primarily because they are 'digital natives',⁷⁶ and some teachers in the verification workshop also mentioned that they and their colleagues often consult with their students on cyber security issues. However, this was not a consensus and some teachers strongly disagreed, arguing that those who asked students for help did so because of their own lack of awareness and not because of a unique understanding on the part of children.⁷⁷ Other participants in the verification workshop who work at CSOs or are journalists also provided nuance, outlining that children may know about finding and using mobile apps, but that does not mean they are aware of cyber hygiene and security.⁷⁸

Parents, carers and guardians who participated across primary data-gathering generally grouped types of cyber violence against children into two main areas: cyberbullying committed by minors; and acts committed by adults, such as stalking and extortion of personal data or blackmail. One verification workshop participant mentioned a case where an adult man was texting a 12-year-old girl, asking her to meet him. In this case, after a swift reaction from the girl's parents, the perpetrator was arrested.⁷⁹ Discussion around this and other similar cases showed that since there is no effective state-led information campaign on online threats, parents' ability to protect their children from such threats depends on two factors: their own level of awareness about cyber threats, and whether they

73. Verification workshop, Tbilisi, 22 December 2022.

74. Interview with government official, Tbilisi, 4 October 2022.

75. Interview with head of CSO and senior member of CSO, Tbilisi, 3 October 2022.

76. Interview with senior member of CSO, Tbilisi, 6 October 2022.

77. Verification workshop, Tbilisi, 22 December 2022.

78. *Ibid.*

79. *Ibid.*

are close enough with their children to be able to communicate effectively about cyber threats and risk. Parents agreed that in most cases, these two factors will not be present simultaneously.

Journalists

Results of the journalists' FGD show that all participants believe their profession puts them at greater risk of being targeted by cyber-criminals, with seven out of 10 saying that they have already been victimised. In response to the question 'Do you feel confident that you can keep your information safe online when using the internet and social media?', all participants in the journalists' FGD said that they were either moderately unconfident or extremely unconfident.⁸⁰

Journalists are generally concerned about 'illegal and covert surveillance by the security services', and they feel that the primary threat of cybercrime is the abuse of their privacy.⁸¹ One participant in the journalists' FGD expressed that they and their colleagues consider this risk to be so high that they have systematically taken measures to mitigate the threat. It should also be noted that several research participants across interviews and FGDs expressed concern that under the Law of Georgia on Information Security,⁸² the security services would have expanded powers of surveillance and therefore journalists would face a greater threat (see 'Trust'). It should be further noted, however, that the security services had existing powers to undertake technical surveillance prior to this legislation. For example, the Law of Georgia on Electronic Communications was amended in 2013–14 to make provision for 'covert investigative activities'.⁸³

Ethnic Minorities

As demonstrated in the ethnic minorities' FGD, one of the main challenges that ethnic Armenians and Azerbaijanis face is the language barrier to accessing cyber resources. Lack of knowledge of Georgian is a serious obstacle to obtaining any type of information, including information on cyber hygiene. Nine out of 11 ethnic minority FGD participants said that they feel their ethnicity has prevented them from receiving or accessing the tools and information that are important to protect them online.

80. Journalists' FGD, Tbilisi, 6 October 2022.

81. *Ibid.*; interview with journalist, Tbilisi, 3 October 2022.

82. Government of Georgia, 'Law of Georgia on Information Security', 6391-Ib, <<https://matsne.gov.ge/en/document/view/1679424?publication=3>>, accessed 30 May 2023.

83. Government of Georgia, 'Law of Georgia on Electronic Communications', 1514, Article 8, <<https://matsne.gov.ge/en/document/view/29620?publication=39>>, accessed 30 May 2023.

As stated by other research participants, in terms of cybercrime awareness there is a significant difference between big cities and rural areas (see ‘Priority Areas’). Therefore, ethnic minorities residing in Samtskhe-Javakheti and Kvemo Kartli face double vulnerability in terms of cybercrime risks.

SMEs

SME representatives mentioned many cases in which their organisations have been targeted by cyber-criminals. The primary cyber-dependent crime they reported experiencing was company data exfiltrated and ransomed by cyber-criminals. SME participants in the verification workshop noted that the most common attack vector in these instances was password compromise, largely through brute-force attacks or poor cyber hygiene. One participant mentioned a case in which a former employee of his organisation used a former colleague’s easy-to-guess password to access company information on current clients and pricings. The former employee then leveraged this information to inform separate negotiations, ultimately stealing clients from his former organisation.⁸⁴

Preventative cyber security measures were consistently considered ‘too expensive among SME research participants’, especially for smaller companies. One attendee of the verification workshop shared that even after major cyber incidents, SMEs prefer to invest in relatively cheap data backup software which would only assist in remediation efforts, rather than cyber security tools to mitigate the risk of threat actors being successful in the first place. General threat perception is quite low for SMEs, especially among research participants from smaller companies – one SME verification workshop attendee stated that their company had not invested more in cyber security because they have faced no major attacks so far.⁸⁵ This attitude among SMEs is not unique to Georgia, although that should not discourage action by government to address the issue.

