KHATUNA MSHVIDOBADZE

GEORGIA CYBER BAROMETER REPORT

Tbilisi
2015

Georgia Cyber Barometer Report

Khatuna Mshvidobadze, Ph.D.

Georgian Foundation for Strategic and International Studies

Prepared for the British Embassy, Tbilisi and the National Crime Agency, London

Editors: **David Smith, Rusudan Margishvili**

Technical editor: **Nino Kavelashvili**

ISBN 978-9941-0-8228-3

Foreword by Dr. Eka Metreveli, Chief Executive Officer (acting) of the Georgian Foundation for Strategic and International Studies

It is with great pride that we present the Georgia Cyber Barometer Report, written by Dr. Khatuna Mshvidobadze, Senior Fellow here at the Georgian Foundation for Strategic and International Studies (GFSIS). This is a comprehensive look at the state of Georgia's cybersecurity, a vital issue for our country's security, economic development and further integration with the rest of Europe. The report is optimistic, saying that the glass is more than half full, because Georgia has already achieved so much in the field of cybersecurity. However, this report is also objective–it clearly identifies areas that need improvement. Most important, it offers concrete recommendations for the next steps that Georgia must take.

In 2008, Georgia became the first country every to sustain simultaneous kinetic and cyber-attacks. At the time, our Internet infrastructure and use was much smaller than it is today. Today, we are much more dependent on the Internet, a fact that underlies our increasing economic development and our international relationships. However, as more of our endeavors move online, we must take greater care not to allow this great benefit to become an engine for war, espionage and crime. Government, business, civil society and our international partners must join together to bolster cybersecurity. In this regard, Georgia Cyber Barometer Report underscores that once again, GFSIS is at the forefront of 21st Century security challenges. With Dr. Mshvidobadze's continued efforts, GFSIS will maintain its leadership in this field.

Finally, I wish to thank the British Government, particularly the British Embassy here in Tbilisi and the National Crime Agency for their generous support of this project. They have provided not only financial support but also intellectual leadership in advancing the proposition that international cooperation underlies improved cybersecurity for us all. We look forward to our continued cooperation with the United Kingdom.

Dr. EKA METREVELI
Acting Chief Executive Officer

Foreword by Her Majesty's Ambassador to Georgia H. E. Alexandra Hall Hall

More and more the internet is becoming integrated into modern life. The governments that serve us, the militaries that protect us, the economy that sustains us and the communications industry that helps us stay in touch are also moving online. There are huge opportunities in cyberspace, but there are also risks.

The UK's aspiration is for a cyberspace where citizens can take full advantage of the opportunities afforded by cyberspace – in forging relationships, building businesses, developing networks of friends and contacts, transcending traditional barriers of geographical distance, different time zones, language and other cultural obstacles – to enrich their lives, maximise opportunities, and fulfil their aspirations. But that also requires establishing effective mechanisms to mitigate the risks, and prevent abuse of the freedoms of cyberspace: where law enforcement is tackling cyber criminals; citizens know how to protect themselves online; cyber space is an effective but secure tool for business; online public services are protected and resilient; and the threats to national infrastructure, national security, or personal welfare have been confronted.

This Georgia Cyber Barometer Report gives a snapshot of Georgia's cyber security. The report sets out all that Georgia is doing to protect its citizens, businesses and critical national infrastructure, and makes recommendations for future priority areas of work. In a domain where the pace of technology change is fast-moving, responding effectively requires a consistent, extensive and evolving effort.

I would like to pay tribute to Khatuna Mshvidobadze who has for two years worked hard to compile this report. I would also like to thank all those that contributed to this report, for their frank views and for their continued commitment to protecting the people of Georgia in cyberspace.

ALEXANDRA HALL HALL
British Ambassador to Georgia

TABLE OF CONTENTS

ABOUT THE PROJECT

Cyber Barometer Report on Georgia is an analysis of cybercrime and cyber threats, responses and related matters in Georgia. This report was written by Dr. Khatuna Mshvidobadze, Senior Associate at the Georgian Security Analysis Center, which is part of the Georgian Foundation for Strategic and International Studies (GFSIS). It was commissioned by the British Embassy in Georgia on behalf of the British National Crime Agency. The report does not necessarily reflect the views of the sponsor.

The aim of the report is to uncover cyber threats to the country and the strengths and weaknesses that characterize the country's ability to respond to those threats. In particular, this report covers levels and types of cybercrime on the Internet in Georgia; law enforcement capabilities, activities and assessments; key elements of critical infrastructure relating to the Internet in Georgia and the current level of cyber security protecting such assets; economic and social prospects; a net assessment and a possible roadmap for further action. The last are intended as recommendations that the UK Government could consider to help further progress and cooperation in Georgia.

To identify the cyber security status of the country, the analyst conducted comprehensive research, including interviews with a mix of local cyber experts and representatives of private businesses and governmental agencies who are in charge of cyber security.

The author would like to thank the following people and organizations for their contributions. Interviews were conducted during 2014 and 2015. Positions indicated are those held at the time of the interview.

- **Irakli Tsiklauri**, Head of Cyber Crime Unit of the Central Criminal Police Department, Ministry of Internal Affairs of Georgia
- **Tariel Alavidze**, Former Head of Cyber Crime Unit of the Central Criminal Police Department, Ministry of Internal Affairs of Georgia
- **Ivane Katsitadze**, Deputy Head of Cyber Crime Unit of the Central Criminal Police Department, Ministry of Internal Affairs of Georgia
- **Otar Gadabadze**, Former Deputy Head of Cyber Crime Unit of the Central Criminal Police Department, Ministry of Internal Affairs of Georgia

- **Aram Panyan**, Detective, Cyber Crime Unit of the Central Criminal Police Department, Ministry of Internal Affairs of Georgia
- **Giorgi Pirveli**, Investigator, Cyber Crime Unit of the Central Criminal Police Department, Ministry of Internal Affairs of Georgia
- **Shalva Kvinikhidze**, Head of International Relations Department, Ministry of Internal Affairs of Georgia
- **Mariam Gogoreliani**, Prosecutor, Chief Prosecutor's Office of Georgia, Department of Procedural Guidance of Investigation in the General Inspection Department of the Central Criminal Police and Department of the Patrol Police of the Ministry of Internal Affairs of Georgia
- **Giorgi Ghibradze**, Deputy Director of the National Center for Crisis Management, State Security and Crisis Management Council of Georgia
- **Giorgi Tielidze**, Senior Advisor, Department of Internal Security and Public Order, State Security and Crisis Management Council of Georgia
- **Irakli Gvenetadze**, Chairman, Data Exchange Agency, Ministry of Justice of Georgia
- **Nata Goderdzishvili**, Head of Legal Division, Data Exchange Agency, Ministry of Justice of Georgia
- **Irakli Lomidze**, Head of the Division of Information Security and Policy, Data Exchange Agency, Ministry of Justice of Georgia
- **David Kvatadze**, Head of CERT.GOV.GE, Data Exchange Agency, Ministry of Justice of Georgia
- **Andria Gotsiridze**, Head of Cyber Security Bureau, Ministry of Defence of Georgia
- **Jemal Vashakidze**, Deputy Head of Communications, IT and Innovations Department, Ministry of Economy and Sustainable Development of Georgia
- **Ramaz Kvatadze**, Executive Director, Georgian Research and Educational Networking Association (GRENA)

- **David Tabatadze**, Senior CERT officer and Products Manager, GRENA
- **David Lee**, President, Magticom
- **Zurab Akhvlediani**, Former Head of Information Security Group, TBC Bank
- **Irakli Kandaria**, Head of IT, APM Terminals, Poti
- **Nino Sarishvili**, Head of International Relations and Communications Department, Of fice of the Personal Data Protection Inspector

DISCLAIMER

The views expressed in this report are those of the author, not necessarily those of the National Crime Agency, British Embassy in Georgia or Her Majesty's Government.

SPECIAL THANKS

The author would like to express a note of special thanks to Dr. Christopher Joyce and Mr. Christopher Goff for their support, patience and counsel throughout this writing.

EXECUTIVE SUMMARY

Since so many of us have moved so much of our lives online, it is unsurprising that the dark side of social existence has moved with us—drugs, gambling, prostitution, pornography, senseless hooliganism and more. Georgia, despite its unique characteristics, is no exception to this worldwide phenomenon.

According to a recent United Nations International Telecommunication Union survey, the percentage of Georgians using the Internet in 2014 was 49%. As of October 2014, the number of mobile Internet subscriptions were 1.88 million. There are no Georgian national statistics available for E-Commerce or online banking penetration. However, anecdotally, it is clear that more Georgians have credit and debit cards, delivery of online purchases is becoming easier and every major bank offers online banking. Consequently, Georgia must prepare itself for increases in online financial crime that will surely accompany its economic and electronic development.

A paper prepared for the British Home Office offers a useful dichotomy to help understand cybercrimes: cyber-dependent crime and cyber-enabled crime. Meanwhile, the Americans think in terms of a trichotomy, adding the category of computer incidental. In such cases, the use of a computer may have been peripheral to the actual crime.

Statistics provided by the Cyber Crime Division (CCD) of the Central Criminal Police Department showed that in 2014 there were about 200 registered cybercrime cases. Although Georgia is a small country, and despite the likely underreporting, incidences of cybercrime seem quite low. Moreover, three things should strike the reader about this list. First, the cybercrimes known to have been committed in Georgia are not particularly creative. Second, they are not technologically sophisticated. Third, they do not involve very high stakes. However, depending on developments in other countries and in Georgia, cybercrime at home could become more sophisticated.

In addition to cybercrime, cyber espionage and cyber war have become fixtures of the virtual landscape, and Georgia has been no exception. One must understand that most Georgian officials place a higher priority on combating cyber espionage and cyber war than they do on fighting cybercrime. Since 2008, Georgia has implemented many steps and advanced its capabilities for cyber security. However, much more should be done in this respect, and cy-

bersecurity is still seen as one among many routine matters by all except those directly charged with securing the country's cyber space.

An interim revision of Georgia's Cyber Strategy and Action Plan is expected in 2015. It should be rewritten with clear, specific and measurable objectives. Georgia has continued to review its laws and it plans to amend laws to bring greater clarity and conformity with the European Convention on Cyber Crime. This requires a nearly perpetual process of review and amendment. Two issues arise in connection with this process. The first is achieving a true government-industry partnership. The second challenge is creating the trained professionals who will be needed to implement the lawfully.

Coordinating the various agencies of the Georgian government now falls to the Council for State Security and Crisis Management, which is subordinated directly to the prime minister. Since the recent constitutional reforms, this is where real political power lies. One of the major players in the Georgian government is the Ministry of Justice, specifically its Data Exchange Agency (DEA), which also runs the Georgian CERT. Another major player is Ministry of Internal Affairs, specifically the CCD. DEA and CCD are staffed adequately, not abundantly, for today, but not for tomorrow. A major problem is the dearth of well-trained computer professionals in the country.

Clearly, since 2008, Georgia has taken significant steps in enhancing cybersecurity. The glass is more than half full. Nonetheless, addressing the crucial problems successfully calls for implementation of a deliberate, consistent cyber policy, prioritized at the state level. Moreover, cybersecurity and cybercrime are truly global issues, so coping with these challenge also requires closer international cooperation and cooperation with like-minded countries.

Based on the observations in this paper, the recommendations are offered in bullet form on pages 61-66.

INTRODUCTION - THE WORLDWIDE CONTEXT

The marriage of the electronic programmable computer and widely available Internet over the last 20 to 25 years has changed the world as perhaps no other technology before it. Worldwide use of Internet technologies is growing by leaps and bounds. For example, in little more than the seven years since the Russia-Georgia war, worldwide Internet use has nearly doubled, both in absolute terms and as a percentage of the population. According to Internet World Stats, more than three billion people, 45% of the world, today use the Internet.[1] Between 2006 and 2012, available bandwidth climbed from 6.7 Terabytes per second (Tbps)[2] to 92.1 Tbps. The projection is that numbers will reach about 607 Tbps in 2018 and about 1100 Tbps in 2020.[3] In other words, more people are doing more on the Internet.

Just about every industry, government and military is run by Internet-connected computers. This affords unprecedented efficiency, convenience and opportunity. The Internet contributes to economic prosperity and growth, quality of life, access to information, social connection and political connection. Governments, for example, can offer information and services online, as well as manage crises. For those who use the Internet, it soon grows to be essential.

The rapid Internet growth also creates new vulnerabilities. Now, countries must deal with new, more efficient threats coming from cyber space. As the NATO strategic concept points out, "Cyber-attacks are becoming more frequent, more organized and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."[4] This is true for a NATO partner country like Georgia as well.

Since so many of us have moved so much of our lives online, it is unsurprising that the dark side of social existence has moved with us - drugs, gambling, prostitution, pornography, senseless hooliganism and more. Here is a list of some of the types of crimes committed online:

- Hacking, that is, exploiting a vulnerability to gain unauthorized access to a computer or computer network for a variety of purposes that compromise the confidentiality, integrity or availability of data.
- Spreading malware, again for a variety of purposes that compromise the confidentiality, integrity or availability of data.
- Distributed denial of service attacks (DDoS), which overwhelm a website or network to prevent its owner or authorized user from using the system for its intended purpose.
- Theft of personal data, which can, in turn, be used to steal or extort money.
- Circumvention of laws, for example, selling controlled drugs directly to online consumers.
- Fraud, including phishing e-mails, E-commerce scams, gaining access to banking information by deceit, etc.
- Child pornography, in particular, possession and distribution of sexual images of minors; however, also extending to recruitment and grooming of minors for the purpose of sexual exploitation.
- Cyber-stalking/bullying.
- Cyber-vandalism, defacement or other alteration of data for political or other purposes, or even for sheer hooliganism.
- Cyber-espionage. Espionage is illegal in just about every country, although in most countries, counterintelligence is a blend of law enforcement and national security.