84. Verification workshop, Tbilisi, 22 December 2022.

85. *Ibid.*

III. Reporting

Primary data-gathering across this project has identified reporting as a central issue in Georgia's experience of cybercrime. According to one senior government official, since 2019, Georgia has seen an increase in citizens' willingness to report cybercrime.⁸⁶ However, research for this paper casts doubt on this assertion and indicates that a persistent reluctance to report remains, especially among certain groups. This is primarily driven by gaps in awareness about existing reporting mechanisms, as well as a lack of trust in government and law enforcement to deliver positive results reliably and capably. It is worth emphasising that this weaker trust in reporting to resolve crimes or harms contrasts with the strong sentiment, outlined in Chapter I, that government is trusted as a cyber hygiene messenger. This chapter focuses on existing reporting mechanisms and processes in Georgia, as well as issues of trust in the capabilities and activities of the police.

Mechanisms

Reporting Processes

Following the establishment of the Cyber Crime Division at the CCPD within the MIA in 2012, the capacity of the MIA to deal with cybercrime incidents significantly increased. Cybercrime incidents that are registered in the MIA's electronic investigation programme by central and regional police units are tracked and analysed by the Crime Analysis Unit within the MIA. This includes the types of crimes outlined under Chapter 35 ('Cybercrime') of the CCG, as listed in Table 1.

The MIA records data on cyber-dependent and cyber-enabled crimes, but the latter are not registered explicitly as cybercrimes; instead, articles such as Article 151¹ ('Stalking') have cyber factors associated with them during investigation and prosecution. According to the MIA, the main source for collecting information is the investigative electronic programme that is used to search for materials and record data on criminal cases related to cybercrime.

Currently, citizens who have become victims of cybercrime have several reporting options:

86. Interview with senior government official, Tbilisi, 4 October 2022.

1. Submit a written report at the police department.
2. Call the central emergency hotline (112).
3. Report a cybercrime electronically by sending an email to a designated address controlled by the CCPD.
4. Call a separate emergency line operated within the CCPD.

Of these, the last option was identified by one interviewee, who is currently a government employee, as a less effective mechanism, since awareness of it is low and citizens prefer to report through a centralised hotline.⁸⁷ The lack of knowledge with regard to existing reporting options causes confusion even among those citizens who are willing to report cybercrime incidents. Such confusion has led people to report cases through alternative non-official channels such as social media – for instance, in the past, citizens would request help from the Facebook page of the Data Exchange Agency, the predecessor of the present-day Digital Governance Agency (DGA). While efforts were made to redirect them to the CCPD, the success of these efforts was modest.⁸⁸

In the private sector, the National Bank of Georgia has a mandate to supervise banks at a policy level and does not offer any technical support. Only banks listed as critical entities are obliged to report cybercrime incidents to the National Bank of Georgia. Across the private sector, the mandate of the DGA, which is responsible for helping the private sector deal with cyber threats, extends to third-category critical infrastructure subjects, namely banks, insurance companies, energy companies, seaports and terminals, Georgian Airways, and cargo companies. Despite the existence of several reporting mechanisms, almost all participants across data-gathering admitted that poor reporting persists and is hampering an effective response to cybercrime. Another former official mentioned that the lack of awareness of reporting mechanisms has caused significant confusion among individuals.⁸⁹ The interview process has shown that even among expert interviewees there are conflicting opinions as to the available reporting processes and, more precisely, the responsibilities of individual agencies. According to an expert interviewee, businesses and CSOs that do not have an obligation to report cybercrime incidents usually do not report due to their lack of awareness and understanding of how the reporting mechanism works and which body they should report to.⁹⁰ Multiple research participants, across interviews, FGDs and the verification workshop, also asserted that a reluctance to report emerges from an expectation that there is a low likelihood that incidents will be investigated because of limited human resources and technical capabilities.

87. *Ibid.*

88. Interview with former senior member of government, Tbilisi, 5 October 2022.

89. Interview with former senior member of government, video conference, 7 October 2022.

90. Interview with former senior member of government, video conference, 18 October 2022.

The use of official reporting mechanisms is more complicated in rural areas. Outside cities, local police forces lack capacity and expertise to deal with cybercrime incidents. This further discourages rural populations from reporting. FGD participants living in rural areas also mentioned that they are more inclined to receive advice from their family members and personal network than to report a cybercrime incident to local police.

Citizen Reporting

Awareness and trust remain two critical issues. Several FGD participants mentioned that they have been victimised by phishing and have reported these cases to the police, but investigations have not been successful, and reporting has required significant effort and time. Another FGD participant with a legal background recalled their experience of reporting a cybercrime but encountering a cynical attitude from the police. The participant nevertheless pursued the case and represented themselves during the trial, but this was dependent on their professional background and knowledge of relevant processes.⁹¹

In most cases, participants said that it would be a waste of time to undertake the reporting process; they instead preferred to contact the relevant private sector entities where the cybercrime took place, in most cases commercial banks, and take the necessary individual measures to protect themselves.⁹² This is not unique to Georgia – recourse to banks, for example, in cases of cyber fraud or cyber-enabled theft is common globally. The issue in Georgia is that this decision is, according to the data-gathering for this report, primarily motivated by a negative decision not to go to law enforcement, rather than by a positive one to choose banks or other businesses. One expert interviewee, however, nuanced this by highlighting an increase in effective awareness-raising efforts by banks in recent years aimed at improving customers' understanding of common threats from cybercrime, although they stressed that in most cases citizens still take protective measures only once they have been victimised, rather than pre-emptively.⁹³ As an example of this, several FGD participants mentioned that they decided to use insurance services that banks offer against cyber attacks only after being targeted.

91. Ethnic minorities' FGD, Tbilisi, 5 October 2022.

92. *Ibid.*

93. Interview with former senior government official, Tbilisi, 5 October 2022.

Children and Young People

From the data-gathering conducted for this report, children have been identified as one of the groups most vulnerable to cybercrime, particularly cyber-enabled crime and online harms such as cyberbullying. Most attendees of the parents', guardians' and teachers' FGD believe that children are extremely unsafe online, and research participants across interviews and the verification workshop agree that cyberbullying is one of the most widespread problems for children and young people (see 'Group-Specific Cyber Vulnerabilities').⁹⁴ Awareness about available reporting mechanisms is among the lowest for cybercrime that involves children. Many parents try to deal with such cases on their own rather than addressing LEAs.⁹⁵ The MIA has different procedures for cybercrime cases committed against children, in line with the provisions of the Juvenile Justice Code of Georgia, which outlines the roles of parents, guardians and teachers in the judicial process. Thus, investigators who deal with such cases are required to go through specialist training.⁹⁶

Women

Cyberbullying has also been identified as one of the key concerns for women and young women and girls in particular. Women are often threatened and blackmailed with the exposure of their private material.⁹⁷ Several expert interviewees pointed to notorious recent cases of prominent journalists and politicians being victimised in this way.⁹⁸ Yet the lack of a track record in successful investigations of such incidents has further eroded trust, and women have been disincentivised to report as their confidence in LEAs has diminished.

Another issue is the lack of knowledge about these types of offences. Many women are unaware that cyber-enabled blackmail and exposure of private or sensitive material constitute a crime. In some cases, there are more complex and deep-rooted cultural explanations, such as shame and stigma with regard to crimes bearing a sexual character – in such cases the number of reported incidents is very low, since women try to avoid approaching the police, fearing that their data may not be protected. An expert interviewee noted that the MIA needs sensitive and well-trained investigators to tackle the problems that women are currently facing in cyberspace.⁹⁹

94. Parents', guardians' and teachers' FGD, Tbilisi, 7 October 2022.

95. *Ibid.*

96. Interview with current government employee, Tbilisi, 4 October 2022.

97. Women's FGD, Tbilisi, 4 October 2022.

98. Interview with member of women's CSO, video conference, 20 October 2022; interview with head of CSO and senior member of CSO, Tbilisi, 3 October 2022.

99. Interview with member of women's CSO, video conference, 20 October 2022.

Following victimisation, women frequently engage CSOs focused on women's rights to access advice, including about whether what they have experienced constitutes a crime. According to an expert interviewee, women generally suffer more from narrow definitions of cybercrime.¹⁰⁰ In most cases, women are victims of cyber-enabled crimes or online harms which are exacerbated by traditional gender roles and conservative views on sexual freedoms. These crimes do not have dedicated articles within the CCG but are instead derived from existing articles on, for example, stalking (Article 151¹). This is not unusual for a national criminal code, but, as one interviewee argued, the lack of a mention of cyber makes it more difficult to navigate the recourse to justice, both for victims and for law enforcement.¹⁰¹ As such, an inadequate consideration of online harms, cyber-enabled crimes or cyber elements of existing crimes creates roadblocks to women's ability to access justice and the MIA's ability to support them in achieving it.

Lack of Effective Information-Sharing Systems

Both former and current officials interviewed for the research for this paper agreed that the lack of inter-agency information-sharing poses a set of challenges. Although the NCSS Action Plan includes specific activities related to the development of an information-sharing platform, currently such a platform does not exist.¹⁰² A former government employee suggested that two separate systems could be developed – one for critical infrastructure subjects and another for non-critical subjects.¹⁰³ Another interviewee, who is also a former government employee, recommended building the information-sharing process on a sectoral basis, starting with either energy or finance.¹⁰⁴

In most cases, information-sharing between agencies takes place through informal methods and personal communication. In general, agencies tend to be reluctant to share information with each other. Some interviewees expressed doubt about how effectively agencies including the MIA and the Cyber Security Bureau share information.¹⁰⁵ Thus, there is a need to understand that information-sharing can be beneficial for all stakeholders. It is noteworthy that both current

100. *Ibid.*

101. *Ibid.*

102. Government of Georgia, 'Georgian National Cyber Security Strategy', pp. 3 and 20.

103. Interview with former senior government official, Tbilisi, 4 October 2022.

104. Interview with former senior government official, video conference, 18 October 2022.

105. Interview with former senior government official, Tbilisi, 5 October 2022; *ibid.*

and former officials admit that there is nothing effective in place in this regard and acknowledge the need to establish an effective system.