A paper prepared for the British Home Office offers a useful dichotomy to help understand cybercrimes: cyber-dependent crime and cyber-enabled crime. "Cyber-dependent crimes," the study says, " are offences that can only be committed by using a computer, computer networks, or other forms of ICT." Such crimes include hacking, malware or DDoS attacks.[5] Cyber-dependent crimes are the same as target cybercrimes, a term used more often in the United States.[6]

Cyber-enabled crimes, the Home Office study says, "Are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT."[7] Theft, fraud and sexual exploitation, for example, are as old as humanity, but computers afford new avenues for their pursuit. One might say that because of their reach and efficiency, computers even magnify the effect of these crimes. Cyber-enabled crimes are the same as tool cybercrimes, the American term.[8]

This British dichotomy is very useful to understand what is going on in the world of cybercrime. However, it also underscores the potential for a records-keeping system to underreport cyber-enabled crimes, introducing statistical error with regard to the incidence of cybercrime, thereby depriving future investigators of case knowledge that could prove useful. To address this problem, the City of London Police, which is the leading British law enforcement authority for economic crime, and the National Fraud Intelligence Bureau have created the website, Action Fraud.[9]

"Action Fraud," says the Home Office report, "captures reports from the public and business on these crimes and classifies them in a way which allows distinctions to be made between computer misuse, online fraud and offline fraud. Action Fraud also assesses them against the provisions of the law and the requirements of [the Home Office Counting Rules] (HOCR). Where a report falls short of being recorded as a crime under HOCR, Action Fraud has the facility to record it as an incident for intelligence and information purposes."[10] The initial assessment of Action Fraud is that it renders a much fuller picture of cybercrime than had been possible with the traditional reporting and recording system.

Meanwhile, the Americans think in terms of a trichotomy, adding the category of computer incidental. In such cases, the use of a computer may have been peripheral to the actual crime.[11] For example, a computer may store a drug dealer's client list or it may be used to research information needed to commit a crime. As computers become more prevalent, their incidental use in just about any kind of crime increases.

Indeed, all three types of cybercrime are on the rise, and matters are made even more complex by the burgeoning variety of Internet-connected computers. In its December 2013 report, Gartner, a leading Internet research firm, writes, "Users continue to move away from the traditional PC (notebooks and desk-based) as it becomes more of a shared content creation tool, while the greater flexibility of tablets, hybrids and lighter notebooks address users' increasingly different demands."[12]

This year, *EMarketer* estimates, there will be over 1.91 billion smartphone users. This statistic is magnified by the fact that, to some extent, smartphones are shared. In, 2016, 2.16 billion people will connect to the Internet via smartphone.[13] Just as crime followed people online, it is following their migration toward mobile devices.[14]

Of course, cybercrime is not only a function of Internet and smartphone penetration. Financial cybercrime, for example, also depends on disposable income, credit card use, E-Commerce penetration, ease of conducting business online, availability of online banking and no doubt some other similar factors.

EMarketer projects business-to-consumer E-Commerce to reach $1.6 trillion this year and $2.5 trillion in 2018. China tops the list by virtue of sheer volume; however, it falls considerably lower on a measure of E-Commerce penetration, that is, the percentage of the population that has made an online purchase. In this case, the United Kingdom, Germany and Japan top the list.[15]

Interestingly, the United States, which has a higher per capita GDP than the UK, falls quite low on lists of E-Commerce penetration. For example, its E-Commerce penetration is about half of Britain's. This underscores that there must be a variety of sociological factors in play in addition to basic econometric indicators. Since cybercrime is correlated with activities like E-Commerce and online banking, this observation also underscores the difficulty of interpolating its costs from global estimates to national ones.

With E-Commerce valued at $1.6 trillion, rising rapidly to $2.5 trillion, and so much more to steal via the Internet, cybercrime is rampant. Regrettably, it is difficult to cite a valid monetary cost to cybercrime. Studies by several well-respected organizations differ widely. There are differences in the definitions of cybercrime and in the methodologies applied to the numbers. There is also a difficulty in determining the true cost of certain cybercrimes. For example, how does one place a monetary value on one state's theft of another's advanced weapons systems designs? Moreover, incidents tend to be underreported due to lack of awareness, concern for reputation, national security and no doubt other reasons. Finally, responses to surveys are subject to self-selection bias.

Nonetheless, a number of organizations try their best to come up with some kind of an estimated monetary cost to cybercrime. *The 2013 Norton Report*, for example, places the value of cybercrime at $113 billion, up from $110 billion in 2012.[16] A very complex econometric approach employed by

McAfee and the Washington-based Center for Strategic and International Studies (CSIS) is much more cautious. "A precise single figure for the cost of cybercrime and cyber espionage is unattainable," the McAfee-CSIS authors write, "but a more accurate estimate of the range of potential losses can be developed." The range they suggest for further research is $80 billion to $400 billion, a wide range, although not one inconsistent with the Norton findings. To conduct the further research, the McAfee-CSIS team suggests four questions.[17]

- Can "tolerated cost" analogies of sufficient accuracy be developed to let us estimate the costs of cybercrime? One proxy of possible interest starts from the proposition that the implicit cost-benefit analysis of "tolerated costs" may be skewed by immediate gratification in the context of computer adoption.
- Is the illicit acquisition of technology through cyber means a significant technology gain for the attackers that poses long-term costs to the victim economy, or does hacking produce only marginal changes in economic activity by both victim and attacker (noting that the effect on individual companies may be ruinous)?
- Do companies discount the cost as a normal part of business, or are they unaware of the real scale of loss and damage?
- Is dollar cost for losses an accurate measure of the effect of cyber espionage and cybercrime, or does this undervalue intangible costs, including trust in the international system or the effect on military power?

During the year that followed the publication of this study, the authors of the McAfee-CSIS report made some progress along the lines they had suggested. Their 2014 study estimates annual range between $375 billion to $575 billion. Although some progress had been made toward calculating accurate figures, the authors were, nonetheless, unable to close the gap. Here is their description of the costs and benefits of the three methodologies applied.

> If we used the loss by high-income countries to extrapolate a global figure, this would give us a global total of $575 billion. Another approach would be to take the total amount for all countries where we could find open source data and use it to extrapolate global costs. This would give us a total global cost of around $375 billion. A third approach would be to aggregate costs as a share of regional incomes to get a global total. This would give us an estimate of $445 billion. None of these approaches are satisfactory, but until reporting and data collection improve, they provide a way to estimate the global cost of cybercrime and cyberespionage.[18]

Apart from their intrinsic interest, these questions are reported here to underscore two fundamental points. First, calculation of cybercrime costs is very complex and, in the end, a single dollar figure may not be the most instructive measure. Second, the answers to these questions are liable to involve some cultural assumptions that are skewed toward the larger world economies. This will render any attempt to interpolate the global numbers to arrive at a cost figure for a smaller, less developed country nearly meaningless.

The Ponemon Institute, which is sponsored by Hewlett Packard, takes a different approach to determining the cost of cybercrime. Rather than attempting to measure a total global or even national value, Ponemon surveys a sample of companies in certain countries. The new 2014 study was conducted in the United States, United Kingdom, Germany, Australia, Japan, France and, for the first time, the Russian Federation, with a total benchmark sample of 257 organizations.

The new report shows significant variation in total cybercrime costs among participating companies in the benchmark samples. The US sample reports the highest total average cost at $12.7 million and the Russian sample reports the lowest total average cost at $3.3 million. It is also interesting to note that all six countries (except Russia) experienced a net increase in the cost of cybercrime over the past year - ranging from 2.7 percent for Japan to 22.7 percent for the United Kingdom. The percentage net change between FY 2014 and FY 2013[19] (excluding Russia) is 10.4 percent.

Cybercrimes continue to be on the rise for organizations. Ponemon found that the mean annualized cost for 257 benchmarked organizations is $7.6 million per year, with a range from $0.5 million to $61 million per company each year.

Ponemon observes a 10.4 percent net change from last year (excluding the Russian sample).[20]

"The evidence suggests that things are getting worse instead of better, despite all the resources that companies are spending on cybercrime," said Larry Ponemon, the Institute's chairman.[21] The variety of attack types from country to country also argues against interpolation of global or developed country figures to individual less-developed countries.

There is no disagreement that world cybercrime is substantial and growing. Moreover, though there will be as many national variations as nations, no country is immune. Computer security companies have created an industry out of issuing reports about trends in cybercrime. Regrettably, most of them have something new to report..

The new 2015 EMC white paper reports on four new trends. One trend is that the cybercrime-as a-service marketplace is going to mature and go as far as offering free trials, money back guarantees and discount for repeat service. Another trend is the mobile threat. The report says, "Given the rate of smartphone adoption around the world, we're seeing more focus on mobile threats and fraud than ever before."The report points out that there will be increased attack attempts against mobile payment systems. Another trend that might be expected is more large-scale retail and banking breaches, as cybercriminals seek more efficient and profitable types of attack. Moreover, the EMC report says, "APTs and similar attacks by nation states are likely to ramp up with regional conflicts driving the perpetrators and their victim selection. Criminal groups will also continue to adopt nation-state tactics."[22]

Just as the substantial growth of smartphones and other devices has contributed to the growth in cybercrime, so will the phenomenon of the Internet of things (IoT). With the introduction of the IPv6 Internet Protocol and advances in computer science and miniaturization, a whole new array of monitorable - and, therefore, penetrable - computer devices is being introduced. In the context of the IoT, a thing is anything that can be assigned an IP address, and IPv6 affords a huge increase in IP addresses.[23] Things include heart monitors, biochips, in-car computers, home or office thermostats, smart appliances and more. The IoT will afford opportunities for remote refrigerator repair, tracking of farm animals and near real-time monitoring of vital signs. The advantages are enormous, however, so are the chances for more cyber malfeasance. There has already been one reported instance of a smartTV, an audio speaker and a refrigerator corralled into a roboted

network (botnet) to send out spam messages.[24] This challenge is already looming in the more developed countries and, though in Tbilisi it may still appear remote, it is likely to appear in Georgia sooner than many think. In addition to expanding the opportunities for larger-and-larger botnets, IoT crime also raises the specter of boutique crimes like hacking into pace makers and in-car computers.

Meanwhile, just as every aspect of crime and human vice has followed the online rush, so have two other activities that have characterized human existence for ages - espionage and warfare.

Not a week goes by without a revelation of some new cyber espionage vector. One recent item in the news is Snake-Uroburos-Turla, which is connected to the crisis in Ukraine. Although reported in the popular press as some kind of cyber-attack in the swirl of events surrounding Euromaidan, the flight of former President Viktor Yanukovych and the Russian takeover of Crimea, Snake is really a long-standing, multi-functional espionage platform that has targeted primarily Ukraine and Lithuania. Even more interestingly, Kaspersky Lab soon revealed that Snake-Uroburos-Turla is related to Agent.btz, an earlier highly effective espionage worm. Agent.btz was so effective that it took American experts over a year to clean it from US government computer networks in a 2008 operation known as Buckshot Yankee.[25]

Espionage is a type crime and it is alive and growing in cyberspace.

THE VIEW FROM GEORGIA

Country Data for Georgia

Population: About 4.5 million people

Capital: Tbilisi, with about 1.2 million people

GDP: (nominal value from IMF) US$ 16.5 billion

GDP per capita: (nominal values from IMF) US$ 3,700

GDP growth: 4.8%

URL for the e-government portal: www. my.gov.ge

World Economic Forum Networked Readiness Index (NRI) ranking: 60th out of 148 economies

UN E-government Survey Ranking: 56th out of 193 member states

ICT USE

According to the World Economic Forum's 2015 *Global Information Technology Report*, Georgia ranked 60th in 2014 out of 148 countries in the Network Readiness Index (NRI).[26] Compared to the 2013 report, Georgia gained 5 positions.[27] The NRI measures the preparedness of an economy to use ICT to boost competitiveness and well-being. In particular, it measures the existing conditions for the development of ICT infrastructure; business and regulatory environment; innovation and competition levels; impact on economic development; readiness of the citizens, business circles and governmental organizations; level of utilization and production of information technologies in the country.

According to a United Nations International Telecommunication Union (ITU) survey, the percentage of Georgians using the Internet in 2014 was 49%.[28] In this respect, a more detailed analysis was made by the Georgian National Communications Commission report in 2014.

That report shows that as of the end of 2014, there are more than 100 ISPs and 603,000 Internet subscribers.[29] The top two ISPs in Georgia by subscribers are:

- Silknet: 234,542
- Caucasus Online: 156,458

In this report, the number of fixed broadband internet subscribers at the end of 2014 was 603,000, up by 14.4% compared to the end of 2013 number of subscribers, which was 527,000. Among these, fiber-optic technology subscriptions were about 52.2%, DSL 34.9%, WiFi 11.5% and WiMax technology subscriptions 1.2%. All other technology subscriptions amounted to 0.1%.