For the private sector, the DGA runs a designated platform on which both private entities and individuals can share information about incidents. The DGA intends to make improvements to the platform's provision of statistical data.¹⁰⁶

Challenges around information-sharing within government are being tackled as part of the UK–Georgia Cyber Partnership programme, which has committed to developing an effective information-sharing framework. Information-sharing is also one of the key activities of the NCSS.

Trust

Most FDG participants and interviewees identified a lack of trust in LEAs as one of the key factors in not reporting cybercrime incidents. Two key factors that have been identified by the research for this paper are lack of trust in LEA capability and lack of trust in LEA reliability.

Lack of Trust in LEA Capability

Most FGD participants did not believe that police can effectively handle cyber incidents, primarily because of the lack of adequate capabilities to investigate cybercrime cases. Additionally, the reporting process itself is assumed to be lengthy and citizens are therefore unwilling to undertake it, especially as they do not believe that it will achieve positive outcomes.

Despite gradual improvements in technical capabilities within the MIA, several expert interviewees believe that specific gaps in human and technical resources remain across the CCPD's Cyber Crime Division. The assumption of non-expert research participants is that cybercrime incidents are difficult to investigate, as their complexity exceeds government capabilities. This issue is exacerbated in rural areas, where the police often lack specialised training on how to deal with cybercrime victims. Supporting this, several FGD participants complained about the lack of police competencies outside big cities. These problems often lead to under-reporting as victims are incentivised to deal with incidents on their own. For instance, in cases of minor fraud, many participants are either reliant on banks or do not bother to report and hence feel unable not to accept the financial loss.

106. Interview with senior government official, Tbilisi, 4 October 2022.

Most participants in the journalists' FGD who had been targeted by cybercrime chose to rely on informal networks rather than reporting to law enforcement.¹⁰⁷ For instance, a regional media executive recalled their experience of reporting a hacking incident directed at their official YouTube channel.¹⁰⁸ In response, the police said that the incident was beyond their capabilities and that the company should strengthen the security of its online accounts. This incident also indicates that generally, LEAs do not have sufficient links with big tech companies to tackle such issues. Due to the police's response, the media executive had to turn to their own network and seek help informally.

Lack of Trust in LEA Reliability

The level of distrust in the decency and reliability of LEAs among participants in the journalists' FGD was particularly high, with several noting that they do not even trust awareness-raising resources disseminated by state channels. One of the key concerns expressed by journalists was the belief that LEAs and the security services would compromise their confidentiality and data privacy.

Confidentiality has been identified as a key problem in rural areas. According to an expert interviewee, it is almost impossible to maintain confidentiality in rural communities, and this makes citizens reluctant to report crimes. Doubts around confidentiality are particularly high among women, since they are more frequently victimised by targeted leaks of their private material and are highly sensitive to this being disseminated further due to poor data hygiene within rural police forces. One interviewee, a former government official, mentioned that many victims fear that reporting may lead to reputational damage, as they believe that their personal data will not be securely handled by the police.¹⁰⁹ Several participants in the women's FGD stated that they usually seek help from other women in spaces such as Facebook groups, but that these spaces often just serve to provide women with confidence and support in approaching the police.

Some expert interviewees expressed concern about the expanding powers of the State Security Service of Georgia's Operational Technical Agency (OTA) under the Law of Georgia on Information Security.¹¹⁰ Generally, trust in the OTA's capabilities is quite high, but trust in the motives behind its activities is relatively low. This is largely due to popular perceptions that the agency misuses the personal information of citizens. Hence, according to one interviewee, greater

107. Journalists' FGD, Tbilisi, 6 October 2022.

108. *Ibid.*

109. Interview with former senior member of government, Tbilisi, 5 October 2022.

110. Interviews, from October 2022 to January 2023.

communication efforts should be made by the OTA to build trust with citizens, though this will be an uphill struggle given existing perceptions of the agency.

Trust in reporting is higher regarding the private sector, and many participants highlighted that they find banks reliable and trustworthy. When victimised by a financially motivated cybercrime, most research participants prefer to report to banks rather than to the police. Many participants negatively assessed current levels of activity by government, highlighting that state agencies must become more proactive in raising cyber awareness and helping the population to develop knowledge about cyber hygiene.

IV. Findings and Recommendations

This chapter draws on the analysis outlined in the paper to present research findings. From these, it elaborates recommendations targeted at stakeholders across the public, private and civil society sectors in Georgia, as well as international actors.

Finding 1: Compromise of online bank accounts, credit and debit card fraud, and compromise of social media and gambling accounts, are the primary cyber-dependent crimes threatening the general population.

Recommendation: The MIA should continue to work with key partners in the private sector to combat the most frequent cybercrimes. The MIA should analyse its recent collaboration with private sector partners, notably gambling companies, to elaborate a model for its multi-stakeholder engagement efforts to target high-incidence cybercrimes. This model should define mechanisms for identifying, approaching and interacting with private companies, and should establish a framework for assessing the effectiveness of collaboration activities. This recommendation aligns with the NCSS's Objective 2 and Task 2.2, to boost public-private partnership and develop effective systems to tackle cybercrime.¹¹¹

Finding 2: Persistent issues exist around information-sharing platforms and processes, both within government and with private sector stakeholders and civil society. Outstanding issues include:

- General uncertainty among expert interviewees, including government and former government participants, as to whether an information-sharing platform exists.
- A lack of institutionalisation and systematisation of information-sharing, which prompts relevant agencies to rely on personal contacts and informal exchanges.

Recommendation: Implement improvements to cybercrime and cyber threat reporting and information-sharing. Cross-government information-sharing practices related to cyber threat and cybercrime should be developed or improved in line with recommendations outlined in the UK-Georgia Cyber Partnership's framework for information sharing. This aligns with objectives outlined in the

111. Government of Georgia, 'Georgian National Cyber Security Strategy', pp. 17-18.

NCSS, and with Georgia's ambition to adopt international best practices.¹¹² Information-sharing practices are necessarily cross-government, so agencies with responsibilities for cyber security must be coordinated by the National Security Council.

Finding 3: General awareness of cybercrime threats is poor. Key aspects of this are:

- Certain vulnerable groups have lower-than-average awareness. These include children, older people, citizens living in rural areas, and ethnic minorities – especially those who do not speak Georgian.
- Low cybercrime awareness among influential groups, such as journalists, police and teachers, has a multiplier effect that produces negative knock-on impacts.
- The education system is insufficiently leveraged to promote cyber awareness. Research has pointed to more opportunities for schools to be used as community centres for inter-group awareness-raising and for primary and secondary curricula to include more about cyber security.
- Low awareness of cybercrime contributes to poor understanding and take-up of cyber hygiene best practices across the population.
- Government information campaigns and LEAs are considered the most trustworthy sources of cyber hygiene information, but friends and family are most often relied upon for information about cyber hygiene.
- Some SMEs do not consider that cybercrime poses a credible threat to them due to their small size and low revenue.
- Certain groups' awareness levels, whether strong or weak, have a multiplier effect on wider awareness and understanding.
- Ongoing cybercrime awareness-raising activities are sparse and decentralised. There is a lack of understanding about the extent of activities across the public sector and civil society.

Recommendation: Government should launch cybercrime awareness campaigns. Government should follow through on commitments under Objective 1 of the NCSS¹¹³ and launch a national cybercrime awareness campaign, which should be coordinated by the DGA in close partnership with the MIA. A partnership between the DGA and the MIA is important, as the former holds responsibility for awareness under the NCSS as well as considerable strategic communications expertise, while the latter is the principal agency responsible for cybercrime and is therefore best placed to determine where awareness improvements would have the most impact. The campaign should also be

112. *Ibid.*, p. 10.

113. *Ibid.*, p. 16.

inherently multi-stakeholder, leveraging existing and future efforts from diverse government agencies/departments, the private sector and civil society – acknowledging that cyber security is ‘everyone’s responsibility’.¹¹⁴ The campaign should integrate principles of a successful information campaign outlined in Chapter I. Separate recommendations regarding the campaign are discussed below.

Recommendation: Put government and law enforcement involvement in the cyber awareness campaign at the forefront. Government information campaigns and law enforcement are seen as trustworthy sources on cyber hygiene. The involvement of the DGA, the MIA and potentially the CCPD should therefore be highlighted in campaign materials, publications and resources. This should include but not be limited to representatives of these agencies engaging with media, agency branding being placed on campaign publications, and official agency social media accounts being leveraged to amplify campaign messaging.

Recommendation: Messaging should focus on three key areas: the nature of cybercrime; cyber hygiene; and reporting.