In order to achieve higher levels of Internet connectivity in the regions beyond the capital, development of mobile Internet may be one way. In this regard, as of October 2014, the number of mobile Internet subscriptions were 1.88 million. In this respect, the market is dominated by three mobile companies: Magticom, which holds about 43% of market share; Geocell, with 34%; and Mobitel with 23%.[30] Mobile Internet technologies are currently 2G, 3G and 4G, however, LTE was introduced in 2015 by these companies.

E-COMMERCE AND ONLINE BANKING

With regard to E-Commerce and online banking, understandably, Georgia does not figure into any of the top-country lists. A simple comparison of Georgia's per capita GDP with those of the countries that top the charts reveals why.[31]

COUNTRY	2014 GDP PER CAPITA IN US$
Georgia	$3,700
Canada	$50,300
Germany	$48,600
Netherlands	$52,000
United Kingdom	$46,000

Nonetheless, Georgia follows the trends of the more developed world and its GDP per capita is rising. Again, taking 2008, the year of the Russia-Georgia war, as a benchmark, Georgia's GDP per capita has increased by 28%.[32]

There are no Georgian national statistics available for E-Commerce or online banking penetration. However, anecdotal evidence suggests that these, too, are increasing. More Georgians have credit and debit cards, delivery of online purchases is becoming easier (although still not easy) and every major bank offers online banking. Consequently, Georgia must prepare itself for the increases in online financial crime that will surely accompany its economic and commercial development.

SOURCES OF INFORMATION

According to the US National Democratic Institute's September 2015 survey, *Public Attitudes in Georgia,* the Internet is perceived as the second most reliable source from which to receive information on political, social and current developments in the country. According to the report, television remains the main source of information for 87% of people; the Internet was named sec-

ond as a source of information.[33] Social media is one of the major Internet sources of information and a platform for political discussions. Facebook is particularly popular with over 1.22million registered users.[34] Social networks serve as an important platform for discussion and information exchange in Georgian society.

E-GOVERNMENT

E-government in Georgia is interpreted as "implementation of public functions through information and communication technologies." E- Government plays an important role in the process of reforming the public sector.

State bodies have stepped up their use of the Internet. For example, departments in the Ministry of Justice, the Ministry of Finance's Revenue Service, the Service Agency of the Ministry of Internal Affairs and others have developed online services that allow citizens to register and receive services, apply for identification cards or file applications. Furthermore, several state services are entering the mobile apps market. For example, the Georgian Police have created an app on which users can check important information or pay fines associated with traffic tickets.[35]

According to a 2014 UN E-Government survey ranking, Georgia placed 56th, gaining 16 positions in two years.[36] The E-Government Development index incorporates access characteristics, such as the infrastructure and educational levels, to reflect how a country is using information technologies to promote access and inclusion of its people. The measurement of E-government is an assessment of a state's use of the Internet and the World Wide Web for delivery of information, products and services, plus the level of telecommunication and human capital infrastructure development in a country.[37]

The Data Exchange Agency of the Ministry of Justice of Georgia and the EU Twinning project, "A Digital Georgia: E-Georgia Strategy and Action Plan 2014-2018," aim to promote a sophisticated ICT environment in the country. The proposed actions take into account already started initiatives and strategies. The E-Georgia strategy is, however, not limited to activities covered under the term E-Government. Instead, it has a broader scope, tackling related fields of innovation to create a prosperous environment for an innovative business sector and an innovative civil society. The role of government is to stimulate innovation in public, private and civil sectors to ensure economic sustainable growth.

The document underlines priorities such as development of E-Services, E-Participation and open government; E-Health; Public Finance Management System; E-Business; ICT-Hub Georgia; Infrastructure; E-Security; Enabling frameworks and governance; and awareness. The document states that Georgia is in a good starting position as there is a high political commitment to ICT development.[38]

With regard to the E-Georgia strategy, the 2014 UN *E-Government Survey* points out that Georgia not only advanced itself in terms of E-government, but also in terms of E-participation. A large gap between the availability of E-service (i.e. supply) and its actual use (i.e. demand and take-up) of the services shrank immensely during the last two years. Based on a scale upon which the top country, the Netherlands, scores 1.0, Georgia has moved from 0.21 to 0.59 in two years.[39]

ICT AND ECONOMIC DEVELOPMENT

Georgia's growing dependence on ICT benefits not only the modernization of government and society but also economic growth. Moreover, Georgia offers an attractive field for investment in ICT. In 2014, the Ministry of Economy and Sustainable Development's long-term strategy in ICT and innovation for 2020 set the goal of moving Georgia into the top 10 countries in the world in terms by improving the Network Readiness Index. According to an EU Commission-sponsored report, the ICT sector in Georgia contributes about 7% to the national GDP, which is relatively high compared to selected benchmarks in the region.[40] The ICT sector brings relatively higher wages, a drive for more training and a multiplier effect, as other businesses benefit from online advertising and E-Commerce.

CYBER CRIME

Georgia began compiling official statistics on cybercrime from 2014. The Information-Analytical Department of the Ministry of Internal Affairs (MIA) of Georgia is in charge of insuring accurate recording. Although, there are no official statistics for 2013, members of the CCD of the Central Criminal Police Department (CCPD) told the author that in 2013, they had investigated about 35 cybercrimes that they considered to be serious. There were many other incidents, they said, that they deemed to be less than serious, attributed to "script-kiddies" and the like. (Script-kiddie is a derogatory term employed by some more sophisticated hackers to describe the less skilled who follow step-by-step instructions, or scripts, to carry out their exploits.)

What follow are unpublished statistics on cybercrime in 2014 and the first half of 2015. They are presented here courtesy of the Ministry of Internal Affairs (MIA). The first table, below, shows the numbers of registered and closed (resolved) cybercrimes during 2014 and the first part of 2015 by the MIA territorial and structural units under articles 284-286 of the Criminal Code. Article 284 is illegal access to a computer system; 285 is misuse of a computer system or/and creation, usage, and dissemination of malicious computer programs; 286 is computer system interference or/and computer data corruption, modification and deletion.[41]

Registered cybercrime by the MIA territorial and structural units under articles 284, 285, 286 of the Criminal Code

Time Period	Articles 284-286		Article 284		Article 285		Article 286	
	Total	Closed	Total	Closed	Total	Closed	Total	Closed
Year of 2014	163	69	144	62	12	7	7	0
Year of 2015 (First six months)	79	22	70	22	3	0	6	0

The second table, below, shows the quantity of registered and closed (resolved) cybercrimes by the MIA Central Criminal Police Department under the Criminal Code of Georgia.

Registered cybercrime by the MIA Central Criminal Police Department under articles 284, 285,286 of the Criminal Code								
	Articles 284-286		Article 284		Article 285		Article 286	
Time Period	Total	Closed	Total	Closed	Total	Closed	Total	Closed
Year of 2014	43	5	33	3	5	2	5	0
Year of 2015 (First six months)	25	0	17	0	2	0	6	0

The third table, below, indicates the registered and closed (resolved) cybercrimes by both the MIA territorial and structural units and the MIA Central Criminal Police Department under Article 255 of the Criminal Code, which is offering to provide child pornography in any form or/and illegal creation and dissemination of pornographic materials.[42]

Registered cybercrime under article 255 of the Criminal Code				
	Year of 2014		First half of 2015	
	Total registered	Closed	Total registered	Closed
Registered by the MIA territorial and structural units	9	2	1	1
Registered by the MIA Central Criminal Police Department (Among which)	8	2	1	1

According to MIA, during 2014 and first six months of 2015, cybercrime under the article 255.1 is not recorded. Article 255.1 of the Criminal Code covers involvement and engagement of a minor in creation and sale of pornographic products or products of a pornographic nature.[43]

MIA was unable to provide cybercrime statistics for cases under Article 180, which is fraud, that is, unlawful appropriation of property or property rights through deception; Article189, which is infringement of copyright or related rights or under Article 210, which is forgery, sale, use, abuse of credit cards or other payment cards. The reason for this is that MIA only recently began to keep statistics and they are still working out of an accurate methodology for reporting. Investigations under Article 324.1 of the Criminal Code, which is cyberterrorism, are the responsibility of the Counterterrorism Center of the State Security Service, formerly part of MIA.

The numbers and characterizations offered by the MIA likely reflect some underreporting, which may be due to a combination of four factors. First, there is a very low level of cybercrime awareness among the Georgian public and among government officials not directly charged with cybersecurity. For example, news on cyberattacks is a leading topic in the worldwide press. In contrast, there is very little news or discussion about this in Georgia. A consequence of this general lack of awareness is that some Georgians may have sustained losses to cybercrime without knowing how they have been victimized. Second, since some Georgian banks are willing to reimburse small account-holders for losses, there may be no perceived need to report such cases to the police in many cases. Third, although cyber-dependent crimes are difficult to mischaracterize, cyber-enabled crimes can easily be characterized as, say, fraud or theft. As volume increases, some better reporting and recording system will be needed. Finally, although private companies are required by law to report certain crimes, there is no mechanism to check whether they do report, or even to aggregate and report on the information that is received.

Understanding that there may be more cybercrime beneath the surface of what the MIA is able to provide, a look at the cases allows us to sketch the nature of cybercrime in Georgia. The following cases are offered toward that end.

- **Malware.** A suspect was accused of illegally producing and distributing malware that compromised the integrity and availability of information on the sites droni.ge, presa.ge and news.ge.

- **Hacking online gambling.** A suspect allegedly hacked into eleven Adjarabet user accounts, diverting a total of 3,900 GEL to his own account. In another case, the hacker illegally accessed Europabet accounts and diverted 3,300 GEL.

- **Hacking a government computer.** A Georgian minor hacked into the Civil Service Bureau network, compromising availability of data for two days.

- **Cyber Hooliganism:** Hackers have posted animated images and text that said that a cyberattack was carried out on the website of the Office of the State Minister for Reconciliation and Civic Equality.

- **Hacking Paybox.** A hacker gained access to the computer system of Novateknolojis, which operates the www.paybox.ge payment system, compromising the integrity of data, thereby diverting over 500,000 GEL.

- **Credit card cloning.** Two Georgians and six Ukrainians cloned 1,137 plastic cards from British banks to credit £170,000 (620,000 GEL) into 45 Internet casino accounts.

- **Hacking and blackmail.** Latvian hackers allegedly compromised the confidentiality of a bank's computer system to steal personal data, and then contacted the bank's CEO to demand money in exchange for not releasing the stolen details.

- **Child pornography.** Interpol informed the CCD of an attempt to sell an exploitative image of a minor on a Georgian server. The perpetrator emerged to be the child's mother.

- **Botnet.** In conjunction with the MIA's Operative Technical Department, the CCD investigated a botnet with 3,000 roboted nodes.

- **Cyber espionage.** According to a 2014 report on APT 28 from the American company FireEye, among many governments of western countries, Georgian government websites and officials were among this group's targets.
- **SIM box fraud.** Fraudsters installed SIM boxes to terminate international calls at local telephone numbers, causing these calls to appear as local calls. A total of 95,000 GEL worth of damage was inflicted.

According to a MIA representatives, this last type of crime has been a new trend in Georgian cyber space.

Although Georgia is a small country, and despite the likely underreporting, incidences of cybercrime still seem quite low. Moreover, three things should strike the reader about this list. First, the cybercrimes known to have been committed in Georgia are not particularly creative. Second, they are not technologically sophisticated. (That said, MIA officials do report anecdotally something of an increase in the creativity and sophistication of cybercrimes. Also, this comment does not apply to, say, the sophistication of cyberespionage directed against Georgia.) Third, they do not involve very high stakes - the upper limit seems to have been about 620,000 GEL (£170,000); most of the crimes appear to involve a few thousand Laris.

The dangers of interpolating a total cost of cybercrime in Georgia from global numbers that are, in themselves, questionable has already been pointed out. However, with just over 200 registered cases in 2014 in Georgia, the best way to estimate the cost of cybercrime may be fairly straightforward—tote up the losses from about 200 cases. This does not account for the value of intangible factors, but none of the methodologies does.

MIA observations reflecting a low incidence of cybercrime appear to be reflected in the approach of privately-owned critical infrastructure. Banks, mobile telephone service providers and ports diligently carry out security best practices. However, they appear to be motivated more by international standards, investor expectations or fear of politically motivated cyber-attacks than by perceptions of rampant cybercrime. One CEO remarked that he was unaware of any attempt at unauthorized penetration of his company's computer systems.

There is no reason to believe that Georgians are any more or less honest than other nations. Moreover, Georgia enjoys a 100% literacy rate[44] and, like Russia and Ukraine, it suffers from the Soviet heritage of high capacity alongside low expectations for normal employment. With nearly half the country connected to the Internet, one would expect more cybercrime.

A possible explanation, which could only be confirmed with further research, is that a combination of low potential payoff, Georgia's unique language and more attractive options elsewhere has suppressed cybercrime in Georgia. In other words, it may be that there are talented Georgian cybercriminals, however, in addition to Georgian, they speak Russian and English and, therefore, they can easily practice their trade against more lucrative targets. This would leave the Georgian cybercrime market open to "script-kiddies" and the few that are sufficiently talented or lucky to rise a step or two above that level.