1. **The nature of cybercrime.** Popular understandings of cybercrime do not align with the definitions outlined in the CCG. On the one hand, this could indicate a need for government to adapt existing legal provisions, but on the other, it demonstrates a need to build awareness of what cyber activities constitute a crime, whether cyber-dependent or cyber-enabled. An awareness campaign, spearheaded by the DGA and the MIA, should therefore focus on education on the nature and signs of cybercrime. Within this, a particular focus should be put on crimes experienced by women and young people, especially relating to abuse of personal or private information.
2. **Cyber hygiene.** A persistent issue is that people either do not know that they should improve their cyber hygiene or do not know how to. In part this is driven by other gaps in awareness around the risks from cybercrime, personal and organisational vulnerability, and the potential impacts of victimisation, which do not provide an incentive to become more aware. Once properly motivated, people implementing cyber hygiene measures, whether in personal or professional settings, can be decisive in improving national cyber resilience and is necessary to achieve a whole-of-society approach to cyber security.
3. **Reporting.** A key driver of poor reporting is a lack of awareness or confusion about existing reporting mechanisms. A national campaign should focus on embedding an understanding of the available reporting options in the population (see ‘Reporting Processes’). This message should emphasise that reporting is neither complicated nor time-consuming and should focus on certain priority areas, including rural areas. As with other parts of the

114. *Ibid.*, p. 14.

campaign, communications around reporting should be accessible in various formats and languages. Another focus of reporting messaging should be to address the lack of confidence that women have in the confidentiality and handling of their cases once they have approached law enforcement.

Recommendation: Make better use of schools and teachers as catalysts for increased awareness across society. The national cyber awareness campaign should concentrate on schools as centres for key vulnerable (children) and influencer (teachers) groups as well as community hubs. The campaign should work with the Ministry of Education, Science, Culture and Sport to leverage schools, for example to distribute cyber awareness and hygiene information and resources, and to host community events.

Recommendation: Focus on strong monitoring, research, evaluation and learning from the outset. Effective monitoring, research, evaluation and learning from campaign inception to completion, including a follow-up analysis, will be crucial to capture accurate understandings of campaign successes and areas for improvement. This will ensure that the value of awareness activities can be measured within government and could lead to the development of best practices that Georgia could share regionally. Developing a monitoring, research, evaluation and learning framework should be the joint responsibility of the DGA, which will own the campaign, and the MIA, which has the most share of interest in its impacts on cybercrime vulnerability.

Recommendation: Implement cyber hygiene training for influential groups. Government, CSOs and international funders should support training on cyber hygiene essentials (behaviours, tools, information sources) for influential groups who have a multiplier effect within their networks, notably teachers, journalists and local law enforcement. Training should emphasise simple and practical solutions and provide key resources such as reference booklets that detail best practices. Courses should leverage existing professional networks (such as the Georgian Charter of Journalistic Ethics¹¹⁵) to identify and reach out to potential participants.

Recommendation: Make the campaign part of broader activities by government to tackle cybercrime risk. The campaign, although important, should not be seen as a fix-all. Improving awareness of cybercrime and cyber hygiene will improve national resilience, but it should not preclude exploring other measures, such as instituting producer and supplier cyber security requirements to take risk away from end users, rather than relying on their adherence to best practices.

115. See 'Code of Conduct of the Georgian Charter of Journalistic Ethics', 1 June 2019, <<https://www.qartia.ge/en/documents/article/75193-code-of-conduct-of-the-georgian-charter-of-journalistic-ethics>>, accessed 30 May 2023.

Therefore, aligning with the objectives of the NCSS, a national cyber awareness campaign is just one part of a national ambition to improve cyber security.

Recommendation: Maintain activity to track ongoing and previous awareness-raising activities. Government should lead on efforts to systematise and transparently communicate about awareness-raising activities. The DGA or MIA should maintain an up-to-date, publicly accessible list of the government's current and previous awareness-building activities. Ideally this list would be created and maintained in partnership with a CSO. NGOs should be able to voluntarily list their activities in the same place.

Finding 4: Citizens' intuitive understanding of cybercrime is wider than the legal definition of cybercrime outlined in the CCG. Articles relating to cybercrime in the CCG only concern cyber-dependent crimes, whereas citizens often also associate cybercrime with cyber-enabled crimes and online harms. This creates misunderstandings and unmatched expectations. For instance, women report being disproportionately victimised by cyber-enabled crimes such as exposure or threatened exposure of private data, but the government does not capture these activities as cybercrime; thus, the government's and the population's framing of the scale of the problem are out of step.

Recommendation: Parliament's Legal Affairs Committee and policy teams within the MIA should explore amendments to the CCG to better account for cyber-enabled aspects of existing criminal Articles. Initiatives by the Legal Affairs Committee and relevant MIA policy teams should be launched to consider the viability of amending certain CCG Articles to include mention of cyber, digital or online methods. The objective of these activities would be to establish whether it is possible or desirable to better recognise the cyber-enabled aspect of existing crimes. Such a change could also reflect the NCSS's acknowledgement that '[the] "cyber" element ... facilitates the commission of various criminal acts ... and allows for the commission of auxiliary crimes' beyond cybercrime conceived 'in a narrow, classic sense'.¹¹⁶

Finding 5: There are insufficient university-level cyber security qualifications and training pathways.