If one draws an analogy with other areas of crime, Georgian cybercriminals may work in the sphere of Russian-speaking organized crime. In other areas of crime, Georgian criminal organizations - *lavrushniki* or thieves-in-law - operate throughout Eurasia as part of this sphere.[45]

CYBER ESPIONAGE AND CYBER WAR

Regrettably, as noted in the worldwide section, above, crime is not at the edge of the dark side of online activity. Cyber espionage and cyber war have become fixtures of the virtual landscape, and Georgia has been no exception. Indeed, Georgia has been one of the loci for both cyber espionage and cyber war. At first glance one might assume that cyber espionage and cyber war rest apart from cybercrime. However, in the Georgian case at least, one must understand all three together for three reasons.

First, espionage is a crime, the cyber aspects of which could involve cyber-dependent or cyber-enabled crimes. Moreover, much of what may be called cyber warfare - if we exclude malware such as Stuxnet that can actually do physical damage - could be the same as the criminal act of gaining unauthorized access to a computer network for the purpose of degrading confidentiality, integrity or availability. The act could be the same until one attributes it to a foreign power or group undertaking it for strategic purposes. For example, a foreign power could access the computer system of an electricity supplier, transportation operator or cellular telephone service for the purpose of creating chaos, demoralizing the population or even preparing the battlefield for a kinetic attack. The initial act, however, would simply be unauthorized access to a computer system. Detection, defense and remediation would involve many of the same people and organizations, whatever the ultimate aim of the intrusion emerges to be.

Second, given Georgia's geopolitical position and recent experience, most Georgian officials place a higher priority on combating cyber espionage and cyber war than they do on fighting cybercrime. This can be gleaned from a reading of official documents such as the *National Security Concept of Georgia*, as well as from conversations with key officials. Countries seeking to cooperate with Georgia should understand Georgia's approach and the reasons behind it.

Third, one need not enter into the discussion of whether a nation-state was involved to recognize that Georgia has been the target of cyber espionage and cyber-attacks attributed to Russian cyber-criminals. It is directly relevant to any examination of cybercrime that there is a group - or groups - of Russian cyber-criminals that hones its skills and sustains itself on crime and then deploys its talents against Georgia for political motives.

CYBER ESPIONAGE

On October, 2014, US cybersecurity firm FireEye released an intelligence report suggesting that an advanced persistent threat (APT) group may be sponsored by the Russian government. The report, *APT 28: A Window into Russia's Cyber Espionage Operations*, detailed the exploits of a threat group known as APT 28 that, since at least 2007, has run a systematic, sophisticated campaign to collect "intelligence that would only be useful to a government" against targets in the United States, other East European countries, NATO, the Organization for Security and Co-operation in Europe and the government of Georgia." According to the report, the type of operations "indicate a government sponsor - specifically a government based in Moscow."[46]

The Georgian CERT's success at detecting and reverse-engineering the multipurpose espionage Trojan known as Georbot further illustrates the cyber espionage threat to Georgia. The following is a synopsis of a Georgian CERT report.[47]

Georbot exploited vulnerabilities in Windows-based computers in Georgia from early 2011. Initially, Georbot was spread by "watering-hole" style infections. The perpetrator infected some Georgian news portals with the Trojan. Any user who visited those sites and entered any one of a list of defense and security-related search terms - NATO, CIA, FBI, intelligence, FSB, general, colonel, etc. - was infected. After Georbot was discovered by the Georgian CERT and communication to its command-and-control servers was blocked, the Trojan was propagated by spam E-Mails.

Once executed, Georbot fully controlled infected computers. It was able to perform video and audio captures using a PC's own cameras and microphones; take screenshots; steal documents; send any files from the local hard drive to the remote command and control servers; scan local networks to identify other hosts on the same network and execute adversary commands on the infected system. Infected computers totaled 390, of which 70% were from Georgia.

The Georgian CERT identified all Georgian infected IPs and gave mitigation strategies and cleaning tools to infected agencies, institutions and individuals. Assisted by the law enforcement agencies of like-minded countries, the CERT obtained log files and system images for forensic analysis. The Georgian CERT worked also with Microsoft, ESET, Snort, Cisco and various blacklists and block lists to create mitigating tools and signatures. It gained full access to command and control servers, decrypted communication mechanisms and malicious files.

The final step was to create a document that mentioned NATO. Knowing that it would be stolen, they infected it with the Trojan. The author received the stolen file and opened it, thereby infecting his computer and opening the backdoor to the same spyware that he had used on his victims. After controlling the perpetrator's computer, the Georgian CERT was able to obtain the hacker's posting on a Russian hacker's forum in which he sought help in exploit development. The hacker's nickname is "Eshkinkot1." The CERT was able to take pictures of him. He is a known hacker operating in Russia.

In sum, Georbot was an information stealing Trojan that was used to target Georgian individuals, government and critical information subjects.

CYBER WAR

In 2008, Georgia was the first country to sustain combined kinetic and cyber-attacks. After a year of study, the U.S. Cyber Consequences Unit (US-CCU), an independent research institute, reported, "Many of the attacks were so close in time to the corresponding military operations that there had to be close cooperation between people in the Russian military and civilian cyber-attack." The US-CCU report indicates that most of the botnets used against Georgia had already been used for criminal activities. A number of American computer security researchers who track botnets said they saw clear evidence of the involvement of Russian Business Network (RBN), a cyber-criminal syndicate.[48] The Cyber-attacks disrupted the Georgian government's information and communication efforts, news portals, financial transactions and Internet traffic for several days.

Another tool used was web postings of instructions to individuals with limited computer skills who could contribute to the cyber-attack efforts. The web-site postings were so productive that forty-three targeted websites were effectively shut down or defaced, in addition to the eleven targeted by the botnets associated with organized crime. Social networks and websites such as stopgeorgia.ru and stopgeorgia.info were used to recruit and prepare such hackers for action. These sites were hosted on servers in the US, Germany and Latvia with already established ties to organized crime, particularly to RBN.[49]

SECURITIZATION AND HOW GEORGIA VIEWS CYBERCRIME, CYBER ESPIONAGE AND CYBER WAR

The concept of securitization offers a benchmark for how intensely nations perceive security issues. The concept of securitization was employed by Arnold Wolfers in 1952[50] and Barry Buzan in 1997.[51] It is the process by which a country deals with a threat outside normal channels, that is, not as a technical or legal matter, but as an existential threat warranting extraordinary attention. Nuclear deterrence in the Cold War and the war on terrorism, particularly as waged by the United States after September 11, 2001, are prime examples.

Despite Georgia's experience in 2008, and despite the fact that cyber threats are perceived as one of the main threats to Georgia's national security, this problem has not yet been fully securitized. It is still seen as one of many challenges, dealt with by legislation, bureaucracies and budget cycles.

In contrast, Estonia placed extraordinary emphasis on cyber security. For one thing, Estonian President Toomas Hendrik Ilves talks about cyber security all the time.[52] Moreover, Estonia has taken a very visible, pro-active role, hosting the NATO Cooperative Cyber Defence Centre of Excellence and forming an Estonian Cyber Defence League.

The 2008 Russian attack on Georgia thrust this country into the forefront of Internet policy and, since 2008, Georgia has implemented many steps and advanced its capabilities for cyber security. However, much more should be done in this respect and cybersecurity is still seen as one among many routine matters by all except those directly charged with securing the country's cyber space.

One consequence of this is that though official statements and documents assign high priority to cyber security, budgets have not matched declaratory policy. In turn, insufficient budgets account for the "elephant in the room" factor that was evident in most conversations with government officials: too many Georgian government computer systems are running pirated/unlicensed software. Replacing all the government's computers would cost a lot of money and, said one interlocutor, the senior leadership simply does not understand the issue. According to the Software Alliance BSA, *Global Software*

Survey of 2014, which rated countries and values of unlicensed PC software installation, Georgia had very high rate of 90% unlicensed software. This constitutes a significant commercial value of nearly 40 million.[53]

According to a 2014 Eurasia Partnership Foundation report, pirated software is widespread in both the public and private sectors. The report says that in central and local government, among about 30,000 personal computers, about 70% are run by unlicensed or pirated software. According to the National Intellectual Property Center Sakpatenti, in 2013-2014, negotiations were held between the Georgian government and the Microsoft on this issue, with a view toward introduction of licensed software in government agencies.[54] In this regard, one government representative told the author that the main obstacle in this respect is available financial resources.

The protection of intellectual property rights (IPR) is closely related, and very important to Georgia's development in ICT and beyond. Georgia has brought its IPR legislation into line with international standards. The Georgian National Intellectual Property Center - Sakpatenti - is the agency formulating and implementing IPR-related policies. Georgia has ratified a number of international conventions related to IPR, and, in 2014, new amendments to IPR laws on trademarks, patents, designs, copyrights and related rights were drafted in order further to harmonize Georgian legislation with EU standards. All that said, in relative terms, IPR has not been a high priority for most of the government and enforcement standards must be raised.

In sum, taking stock of what has been done since 2008, reading the emphasis placed on cyber security and speaking with government officials, one certainly gets the sense that cyber security is a high priority in Georgia, even if it falls a step below the securitization one sees in Estonia. That said, beyond the government cyber security community, there is insufficient understanding and, therefore, insufficient funding to fix some major problems.

Moreover, beyond the people charged with combating cybercrime - primarily the CCD - concern for cybercrime in Georgia is a step below concern over politically motivated attacks. Regrettably, this is reflected in the attention given the subject by prosecutors and the judiciary.

STAKEHOLDERS

In the online world, there are three types of stakeholders: government, private and individuals. Although traditional discussions of security tend to focus on government, cybersecurity considerably shifts the focus to business. Businesses are stakeholders in three important ways. First, private business owns much of the infrastructure that is critical to the efficient functioning of society and, therefore, to its security. Second, business is the engine that can transform ICT potential into economic development. Third, businesses are consumers of ICT services. Finally, we must not forget the individual Internet user. The direct nature of the Internet means that each of the 2.18 million[55] Georgian Internet users is tied to this vast system of systems in a way unprecedented in more traditional societal pursuits. Nonetheless, though 1.22 million Georgians use Facebook, understanding of the Internet, computers and cyber security remains low.

GOVERNMENT

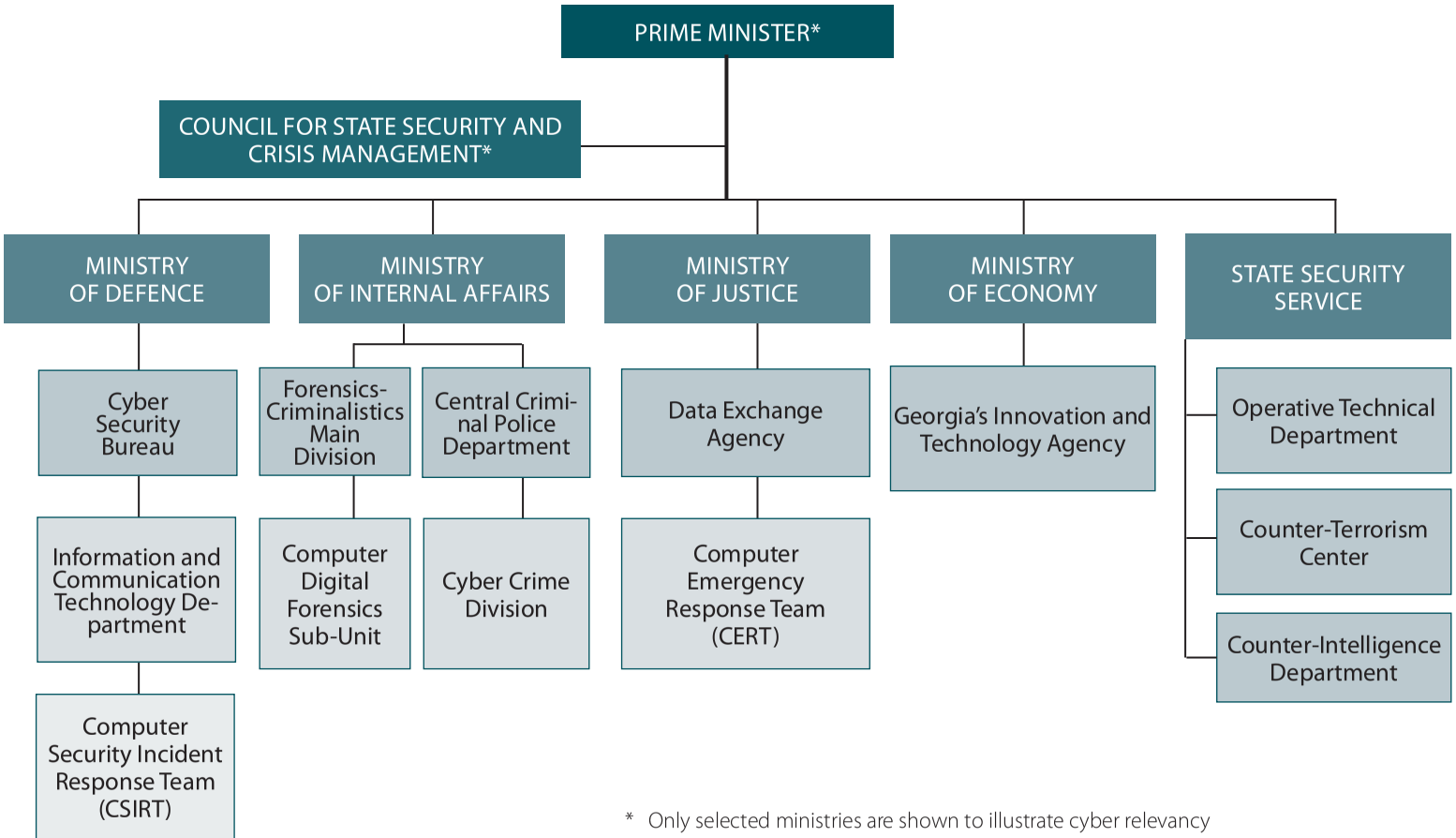
COUNCIL FOR STATE SECURITY AND CRISIS MANAGEMENT-OFFICE OF THE PRIME MINISTER

Inter-agency coordination of Georgian government cybersecurity had been a function of the National Security Council, subordinate to the president. Due to constitutional changes, however, this function has shifted to the office of the prime minister. The Council for State Security and Crisis Management, often simply referred to as the National Security Council or the other National Security Council, now coordinates the various agencies. The council is an advisory board for Prime Minister Irakli Garibashvili and is directly subordinated to him. Accordingly, the Prime Minister is the head of the Council.