Recommendation: Expand higher-education opportunities in cyber security and cybercrime. Universities, the David Aghmashenebeli National Defence Academy and other centres of learning should be supported by government to expand their offers of degrees and modules focused on cyber security and cybercrime. Government could do this through, for example, providing guaranteed sponsorships to newly launched cyber security programmes. This approach would also allow government to tackle the gender imbalance across the cyber

116. Government of Georgia, 'Georgian National Cyber Security Strategy', p. 13.

security and wider tech workforce by targeting and/or providing additional scholarships for women. The initial focus of this initiative should be on postgraduate education opportunities. This recommendation directly builds on part of the NCSS's Task 1.1, to introduce 'bachelor's and master's degrees in this field at accredited educational institutions'.¹¹⁷

Finding 6: People are reluctant to report cybercrime to law enforcement, whether they understand it as a cyber-dependent or cyber-enabled crime. Reasons for this include:

- Low awareness about what cybercrime is and when one has been committed.
- A lack of understanding about official reporting mechanisms, including where and how to report, how to preserve evidence, and what kind of support is available. This is particularly acute among parents, who struggle to understand how to report on behalf of their children.
- Low trust in the police's capacity to deal with reported incidents, especially among rural populations.
- Low trust that police will be responsible with information about the case and will preserve data confidentiality. This is more acute in cases where sensitive or personal data, such as private photos, has been stolen or is being misused by cyber-criminals. Where these cases affect women, the reporting likelihood is especially low due to cultural and social stigma.
- Citizens have higher confidence in reporting to banks than to law enforcement.

Recommendation: Run courses for local police on supporting victims of cyber-dependent and cyber-enabled crimes as well as online harms. Efforts are being made to increase capabilities and capacities to tackle cybercrime, but victim-centric measures are under-prioritised. Local police would benefit from training around sensitive and confidential data collection and handling for victims of cybercrime and online harms (which pass the threshold of criminality) defined broadly. This training should focus on sensitivity around cyber-enabled crimes and criminal online harms which disproportionately impact children and women. It should aim to increase local police capabilities, thus incentivising reporting and improving data collection on crimes. A particular emphasis across these activities should be to amend or otherwise strengthen handling procedures such that expectations by women about the privacy and confidentiality of their case information are met or, where they are not, that there is a clear system of accountability to further incentivise secure handling of victim data.

Finding 7: The shortage of certified/qualified employees across the cyber security ecosystem is more pronounced in certifications/qualifications that have a higher failure rate or cover more sensitive topics.

117. *Ibid.*, p. 16.

Recommendation: International funders of cyber security qualifications and certifications should be less risk averse. International cyber capacity-building funders should support access to qualifications and certifications which have higher failure rates and in which there is a gap in the Georgian ecosystem. Currently funders are risk averse, supporting low failure rate schemes and excluding qualifications or certifications on sensitive topics. Increased funding for higher-risk qualifications/certifications should, however, be accompanied by thorough monitoring, evaluation and learning processes to ensure value. Additionally, holistic risk assessments should be conducted on funded courses, including an assessment of their appreciation of ethical and legal considerations. The identification of courses should build from the baseline of those identified in Task 3.1 of the NCSS, and a consultative and needs-based approach to identifying further specific certifications/qualifications should be taken.¹¹⁸

Finding 8: Insufficient data is available on cybercrime in Georgia.

Recommendation: The MIA should conduct and publish an annual analysis of cybercrime disaggregated by characteristics that increase vulnerability. The Crime Analysis Unit of the Analytics Division of the Department of Information and Analytics within the MIA should conduct an annual analysis of cybercrime incidences disaggregated by factors including region, gender, employment and age. To support this function, it is important that greater resourcing is given to the Crime Analysis Unit. The desired outcome would be for society to become more aware of specific cybercrime threats, businesses and organisations to be able to better prepare, and civil society to understand how to better target support. This recommendation is coherent with NCSS Task 2.2, to '[d]evelop an effective system to tackle cyber crime', as it provides and examines the necessary data to best organise against cybercrime.¹¹⁹

Finding 9: Parents struggle to protect their children from diverse cybercrimes and online harms on their home networks.

Recommendation: Internet service providers should include parental safety controls as standard. The government or the Georgian National Communications Commission should consider requiring internet service providers to include parental safety controls as part of home broadband packages for no additional cost.

118. *Ibid.*, p. 20.

119. *Ibid.*, p. 18.

Conclusion

The analysis in this paper suggests that the government of Georgia has made some progress, albeit limited, in tackling the threat of cybercrime in recent years. Concerted efforts have been made to reform aspects of the CCG, develop police capacities and work with the private sector to target high-incidence crimes. The government has pointed to falling rates of reported cybercrimes to demonstrate the effectiveness of these measures, but this is not a complete picture. Declining rates of cybercrimes covered by the CCG relate only to cyber-dependent crimes and fundamentally rely on victims reporting offences. This paper finds, through examining the experiences of FGD participants, that cyber-enabled crime and online harms are common, particularly among vulnerable groups, and that strong disincentives exist to reporting them.