The council is composed of the following permanent members: Secretary of the Council, Minister of Internal Affairs, Minister of Defense, Minister of Foreign Affairs and Minister of Finance.[56]

The council coordinated the government's activities of updating the Law on Information Security and defining the lists of critical information system subjects. The council is also responsible to coordinate the ongoing update of the Cyber Security Strategy. The main challenge of the council is to achieve effective inter-agency coordination.

The chart below shows the Georgian government organizations responsible for cyber and information security.



* Only selected ministries are shown to illustrate cyber relevancy
* The Council has an inter-agency coordinating role

MINISTRY OF JUSTICE - DATA EXCHANGE AGENCY - CERT

The principal government organization responsible for non-military cybersecurity in Georgia is the Data Exchange Agency (DEA). DEA is a Legal Entity of Public Law, subordinated to the Ministry of Justice. It began operations in January 2010. The agency's core functions are development of E-Government, creation and development of data exchange infrastructure, information security in cyberspace, increased awareness, setting ICT standards for the public sector and elaborating information security policies.

DEA twice a year also runs Cyber Security Forum, which brings together the public and private sectors on a voluntary basis. The mission of the forum is to discuss and exchange ideas related to information and cybersecurity.

An important part of the agency's mandate is information security for public sector critical information system subjects. This function includes:

- Conducting awareness raising activities among critical information system subjects, the rest of the government, local IT businesses and the general population.
- Supporting government agencies in adopting and implementing information security policies.
- Developing state-wide standards and procedures for information security through legislation and regulations (based on ISO 27000).
- Delivering initial training courses on information security to government officials representing critical information system subjects.
- Directing Georgia's Computer Emergency Response Team (CERT). The CERT started its operation in January 2011 inside DEA. Its main functions are:
    - Responding to cyber incidents upon request
    - Monitoring Georgian cyberspace and analyzing cyber resources for vulnerabilities
    - Providing penetration test service on the basis of written contracts

- Providing IP monitoring services for identification of malicious traffic
- Conducting static source code analysis services
- Black listing service
- Web-site intrusion detection systems – (Threat Factor)
- Conducting malware analysis
- Providing training in incident handling to critical information system subject representatives

The DEA has completed large-scale projects of information security policy development and implementation at the Ministry of Justice, Ministry of Economy and Sustainable Development, Ministry of Health, Labor and Social Affairs and the Parliament of Georgia. Similar projects are ongoing in other ministries.

Cyber incidents on critical information system subjects are dealt by DEA. In 2014, through the newly launched cyber incident management system (OTRS), DEA detected 350 incidents in critical information system subjects. All detected incidents were handled by the CERT.[57]

The Georgian CERT identifies and responds to each incident, including prevention and mitigation of consequences. Whether these acts are legally assessed as cyberterrorism, a crime of sabotage or cybercrime is a separate matter that is to be decided by the relevant law enforcement entities, which have investigative jurisdiction over such offences.

In carrying out its functions, the CERT cooperates with a wide range of international partners. Among them are Shadow Service, Team Cymru, Arbor Networks, Network Security Incident Exchange, Quarantine Net and Clean MX. As a result of this cooperation and its own efforts, in a typical month, the CERT shuts down an average of 20 phishing sites, helps with 25-30 defaced websites and deals with 30-35 malware sites located in Georgian cyberspace.

The Georgian CERT obtained the right to use the trademark "CERT" officially in 2014. It is also a member of the following organizations:

- International Telecommunication Union 2011
- FIRST - the international confederation of trusted computer incident response teams (2013)
- Trusted Introducer - the trusted backbone of the security and incident response team community in Europe (2012)

CERT.gov.ge is planning to become a member of European Government CERTs group (ENISA).

With regard to personnel, it should be noted that DEA has four Certified Information Security Managers (CISM) and two Certified Information System Auditors (CISA).

DEA has also developed an extensive network of international contacts and developed a large international outreach program. One measure of the international respect that DEA has garnered for Georgia is the growth of the Georgian ICT Development and Cyber Security Event - GITI - which will hold its eighth iteration this November in Tbilisi. The purpose of the GITI conference is to describe the significance of information technology in terms of creating an engine of growth for socio-economic development of the region.

Another example is a recently begun project sponsored by NATO's Science for Peace and Security Program. Recognizing that infrastructure protection and responses to cyber incidents can serve to benefit all neighbors in the Black Sea and South Caucasus region, cyber defense experts and government representatives took part in a workshop in Tbilisi, from 29 June to 1 July, 2015 to discuss options for increased cooperation. The initiative aims to improve regional cooperation by creating trust, information sharing and developing common cyber defense measures.[58] A follow-on meeting was held in Kvareli on October 8, 2015.

MINISTRY OF INTERNAL AFFAIRS - CENTRAL CRIMINAL POLICE DEPARTMENT

The Ministry of Internal Affairs (MIA) of Georgia is responsible for law enforcement, including cybercrime law enforcement. This activity is carried out by the Central Criminal Police Department (CCPD), which created its Cyber Crime Division (CCD) in December 2012. The CCD was created within the framework of the European Convention on Cyber Crime, which requires member states to establish special units to investigate cases of cybercrime. Currently, the CCD has 15 staff members. It is divided into two sub-divisions, the Technological Research and Integration and the Anti-pornographic and Illegal Content sub-divisions. It also serves as Georgia's 24/7 international contact point.

The MIA has also established the Special Sub-unit for Computer-Digital Forensics within the Forensics-Criminalistics Main Division. This sub-unit is the first handler of digital forensic evidence. The Operative Technical Department, which served as the MIA CERT and was used in case of necessity in the cybercrime investigation process, was moved to the newly created State Security Service. Another alternative, in case of necessity, is the Levan Samkharauli National Forensics Bureau, a legal entity of public law subordinate to the MIA. Computer forensics is among the many services rendered by this bureau.

The MIA has elaborated the document, *Standard Operating Procedures for Handling Digital Evidence*. These procedures specify the technical rules that are to be used in seizing and examining digital evidence. This document is now in the process of interagency discussion.

With regard to capacity-building, the MIA Academy has developed training modules for national first responders and cybercrime police investigators. The training modules cover the following issues:

- Cybercrime case studies
- Search and seizure of electronic evidence
- Legal aspects of cybercrime
- Types of cyber-attacks.

MIA has also started an active cybercrime awareness campaign. In 2014, under the framework of its public awareness campaign, it created a short film series called Identification. The first series was devoted to cybercrime issues. The project was funded by the US Embassy in Georgia.

The MIA actively cooperates with an array of European law enforcement agencies, as well as with the US Federal Bureau of Investigation (FBI) in handling cybercrime cases.

In 2014, the MIA signed a memorandum of understanding with National Crime Agency of the United Kingdom on cooperation, including on cybercrime, in the context of the fight against organized crime.

Furthermore, the MIA has sought to build capacity through international cooperation. For example, between 2011 and 2014, it participated in the Council of Europe's project for the Eastern Partnership countries, "Cooperation against Cybercrime." The objective of this program was to strengthen the capacities of the criminal justice authorities of Georgia for effective cooperation against cybercrime.[59] The MIA also participated in a bilateral project with Estonia to enhance the capacities of Georgian MIA units. This program ended in 2013; however, there are plans to resume it. In 2013, under the aegis of the US Embassy and the FBI, training on cybercrime issues was held in the Police Academy. In 2014, study visits on organized crime and various forms of cybercrime were carried out in France, Germany, Poland and the UK. MIA representatives participated in various training courses that helped to increase their qualification in fighting cybercrime.

CDD representatives mentioned that as cybercriminals become more sophisticated, it becomes harder to fight them. "To fight them effectively requires improving technical abilities. To obtain a high qualification in this field requires high level technical training." In particular, CDD representatives expressed interest in assistance and training in best western practices in tactics, techniques and procedures (TTPs) of legal forensic investigation and analysis, rules of evidence and effective case preparation, including international requests for information, assistance and extradition.

STATE SECURITY SERVICE OF GEORGIA

In July 2015, by order of Georgian government, the State Security Service of Georgia was established. The main functions of this agency are to protect constitutional order, sovereignty, territorial integrity and military potential of the country from illegal actions of foreign special services and individuals; to discover attempts at changing the government unconstitutionally; to ensure the country's economic security; to fight against terrorism; to fight against transnational and international crime; to fight against corruption; and to protect state secrets.

In sum, the new agency decoupled the intelligence and security functions from Georgia's MIA. The Counterterrorist Center, Counter Intelligence Department, State Security Agency, Anti-Corruption Agency, Special Operations Department, and Operative Technical Department moved under umbrella of the State Security Service.[60] The Operative Technical Department is responsible for the implementation of covert investigative activities, for example, under the Article 143.1, which are telephone call eavesdropping and recording and extraction of information from communications channels based on legally established procedures. Nonetheless, moving the Operative Technical Department to the State Security Service does not exclude MIA's right to conduct covert investigative activities.

PROSECUTORS AND THE JUDICIARY

Of course, for a law enforcement system to work, efficient policing is insufficient; prosecutors and courts must be part of the equation. Regrettably, it appears that Georgian prosecutors and court officials are not keeping pace with cyber technology.

This has created some concern in both DEA and the CCD. According to CCD representatives, prosecutors and judges lack understanding of cyber cases. They claim that there have been several cases in which, despite solid evidence and evidence procedures, "the final verdict was far from appropriate because of their lack of understanding of the case."

To address this shortcoming, DEA offered training for prosecutors in March 2014. The training was about what is cyber space, cyber security and cyber law.

About 10 representatives from the prosecutor's office attended. Nonetheless, one official still laments, "There were cases in which some of the representatives from the prosecutor's office dropped the training course because it was too complicated for them. This is the main gap that should be filled." This appears to be the major Achilles Heel in Georgia's efforts to combat cybercrime. A representative of the Prosecutor's Office mentioned to the author that in some cases it is hard to process cyber cases as fully understanding the technical sides of those cases can be somewhat challenging.

MINISTRY OF DEFENCE

On December 24, 2013 the Georgian Parliament amended the Law on Information Security to create the Cyber Security Bureau (CSB), a legal entity of public law inside of Ministry of Defence of Georgia.[61] The Bureau was created in February 2014. Later the same year, the list of critical information subjects in the defense sector was created. The amended law also says that in the defense field, approval of the list of critical information system subjects lies with the Georgian government. The list was developed by the Ministry of Justice in coordination with the Ministries of Defense and Interior was approved by the Prime Minister of Georgia.

The new list of critical information system subjects in defense filed was created in September 29, 2014 by the government order # number 567.[62] The list contains the following:

1. Ministry of Defence of Georgia (MOD)
2. Military Hospital of the MOD, LEPL
3. Cadets Military Lyceum of the MOD, LEPL
4. National Defense Academy of MOD, LEPL
5. Cyber Security Bureau of MOD, LEPL

The main mission of the organization is to ensure security of information and communications in the defense field, identifying emerging and potential risks in cyber space and methods for timely prevention. The CSB is actively working to improve the relevant legislative framework to harmonize it with in-

ternational standards. The CSB's pertinent information security policy should meet the minimum requirements established by ISO and ISACA. Cooperation with international organizations, partner countries and other government agencies of Georgian government are among the responsibilities that bureau must meet. The CSB operates the Computer Security Incident Response Team (CSIRT) and the Computer Security Incident Response Coordination Center. (CSIRT/CC).

MINISTRY OF ECONOMY AND SUSTAINABLE DEVELOPMENT

The purpose of the Ministry of Economy's program Innovative Georgia 2020 is to develop the Georgian economy by utilizing ICT technologies. One specific goal of Innovative Georgia 2020 is to advance Georgia's position in information and communication indexes by 2020. To achieve this, Georgia's Innovation and Technology Agency was created to turn Georgia into an ICT regional hub, to encourage the spread of high-speed Internet infrastructure across the country and to create techno-parks, IT incubators and innovative laboratories.