Georgia is constrained by several factors in its resilience against cybercrime and in the government's ability to understand the problem. These factors include: low awareness; mismatched understandings of cybercrime; and disincentives to reporting.

Low awareness of the cybercrime threat is pervasive and heightened among certain vulnerable groups, namely children, older people, rural residents and non-Georgian-speaking ethnic minorities. As a result, knowledge about cybercrime risk-management techniques, or cyber hygiene, is poorly dispersed, and public take-up is low. While this is not unique to Georgia, it worsens the national risk profile as there are more vulnerable points on the threat surface, whether in personal or organisational networks. The experience of cybercrime is therefore often rooted in confusion or misunderstanding, as people do not recognise the threat or risks facing them.

Common intuitive understandings of cybercrime as cyber-enabled crime or online harms such as cyberbullying and online fraud do not match with CCG articles which limit cybercrime to cyber-dependent crime and do not make explicit provision for the cyber-enabled aspects of other crimes. This illustrates the mismatched understanding of cybercrime between government and citizens. While this is not conclusively a problem with either common understandings or with the CCG, it contributes to people's perception of the efforts that government has made and indicates which areas they believe are most vulnerable and should be focused on.

Disincentives to reporting cybercrime prevent government from accurately understanding the scale of the problem. The simplest of these is a lack of awareness and understanding – people often do not know when they have been

victimised, how to report it, or what evidence to preserve. This uncertainty partly feeds under-reporting. The other main factor is a lack of trust. This has two aspects: people believe that government, in this case law enforcement, lacks the capability to undertake cybercrime investigations; and people worry that those handling their case are not reliable and that they will not preserve the confidentiality of disclosed or compromised data – this is particularly acute in rural contexts. Cybercrime is therefore often experienced as a private burden for which people feel unable to access law enforcement support.

To address these problem areas, the government should take a joined-up approach, leveraging relevant departments, as well as partners in the private sector and civil society. First and foremost, the government should undertake an ambitious national awareness campaign with the aim of both improving people's understanding and thus their overall resilience, and of building trust that law enforcement is able to help in a way that is supportive and victim-centric. Beyond this central plank, other activities, such as expanding higher-education opportunities in cyber security, targeted training for local police forces, and mandating internet service providers to include parental security functionalities as standard, will go a long way to strengthening overall cybercrime resilience.

Issue areas that are less addressed within this paper, but which the government should also consider, are the role of cyber security requirements on producers and suppliers to shift the cybercrime risk away from users, the place of multilateral cooperation in targeting international cybercrime, and a focus on enterprise. This final point is particularly important to guarantee cyber security as Georgia's economy continues to digitalise.

With threats from cyber, including cybercrime, growing in impact and reach, and the regional security context remaining tense, Georgia should take the opportunity now to build strong capacities in case it needs to surge these in future. To do so, the government must take a whole-of-society approach, appreciating that cyber security capabilities and expertise are concentrated in the private sector. This will enable Georgia to become a more resilient and cyber-secure country, strengthening its defence against cyber threats, including cybercrime, and building its reputation as a regional leader in cyber security.

About the Authors

Joseph Jarnecki is a Research Fellow in the Cyber team at RUSI. Joseph's experience covers cyber capacity building, cybercrime harms, threats and opportunities from advanced and emerging technology, ransomware and multi-stakeholder approaches to cyber strategy. Currently his primary research is on the experience of cybercrime, the role of technology companies in national cyber defence and horizon-scanning opportunities and risks from emerging and disruptive technologies. He has a particular interest in the role responsibility plays in a whole-of-society approach to cyber security.

Natia Seskuria is a Founder and Executive Director of the Regional Institute for Security Studies, a Tbilisi-based think tank and an official partner of RUSI. She is also an Associate Fellow at RUSI. Natia holds an advisory position at Chatham House and is a lecturer in Russian politics. She has broad experience in policymaking and strategic foresight, and provides analysis on defence and security issues. In the past, she served at the Office of the National Security Council of Georgia and the Ministry of Defence of Georgia. Natia's research focuses on Russia's domestic and foreign policy, in particular Russia's relations with its neighbours, its strategic approach to occupied regions, its relations with the West and the use of 'active measures'. She is a frequent commentator on major media outlets including the BBC, France 24 and CNN.

Tatia Chikhladze is a Research Fellow at the Regional Institute for Security Studies and an Associate Professor at the British University of Georgia. Her research interests include Black Sea regional security, hybrid warfare and the resilience of post-Soviet authoritarian regimes. Tatia has extensive experience of working in analytical positions at different public institutions in Georgia, including the National Security Council, the Office of the State Minister of Georgia for Reintegration, and the Ministry of Internal Affairs. She completed her PhD at the University of Bremen in Germany, received her first Master's degree, in Social Sciences, at Tbilisi State University and her second Master's degree, in Russian and East European Studies, at the University of Oxford.