Meanwhile, the European Bank for Reconstruction and Development (EBRD) and the Government of Finland cooperate with the Ministry of Economy and the Georgian National Communications Commission on the program Georgia: Information and Communications Policy and Regulation Development. The main aim of the program is to prepare complex project documentation for information and communications policies in Georgia. With the help of EBRD experts, the documents, *Digital Broadcasting Transition Policy* and *Legislative Action Plan for Digital Broadcasting* were prepared.

At the behest of the Ministry of Economy, major reforms have been conducted in Georgian electronic communication networks such as a national numbering system for telephone codes.

Although the Ministry of Economy's objectives are all laudable, these could be made more precise, accompanied by strict metrics to measure progress.

GEORGIAN NATIONAL COMMUNICATIONS COMMISSION

The Georgian National Communications Commission (GNCC) regulates Internet Service Providers (ISP), including their security arrangements. The GNCC could wield its considerable power to enhance cybersecurity. For example, the GNCC could provide a cybersecurity communication platform between ISPs, on the one hand, and the CCD and CERT Georgia, on the other. Apart from cooperation mechanisms, the GNCC has regulatory authority that could be used to help improve cybersecurity by setting a voluntary code of practice or even mandatory rules for ISPs, asking that they maintain a system for notifying infected computers, keeping up-to-date threat information, providing resources for end users, and establishing a reporting mechanism to inform the government about severe cyber security threats. ISPs could take advantage of both information asymmetry and economies of scale to provide more security at a lower cost, particularly for individual Internet users and small businesses. This would have positive effects on the development of Georgian cyber space.

OFFICE OF THE PERSONAL DATA PROTECTION INSPECTOR

The office of the Personal Data Protection Inspector was established in July 2013 on the basis of the Georgian Law on the Personal Data Protection that came into force in May 2012.[63] The main purpose of the law is to process personal data in such a way that the rights, freedoms and privacy of individuals are protected. According to the law, the Personal Data Protection Inspector is responsible for supervising the implementation of data protection legislation, monitoring and enforcing this law, providing instructions to the public and the private sector about how to ensure adequate protection of personal data, reviewing data-related complaints and appeals, inspecting public and private entities to ensure that the data processing is carried out in compliance with the law and raising public awareness on the protection of personal data.

Furthermore, the Personal Data Inspector has the right to inspect the lawfulness of data processing by the private sector upon his or her initiative. If the inspector detects violations, he or she can request that any deficiencies be eliminated or request temporary or permanent termination of data processing, blocking, deletion, destruction or depersonalization of data, termination of transmission of personal data, etc. Additionally, if the Inspector identifies an administrative offense, he or she is authorized to impose administrative liability on the information processor.

INTELLECTUAL PROPERTY RIGHTS ENFORCEMENT

The Georgian National Intellectual Property Center - Sakpatenti - is the agency that formulates and implements IPR related policies. It deals with all IP rights, including patents, copyrights and related rights, trademarks, new plant and animal varieties, etc. Another player in this respect is the Georgian Copyright Association.

GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION (GRENA)

GRENA is an organization of 14 people, in operation since 1999, that functions in the fields of education and training. Its projects are undertaken in cooperation with universities, with the support of the European Commission, NATO Science Program, Open Society Georgia Foundation and the International Science & Technology Center. As the oldest cybersecurity and training organization in Georgia, GRENA has built considerable respect for its expertise. In particular, GRENA played a key role in mitigating Russian cyber-attacks during the 2008 war.

Since 2004, GRENA has run the Cisco Regional Networking Academy, offering the following courses:

- Cisco Certified Network Associate (CCNA)
- CCNA Security
- Cisco Certified Network Professional (CCNP)

GRENA has a distance learning center that enables students to pass certification exams via Internet.

In its security role, GRENA has operated a two-person CERT for its member organizations since 2007. The CERT was established with the support of the NATO Science Program. It is a member of the European CERTs Trusted Introducer network and has close cooperation with organizations working on cybersecurity in many countries. The GRENA CERT offers the following services:

- Intrusion detection system that checks incoming and outgoing packets on networks.
- Incident coordination - investigation and resolution of incidents in cooperation with CERT teams from different countries.

- Dissemination of information about various threats.
- IP Monitoring and dissemination of information about cyber incidents on Georgian networks.

CRITICAL INFRASTRUCTURE

As examples of privately-owned critical infrastructure, the author interviewed representatives of a cellular and Internet service provider, a bank and a seaport.

- Magticom serves about 1.7 million cell phone users and about 700,000 mobile Internet subscribers as well as customers of a satellite broadcast system, which, among other customers, serves the 64 Justice Houses throughout Georgia.
- TBC Bank is a full-service commercial bank operating as a joint stock company. The bank serves about million customers. It is headquartered in Tbilisi, with most of its business in Georgia, although it has some interests in Azerbaijan and Israel.
- APM Terminals operates the Port of Poti. The company is headquartered in The Hague, although it is owned by the Danish Maersk Group. APM operates 64 terminals in 39 countries. Poti Port handles containers as well as break-bulk cargo with 15 berths with an aggregate length of 2,900 meters.

All three companies were well aware that their businesses comprise infrastructure that is critical to the security of Georgia and expressed no reluctance to work with the Georgian government. Nonetheless, their motivations for cybersecurity measures appeared to spring from good and sufficient business reasons of their own, including compliance with industry and international standards. In all three cases, the IT departments are responsible for cybersecurity.

The Port of Poti complies with ISO 9001-2000 standards. If APM can maintain efficiency and security, Poti could fulfill its capacity of 25 million tons of cargo

per year. The computer system that controls port functions is closed and based upon an uncommon operating system. Less critical systems are connected to the Internet and interface with Georgian Customs Service and four container lines. Given that they operate a closed system, the port's IT managers' main concern is insider threats. Accordingly, personnel security measures are in place. All company personnel must undergo a computer-based training program.

TBC Bank follows ISO and NIST standards. Moreover, having raised capital through an initial public offering (IPO) last June on the London Stock Exchange, it incurs further security requirements. However, officials pointed out that the IPO process can be a double-edged sword because it also requires considerable transparency to enable due diligence. Possible concerns include outsourcing of certain computer security functions, insider threats and limited staffing. Nonetheless, officials say they are confident of the integrity of their contractors and personnel security procedures are in place. Under-staffing is real, but cross-functioning is well planned, including coming together as a CERT, if necessary.

Magticom's security approach is comprehensive, bringing together physical security and cybersecurity. The company must comply with ITU standards, however, these are not particularly rigorous for cell phones. Magticom's system is closed and it does no outsourcing. The biggest concern is a physical threat to fiber optic cable. Looking forward, Magticom officials are also concerned about cybercrime aimed at over half million and growing smartphones in Georgia.

These thumbnails, of course, are nothing near a security audit to evaluate the cybersecurity situation in these three companies. Nor is there any indication that these companies are representative of others. Still, one comes away from them with a sense of having seen intelligent, dedicated people pressing forward on the challenges. Georgian government officials must not assume that privately-owned companies that operate critical infrastructure are doing nothing, absent legal compulsion.

A report should be prepared on the state of cybersecurity among privately owned companies that own critical infrastructure. Moreover, the government must find ways of communicating and working with industry.

CONCEPTS, LAWS AND PLANS

NATIONAL SECURITY CONCEPT

Given Georgia's 2008 experience, the authors of the new *National Security Concept* write:

> During the 2008 Russian-Georgian war, the Russian Federation conducted large-scale cyber-attacks, in parallel with the ground, air, and naval attacks. These attacks showed that the protection of cyberspace is as important for national security as land, maritime, and air defenses...The security of cyber space and the protection of electronic information is very important for Georgia. As information technologies rapidly evolve, critical infrastructure is becoming more dependent on them. Therefore, combating cybercrime and protecting against cyber-attacks is very important to the national interests of Georgia.[64]

The strategy points out the importance of cooperation with partner states for the country's cyber security.

CYBER SECURITY STRATEGY AND ACTION PLAN

The *Cyber Security Strategy and Action Plan* is under revision. The updated strategy and its action plan is expected by the end of the 2015. The new strategy is being developed by the Permanent Inter-agency Commission under the auspices of the Council for State Security and Crisis Management.

Meanwhile, the *Cyber Security Strategy and Action plan* for 2013-2015 was approved on May 17, 2013 by Presidential Order number 321. Georgia's cyber security strategy was evolved on the basis of *Georgia's Threat Assessment Document 2010-2013* and the *National Security Concept of Georgia*. The document was developed by the Permanent Inter-agency Commission tasked with coordination of drafting national security strategic documents, operating at the National Security Council of Georgia.

The strategy calls for the creation of cybersecurity system principles that will not only facilitate the protection of the information infrastructure against cyber threats, but will also help the socio-economic development of the country.

The strategy lists the following eight principles that are necessary to achieve better protected cyberspace: uniform government approach; government and private sector cooperation; research and analysis; new legislative and regulatory framework; institutional coordination for ensuring cyber security; public awareness; education and training and international cooperation.[65]

The challenge facing the new Council for State Security will be twofold: 1) achieving sufficient interagency coordination to achieve something concrete and 2) rewriting the strategy with clear, specific and measurable objectives.

THE EUROPEAN CONVENTION ON CYBER CRIME

On June 6, 2012, Georgia ratified the *European Convention on Cyber Crime*. The treaty, which Georgia signed in 2008, requires not only cross-border law enforcement cooperation, but also harmonization of certain laws pertaining to cybercrime. This took some time and ratification was impossible until Georgia passed its Law on Information Security. The European Convention entered into force for Georgia on October 1, 2012.[66]

During 2008 and 2009, the MIA was involved in the Council of Europe and European Commission's Joint Project on Cybercrime, which aimed to harmonize Georgian legislation with the Cybercrime Convention. Within the framework of the project, important amendments were incorporated in the Georgian Criminal Code and the Law on Criminal Procedure.

Georgia has continued to review its laws and plans to amend laws to bring greater clarity and conformity with the convention. This requires a nearly perpetual process of review and amendment. Like any country, Georgia must adapt its laws to a relatively new international agreement and adapt to new technology. However, having regained its independence almost two and a half decades ago, Georgia is still trying to modernize its entire legal system with practical experience and some foreign assistance.

LAW ON INFORMATION SECURITY

The Law on Information Security is applicable to legal persons and state agencies recognized as critical information system subjects. In 2014 – 2015, many amendments were made to the law. Accordingly, the new list of critical information system subjects and their categorization, including in the defense field,

shall be approved by an order of the Government of Georgia. The Ministry of Justice, in agreement with the Ministries of Defence and Internal Affairs and the State Security Service shall submit a draft order to the Government of Georgia for approval. Before this amendment, the list was defined by a decree of the President of Georgia, based upon a list developed by the National Security Council. Another amendment to the law created the Cyber Security Bureau (CSB) as a legal entity of public law under the supervision of Ministry of Defence of Georgia.

The law sets a number of obligations and requirements for critical information system subjects such as a duty to adopt information security policies compliant with the ISO 27000 and the standards set by the Information Security Audit and Control Association (ISACA). Those organizations that are on the list of critical information system subjects are also required to appoint information security officers and cyber security personnel. Moreover, they have a duty to conduct information asset management to categorize these assets in terms of their criticality. The law also authorizes critical information subjects to conduct information security audits, undergo penetration testing, and to add or install and manage a network sensor for the detection of cyber incidents. The law defines the competencies of the Georgian CERT as a national CERT and defines its interaction and exchange of data with owners of critical information systems.

The DEA does not have access to the critical information system subjects' information systems or information assets unless a subject voluntarily provides DEA access to these. A critical information system subject's information security manager must inform the CERT of computer incidents; however, it is up to the subject to decide whether to accept the CERT's assistance. The CERT would have no right to access a subject's data, without permission. Any legal entity or state agency that is not a critical information system subject may voluntarily implement information security mechanisms provided in the legislation. This law does not apply to mass media, publishing companies, scientific, educational, religious and community organizations or to political parties.[67]

The law is supplemented by a number of sub-normative acts that define and further develop the legal provisions for practical implementation. So far, there are seven orders on:

- Computer Emergency Response Team (CERT) of the Data Exchange Agency
- Approval of minimum standards for an information security officer of a critical information system subject
- Configuration of network sensors in the networks of the critical information system subjects
- Minimum requirements of information security
- Approval of rules for authorization of persons and organizations eligible to perform information security audits, authorization procedures and costs
- Rules for conducting an information security audit
- Approval of rules on information assets management

In case of the MoD Cyber Security Bureau there are three orders:

- Computer Security Incident Response Team (CSIRT)
- Minimal requirements of information security
- Rules for information asset management.

The CSB shall define requirements for critical information system subjects in the field of defense in accordance with the standards and requirements established by the ISO and ISACA.

The law was amended in order to strengthen the implementation of regulations that pertain to the protection of confidential and internal use information at the critical information system subjects.

The updated list of critical information system subjects was approved by Governmental Order number 312 on April 29 2014. It includes 39 organizations:[68]

1. Ministry of Justice
2. Ministry of Corrections
3. Ministry of Foreign Affairs
4. Ministry of Finance
5. Ministry of Internal Affairs
6. Ministry of Regional Development and Infrastructure
7. Ministry of Labor, Health and Social Affairs
8. Ministry of Economy and Sustainable Development
9. Parliament of Georgia
10. Administration of the President
11. Government Chancellery
12. National Bank
13. The Office of Chief Prosecutor of Georgia
14. Tbilisi City Hall
15. The Central Election Commission
16. SMART LOGIC, LEPL
17. State Procurement Agency, LEPL
18. Social Service Agency, LEPL
19. National Examination Center, LEPL
20. State Service Development Agency, LEPL
21. Financial and Analytical Service, LEPL
22. National Civil Registry Agency, LEPL
23. Revenue Service, LEPL
24. Financial Monitoring Service of Georgia, LEPL
25. State Regulatory Agency for Medical Activities, LEPL

26. National Center for Disease Control and Public Health, LEPL
27. Georgian Health Mediation Service, LEPL
28. Civil Aviation Agency, LEPL
29. Maritime Transport Agency, LEPL
30. Land Transport Agency, LEPL
31. Education Management Information System, LEPL
32. Georgian Railway, JSC
33. Sakaeronavigatsia, Ltd (air traffic control)
34. United Airports of Georgia, Ltd
35. National Center for Educational Quality Enhancement, LEPL
36. Border Police, MIA
37. Service Agency, MIA, LEPL
38. Service of "112" MIA, LEPL
39. National Environment Agency, LEPL

With its Law on Information Security, Georgia has conformed to the European Convention and achieved more than some other quite large democratic countries. That said, two issues arise in connection with this law. The first is achieving a true government-industry partnership. Most government officials assessed private business to be somewhat reluctant to cooperate. The second challenge is creating the trained professionals who will be needed to implement the law fully. One expert who asked not to be quoted said:

> There is no university in Georgia that is able to give a good education in computer science or cyber security. None of the existing universities has such capabilities here. Implementation of the information security law is a challenge - do we have enough cyber security personnel in the country to follow all the requirements that are written in the law? All defined organizations need at least 2-3 persons working the problem. Are we capable? We just don't have enough people.

CRIMINAL CODE

In Georgia, cybercrime issues are regulated by Chapters 25, 27, 32, 35, 38, of the Criminal Code, according to which, criminal responsibility is established for committing any of the following illegal actions in cyberspace:[69]

- Illegal access to a computer system (Art. 284)
- Misuse of a computer system or/and creation, usage, and dissemination of malicious computer programs (Art. 285)
- Computer system interference or/and computer data corruption, modification and deletion (Art. 286)
- Offering to provide child pornography in any form or/and illegal creation and dissemination of pornographic materials (Art. 255)
- Involvement and engagement of a minor in creation and sale of pornographic products or products of a pornographic nature (Art. 255.1)
- Infringement of copyright or related rights (Art. 189)
- Cyber terrorism (Art. 324.1)
- Forgery, sale, use, abuse of credit cards or other payment cards (Art.210)
- Fraud, that is, unlawful appropriation of property or property rights through deception (Art. 180)

Article 324 was amended in 2012 and articles 255 and 255.1 in 2013. Article 285 similarly was amended in 2014. In keeping with an ongoing review, the government plans further amendments to bring them into conformity with the European Convention. These amendments will be designed to bring greater clarity to existing law, bringing Georgian legislation closer to the standards set by the Convention.

STRATEGY ON COMBATING ORGANIZED CRIME

In 2013, the Ministry of Internal Affairs elaborated the draft *Strategy on Combatting Organized Crime*, with subchapter 1.3 on combating cybercrime. The strategy gives a general overview on cybercrime and already implemented initiatives. It outlines MIA's main goals for combating cybercrime: public awareness, periodic review of the legislative framework, capacity-building of the agencies involved in combating cybercrime, deepening cooperation between law enforcement agencies and the private sector and deepening cooperation with like-minded countries and international organizations like the OECD, EU, OSCE, NATO, UN/ITU and CoE. The strategy was approved by the Government of Georgia in October 2013.[70]

CHANGES IN THE LAWS ON ELECTRONIC SURVEILLANCE

In September 2014, new amendments to the Law on Data Protection went into force. These granted the Personal Data Inspector power to inspect and monitor data processing by law enforcement agencies, including the lawfulness of implementation of surveillance and interception during covert surveillance activities envisaged by Article 143.1(a) of the Criminal Procedure Code, which covers telephone call eavesdropping and recording.

Changes in the Data Protection Law triggered amendments in the Criminal Procedure Code, the Law on Electronic Communications and the Law on Operational Investigative Activities. These changes became the objects of thorough scrutiny by civil watchdogs.

According to the changes in Criminal Procedure Law on covert investigative activities, the process of covert tapping and recording of telephone conversations will be carried out under a two-stage electronic system that requires consent from law enforcement and the Personal Data Protection Inspector. The two-stage electronic system means that both law enforcement and the Personal Data Inspector will have the keys for direct access to the data of communication companies.[71]

Defenders of the amendment underline the fact, that although law enforcement officials will have access to a company's data immediately after court authorization, they will not be able to start tapping personal data without the Personal Data Protection Inspector's electronic consent.

Opponents argue that the so-called key should not be in hands of law enforcement but instead in hands of the electronic communications companies. In

response, a document entitled *Government Paper on the Non-Governmental Organization Coalition Report* points out that granting the key to the provider companies will make it very hard to control them. Furthermore, the key will grant them access to communications content. "Georgia is an occupied country and mobile operators are foreign residents," the government response says.[72]

The two-stage electronic consent system does not extend to obtaining data transmitted through the Internet. Regarding this issue, Transparency International (TI) writes that a law enforcement agency "retains the right to intercept and record unlimited amounts of information transmitted through Internet providers without any external oversight mechanism. In this case, the Personal Data Protection Inspector carries out the inspection only by comparing information provided by the court, the Prosecutor's Office and an electronic communications service provider and by verifying the legality of processing of data by a data processor/authorized person." TI points out that "Such oversight system has only a formal character because the law enforcement begins obtaining information from Internet providers without any external control. While carrying out the inspection, the Inspector relies on the good faith of the law enforcement body to provide accurate information."[73]

Transparency International also criticizes the provision in the Criminal Procedure Law regarding software. TI expresses its concern that "the software which is necessary for the functioning of the special electronic system will be created by law enforcement. That means that the law enforcement agency will create a system by which it will be controlled. This fact certainly contains a considerable risk that the software will be programmed in a way which will make it possible to obtain information bypassing the means of control."[74] This provision covers the article 143.1 (a) and (b) that are: [75]

(a) Telephone call eavesdropping and recording;

(b) Extraction of information from communications channels (communication facilities, computer networks, wired communications and station-level equipment of facilities), from computer systems (directly and/or remotely) and, for this purpose, installation of relevant software in computer systems.

Changes were also made in the Law on Electronic Communications. The law establishes legal and economic grounds for the pursuit of activities by means of electronic communications networks and facilities within the territory of Georgia, as well as principles for the development and regulation of the competitive environment in this sector. It also defines the functions of an independent national regulatory authority (the Georgian National Communications Commis-

sion), specifies the rights and obligations of natural persons and legal entities owning, using or providing services by means of electronic communications networks and facilities.[76]

According to the new amendment to the Law on Electronic Communications, adopted on November 30, 2014, if requested, electronic communications companies must have the technical ability in real time to provide communications content and identifiable data from their networks to the monitoring systems of authorized agencies. Electronic communications companies are also obliged to notify the Personal Data Protection Inspector of identifiable data provided to a law enforcement agency.[77]

According to further changes in the Law on Electronic Communications, an authorized agency may copy identifiable data from communications channels and store them for two years. An authorized agency can copy data without a judge's ruling or a prosecutor's decision. Authorization is only necessary to use the data.[78]

These provisions were heavily criticized by the Public Defender's Office as they give authority to law enforcement agencies to copy data without court approval.[79]

The state body authorized to conduct covert investigative activities under sub-articles (a) and (b) of Article 143.1 of the Criminal Procedure Code is the Operative Technical Department of the newly established State Security Service and the MIA.

According to the Law on Criminal Procedure, covert investigative activities can be conducted with court approval. However, in case of emergency, they can be authorized by a prosecutor when delay may cause destruction of important data or make it impossible to obtain the data. In such a case, within 24 hours, the prosecutor is obliged to seek judicial approval. The prosecutor must prove the legality of the urgent covert investigative activities. Thereafter, the court has 24 hours in which to make a decision.[80]

CONCLUSIONS AND RECOMMENDATIONS

In 2008, Georgia was jolted into the world of cybersecurity. The country did not react as resolutely as Estonia did, but it placed the matter solidly on the agenda. Clearly, since 2008, Georgia has taken significant steps in enhancing cybersecurity. The glass is more than half full. Nonetheless, addressing this crucial problem successfully calls for implementation of a deliberate, consistent cyber policy, prioritized at the state level. Georgia is trying to catch up to its European partners. There are two general hurdles to achieving this - lack of awareness and lack of resources. Meanwhile, for Georgia, as for the rest of the world, the volume and sophistication of threats is rapidly growing. Reports of crimes against a mobile devices will likely soon appear, opening up a whole new sphere of cybercrime.

DEA and CCD are staffed with intelligent, able and enthusiastic people. They are staffed adequately, although not abundantly, for today, but not for tomorrow. A major problem is the dearth of well-trained computer professionals in the country. The State Security Council is relatively new, but its leadership expresses the intention to make changes and coordinate the relevant agencies of the government. Moreover, this organization is close to the prime minister, which is where the constitutional changes have placed political power. Efforts to improve the cybersecurity situation in Georgia and to enlarge its constituency should begin with these three organizations and work outward.

Based on the observations in this paper, the following recommendations are offered. The top priority recommendations are summarized in the table, below.

- **Government organization and government relations with the private sector**
  - The new Council for State Security must become familiar with policies and best practices to develop policy, encourage buy-in and coordinate the activities of various government agencies.
  - Best practices in creating effective government-private sector partnerships must be brought to Georgia as a matter of high priority.

- The government must develop an effective and feasible plan to replace government computers as needed and install only genuine software. In replacing or installing new hardware, only products of trusted companies should be used. This will take time and money, but it simply must be done. The gravity of this matter must be communicated by all interlocutors.
    - The new hardware and software must feature appropriate security systems and it must be networked with an eye on security.

- **Review of policies and laws**
    - As State Security Council officials are aware, Georgia must update the Cyber Security Strategy and Action Plan with clear, specific and measurable objectives.
    - An ongoing mechanism must be established for Georgia to review its body of law regularly and methodically, to consult legal experts from partner countries, the Council of Europe and the European Union, and to submit to its parliament proposed amendments that adapt to changing technology and bring it ever closer to European standards.
    - A tension between the protection of constitutional rights and operational investigation requirements exists. Georgia needs assistance to develop appropriate judicial mechanisms to address this situation.
    - The Law on Information Security must be amended as soon as possible and the list of privately owned critical information system subjects must be developed, approved and published.
        - Meanwhile, an assessment of the cybersecurity practices of private sector critical information system subjects should be conducted.

- **Increasing awareness of cybersecurity and cybercrime - public, government, senior leadership**
  - Plan and implement a public awareness program to familiarize the Georgian public with cybercrime, threats to children, preventive measures and reporting procedures.
    - Consider best practices in other countries.
    - Consult media, schools and interested companies to develop the best ways to reach various publics.
  - Develop and deliver a simple computer hygiene course for all Georgian government employees.
  - Develop a series of short briefings and discussions on key topics for Georgia's senior leaders.

- **Cybercrime reporting mechanism**
  - After the public awareness program begins to have an impact, introduce a new cybercrime reporting mechanism, modeled on the British Action Fraud portal, adapted to Georgian needs.

- **Education and training**
  - Develop a program to assist and train MIA officials in best western practices in tactics, techniques and procedures (TTPs) of legal forensic investigation and analysis, rules of evidence and effective case preparation, including international requests for information, assistance and extradition. In this regard, it is important to note that MIA officials need to move beyond basic instruction to advanced levels of proficiency by western standards.
  - Develop programs with research institutes and universities to:

- Insure that those already working in the field have the knowledge and skills necessary to fulfill the roles required by the Law on Information Security of every critical information system subject.
- Recruit new professionals to the field with training that would qualify them to assume the positions required by the Law on Information Security.

- Develop a program with the MIA to train the first responders and Criminal Police on the basics of gathering and preserving the integrity of digital evidence and maintaining the chain of evidence.
- Design and deliver a cyber training program specifically for prosecutors and judges.
- Develop a series of seminars for CCD and DEA professionals on advanced topics like research on the deep web, anonymization and pro-active techniques to anticipate cybercrimes and cybercrime trends. Use learned techniques to study
  - Sophisticated cybercriminals.
  - Likely trends - worst case and best case - in Georgian cybercrime.
  - How to assist law enforcement agencies in like-minded nations.
- Work with CCD professionals on cybercrimes against mobile devices, the likely next big trend.
- Continue to develop systems to collect, aggregate, analyze and report statistics on cybercrime, adopting the best practices of western partners.

Summary of the Top Priority Recommendations for Georgia and Partner Countries

TITLE	RECOMMENDATION DETAIL
Best practices	Develop a government-wide cybersecurity best practices manual and accompanying training programs.
Government awareness	Develop and deliver a series of short briefings and discussions on key topics for Georgia's senior leaders. Develop and deliver a simple computer hygiene course for all Georgian government employees.
Legitimate computer software and hardware	Develop am effective and feasible plan and schedule to clean all Georgian Government computers and networks and install only properly licensed software, including operating system software, and to replace hardware, as necessary.
Cyber Security Strategy and Action Plan	The plan must be revised during 2015, as planned, accompanied by clear, specific and measurable objectives.
Legal consultation	Create an ongoing consultative mechanism between Georgia and its western partners to review cyber-related laws and to strengthen the protection of constitutional rights.
The judicial system	Design and deliver a cyber training program specifically for prosecutors and judges.
Privately owned critical information system subjects	The list of privately owned critical information system subjects must be developed, approved and published as soon as possible.

Assess cybersecurity in the private sector	Conduct a thorough assessment of the cybersecurity situation and practices in key components of the private sector.
Increase public awareness	Plan and implement a public awareness program to familiarize the Georgian public with cybercrime, threats to children, preventive measures and reporting procedures.
Develop MIA capacity	Develop and deliver a program to assist and train MIA officials in best western tactics, techniques and procedures (TTPs) of legal forensic investigation and analysis, rules of evidence and effective case preparation, including international requests for information, assistance and extradition.
First responders and police	Develop and deliver a program with the MIA to train the first responders and Criminal Police on the basics of gathering and preserving the integrity of digital evidence and maintaining the chain of evidence.

In all these endeavors, it is important to develop clear, attainable and measurable objectives. Georgia has learned how to gain knowledge from its partners and to cooperate with like-minded countries for mutual benefit. Cybersecurity and cybercrime are truly global issues, so coping with these challenge also requires closer international cooperation and cooperation with like-minded countries.

NOTES

1. *Internet Usage Statistics, The Internet Big Picture.* Internet World Stats. Retrieved from http://www.internetworldstats.com/stats.htm and Internet World Stats. *Internet Growth Statistics.* Retrieved from http://www.internetworldstats.com/emarketing.htm

2. 1 terabyte ≈1,000 gigabytes

3. Brodkin, John, *Bandwidth Explodes: As Internet Use Soars, Can Bottlenecks be Averted?* ArsTechnica. May 1, 2012.Retrieved from http://arstechnica.com/business/2012/05/bandwidth-explosion-as-internet-use-soars-can-bottlenecks-be-averted/

4. *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* NATO. November 2010. Retrieved from http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf

5. McGuire, Mike & Dowling, Samantha, *Cyber Crime: A Review of the Evidence*. United Kingdom, Home Office, October 2013. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

6. Brenner, Susan, *Cybercrime: Criminal Threats from Cyberspace.* Santa Barbara, California: Praeger, 2010

7. Mcguire & Dowling

8. Brenner

9. See the Action Fraud website at http://www.actionfraud.police.uk/about-us/who-we-are

10. McGuire & Dowling

11. Brenner

12. *Gartner Says Worldwide Traditional PC, Tablet, Ultra mobile and Mobile Phone Shipments On Pace to Grow 7.6 Percent in 2014.* Gartner.com. January 7, 2014. Retrieved from http://www.gartner.com/newsroom/id/2645115

13. *2 Billion Consumers Worldwide to Get Smart (phones) by 2016.* EMarketer.com. Retrieved from http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694

14. Mayer, Andre, *Smartphones Becoming Prime Target for Criminal Hackers.* CBC News. March 6, 2014. Retrieved from http://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126

15. *Retail Sales Worldwide Will Top $22 Trillion This Year.* EMarketer.com. December 23, 2014. Retrieved from, http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/1011765

16. *2013 Norton Report, Symantyec.com.* Retrieved from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

17. *The Economic Impact of Cybercrime and Cyber Espionage.* Center for Strategic and International Studies. July 2013.Retrieved from http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf

18. *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II.* Center for Strategic and International Studies. June, 2014. Retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

19. FY, an American fiscal year, runs from October 1 to September 30

20. *2014 Global Report on the Cost of Cyber Crime.* Ponemon Institute. October, 2014. Retrieved from https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

21. Ibid.

22. *CYBERCRIME 2015 An Inside Look at the Changing Threat Landscape.* EMC. Retrieved from http://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf

23. *Internet of Things (IoT)*. WhatIs.com. Retrieved from http://whatis.techtarget.com/definition/Internet-of-Things

24. Hu, Elise, *What Do You Do if your Refrigerator Begins Sending Malicious E Mails?*NPR—All Tech Considered. January 16, 2014.Retrieved from http://www.npr.org/blogs/alltechconsidered/2014/01/16/263111193/refrigerator-hacked-reveals-internet-of-things-security-gaps

25. Gostev, Alexander, *Agent.btz: A Source of Inspiration?* Kaspersky Lab SecureList. March 12, 2014. Retrieved from http://www.securelist.com/en/blog/8191/Agent_btz_a_source_of_inspiration

26. Dutta, Soumitra, Geiger, Thierry & Lanvin, Bruno. *The Global Information Technology Report 2015*. World Economic Forum.Retrieved from http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf

27. Dutta, Soumitra et.al., *The Global Information Technology Report 2013*. World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_GITR_Report_2014.pdf

28. *ICT Facts and Figures 2015*. International Telecommunications Union. Retrieved from: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

29. *2014 Annual Report*. Georgian National Telecommunications Commission. Undated. Retrieved from http://www.gncc.ge/uploads/other/1/1344.pdf

30. Ibid.

31. *GDP per Capita*. The World Bank. Undated. Retrieved from http://data.worldbank.org/indicator/NY.GDP.PCAP.CD

32. Ibid.

33. Thornton, Laura, *Public Attitudes in Georgia*. National Democratic Institute, 2015. Undated. Retrieved from https://www.ndi.org/files/NDI%20Georgia_April%202015%20Poll_Public%20Issues_ENG_VF_0.pdf

34. *January 2015 Facebook use in Armenia, Azerbaijan and Georgia* – according to Facebook. Katy Pearce. January, 2015. Retrieved from http://www.katypearce.net/january-2015-facebook-use-in-armenia-azerbaijan-and-georgia-according-to-facebook/

35. *Georgia: Freedom on the Net 2014*. Freedom House. Undated. Retrieved from https://freedomhouse.org/report/freedom-net/2014/georgia

36. *United Nations E-Government Survey 2014*. United Nations. Undated. Retrieved from http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Suvey/E-Gov_Complete_Survey-2014.pdf

37. Ibid.

38. Krabina, Bernhard, Liu, Po-Wen. *A Digital Georgia: e-Georgia strategy and action plan 2014-2018*. Undated. Retrieved from http://www.dea.gov.ge/uploads/eGeorgia%20Strategy.pdf

39. United Nations E-Government Survey 2014

40. *Georgia: ICT Environment, Innovation Policies &International Cooperation*. European Commission, EU- Eastern Europe and Central Asia. Undated. Retrieved from http://eeca-ict.eu/images/uploads/pdf/EECA_counires_reports_NEW/ICT-Env_Inno-policies_and_Inter-coop_report_GEORGIA.pdf

41. *Criminal Code of Georgia*. Legislative Herald of Georgia, 1999 (as amended). Retrieved from https://matsne.gov.ge/ka/document/view/16426

42. Ibid.

43. Ibid.

44. *Literacy Rate, Adult Total*. The World Bank. Undated. Retrieved from http://data.worldbank.org/indicator/SE.ADT.LITR.ZS

45. *Georgian Organized Crime Blitz in Europe*. In Moscow's Shadows. June 20, 2013. Retrieved from http://inmoscowsshadows.wordpress.com/2013/06/20/georgian-organized-crime-blitz-in-europe/

46. *APT28: A Window into Russia's Cyber Espionage Operations?* FireEye. October 27, 2014. Retrieved from https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html

47. Akhvlediani, Zurab, *Cyber Attacks on Georgian Government Resources*. Data Exchange Agency. May 29, 2012. Retrieved from http://www.slideshare.net/DataExchangeAgency/cyber-attacks-on-georgian-governmental-resources

48. *The US-CCU Report on the Georgian Cyber Campaign*. United States Cyber-Consequences Unit, US-CCU Special Report. August 2009.The full text is available at http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.Hereafter cited as US-CCU Report

49. Ibid.

50. Wolfers, Arnold, *National Security as an Ambiguous Symbol.* Political Science Quarterly 67(4), 1952

51. Buzan, Barry, *Rethinking Security After the Cold War*. Cooperation and Conflict (32), 1997

52. Stavrides, James, *My Interview with Cyber Expert, Estonian President Toomas Hendrik Ilves*. The Fletcher School. October 9, 2013.Retrieved from http://sites.tufts.edu/fletcherdean/my-interview-with-cyber-expert-estonian-president-toomas-hendrik-ilves/

53. *The Compliance Gap BSA Global Software Survey*. BSA. June 2014. Retrieved from http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf

54. *European Neighboring Policy Action Plan and Eastern Partnership Bilateral and Multilateral Guidelines and their Implementations in the Areas of Trade and Related Fields in Georgia*. European Partnership Foundation Report.January, 2014. Retrieved from http://www.epfound.ge/files/report_2013__geo.pdf

55. *Internet live stats*. Internet Users by country (2014). Retrieved from http://www.internetlivestats.com/internet-users-by-country/

56. *Approval of Regulations*. Council for State Security and Crisis Management. January, 2014.Retrieved from http://www.government.gov.ge/files/382_39895_502469_38060114.pdf

57. *2014 Annual Report*. Data Exchange Agency. Undated. Retrieved from http://www.dea.gov.ge/uploads/DEA_Anual_report_2014_Draft_v1_2.pdf

58. *Enhanced cyber Defence cooperation in the South Caucasus and Black Sea region*. NATO. July 29, 2015. Retrieved from http://www.nato.int/cps/en/natohq/news_121969.htm?selectedLocale=en

59. *Eastern Partnership - Cooperation against Cybercrime*. Ministry of Internal Affairs. Retrieved from http://police.ge/en/ministry/structure-and-offices/international-relations-department/donor-coordination/proeqtebis-shesakheb/ongoing-projects/eastern-partnership-cooperation-against-cybercrime

60. *Approval of the Statute of the State Security Service*. Legislative Herald of Georgia. July 30, 2015. Retrieved from https://matsne.gov.ge/ka/document/view/2930985

61. *Amendment to the Law on Information Security*. Legislative Herald of Georgia. December 24, 2013.Retrieved from https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2162943

62. *Governmental Order #567 on approval of the critical information system subjects list in Defense field*. Legislative Herald of Georgia. September 29, 2014. Retrieved from https://matsne.gov.ge/ka/document/view/2521602

63. *Georgian Law on Personal Data Protection*. Legislative Herald of Georgia. Consolidated version. July 8, 2015. Retrieved from https://matsne.gov.ge/en/document/view/1561437

64. *National Security Concept of Georgia*. Government of Georgia. MFA. Undated. Retrieved from http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx

65. *Cyber Security Strategy*. Legislative Herald of Georgia, May 17, 2013. Retrieved from https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1923932&lang=ge

66. *Convention on Cybercrime*. Council of Europe Treaty Office. Undated. Retrieved from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT= 185&CL=ENG

67. *Law of Georgia on Information Security*. Legislative Herald of Georgia. Retrieved from: https://matsne.gov.ge/en/document/view/1679424

68. *Governmental Order #312 on approval of the critical information system subjects list*. Legislative Herald of Georgia, April 24, 2014. Retrieved from https://matsne.gov.ge/ka/document/view/2333175

69. *Criminal Code of Georgia*. Legislative Herald of Georgia, 1999 (as amended). Retrieved from http://tcc.gov.ge/uploads/kanonebi/sisxlis_samartlis_kodeqsi.pdf

70. *National Strategy for Combating Organized Crime 2013-2014*. Police.ge. Undated. Retrieved from http://police.ge/files/OCC/Organized%20Crime%20Strategy-ENG.pdf

71. *Amendments to the Law on Criminal Procedure Code*. Legislative Herald of Georgia. November 30, 2014. Retrieved from https://matsne.gov.ge/ka/document/view/2593029#DOCUMENT:1

72. *Georgian Government Comments to the Non-Governmental Organization's Coalition Report*. Administration of the Government of Georgia. Undated. Retrieved from http://gov.ge/files/323_49254_692246_NGOs2YearProgressReport-CommentsAOG20.05.2015.pdf

73. *Nine threats to your personal life stemming from the new legislation on secret wiretapping,* Transparency International. December 23, 2014. Retrieved from http://www.transparency.ge/en/blog/nine-threats-your-personal-life-stemming-new-legislation-ons-secret-wiretapping

74. Ibid.

75. *Criminal Procedure Code*. Legislative Herald of Georgia. Consolidated version. September 29, 2015. Retrieved from https://matsne.gov.ge/ka/document/view/90034

76. *Georgian Law on Electronic Communications*. Georgian National Communications Commission. May 19, 2011. Retrieved from http://www.gncc.ge/ge/legal-acts/parliament/laws/saqartvelos-kanoni-eleqtronuli-komunikaciebis-shesaxeb-8082.page

77. *Amendments to the Law on Electronic Communications*. Legislative Herald of Georgia. October 31, 2014. Retrieved from https://matsne.gov.ge/ka/document/view/2457343

78. Ibid.

79. Tarkhnishvili, Nino, *Two "Keys" is Still Controversial*, Radio Liberty. March 31, 2015. Retrieved from http://www.radiotavisupleba.ge/content/ori-gasagebi-isev-sadavoa/26929588.html

80. *Criminal Procedure Code*. Legislative Herald of Georgia.