RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

MAIN STRATEGIC DIRECTIONS OF DEFENSE AGAINST DESTRUCTIVE RUSSIAN CYBER OPERATIONS

ANDRIA GOTSIRIDZE

123

EXPERT OPINION

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

ANDRIA GOTSIRIDZE

MAIN STRATEGIC DIRECTIONS OF DEFENSE AGAINST DESTRUCTIVE RUSSIAN CYBER OPERATIONS

123

2019

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN 978-9941-8-1239-2

Factors that need to be taken into account when formulating a new National Cyber Security Strategy. At the end of the second decade of the 21st century, cyber security is becoming more and more important as a part of state security. Political, military, social and criminal processes have mostly migrated to cyberspace. The cyber domain, the fifth area of confrontation, is constantly used for reaching political, economic or military goals. Well-developed cyber-attack potential enables many states, especially Russia, to successfully use cyberspace during wars, conflicts or peacetime to obtain geopolitical superiority.

The usage of cyber elements in inter-state relations and conflicts has experienced a significant transformation in a short period of time. If the cyber attacks in the first decade of the century were designed to achieve mostly technical effects, such attacks have mainly made way for cyber operations performed for information-psychological influence from the middle of the second decade. For Georgia, Russia's destructive cyber operations continue to be the main threat – aimed at technical as well as psychological effects, they are rather dangerous for our country. It must be pointed out that in recent years, Russia's destructive cyber activities have moved beyond the post-Soviet area and election processes in Europe and the United States have often been targeted by hackers affiliated with Russian government structures. Cyberspace has turned into an important theatre for Russian propaganda content and Russian informational confrontation in general which is yet another testament to the risks flowing from cyber operations designed to achieve information-psychological results.

Russian Cyber Threats: Main Directions and Goals

As of today, the cyber threat from Russia towards Georgia is real and compared to the cyber attacks of 2008, the level of cyber threats has grown owing to several factors. Russia has not only altered its aggressive cyber policy, but has also significantly increased its cyber attack potential and extended the fields of usage of cyber operations for attacks aimed at having a technical effect as well as for psychological influence operations conducted in cyberspace. The information-psychological effect of such cyber operations is to alter perception in the Kremlin's favor and reduce pro-Western sentiments, typically causing the pro-Russian elites to strengthen which is an important precondition for conventional actions. Hereby it should also be pointed out that compared to 2008, Georgia's

dependence on information and communication technologies in much higher now which, in the case of a cyber attack, increases the scale of the expected damage.

In a democratic state, the majority of critically important services are located in the private sector. Business development is one of the main factors for economic growth and economic security in general. This is exactly why the cyberspace of businesses often ends up to be the victim of inter-state relations which, in its turn, has noticeable influence on the state itself. Parallel to the ever-increasing usage of cyberspace, the risks are growing proportionally as well. Unfortunately, there is no immunity from cyber threats.

From the beginning of the 21st century, fields such as state structures, media and communications, industry, energy, political organizations and others have become the targets for Russian cyber operations of varying difficulty and intensity in tens of countries.

The analysis of developments in cyberspace for the past two decades and the usage of cyber elements in conflicts make it clear that the negative effects of cyber operations conducted by Russia are diverse and could serve different purposes:

- **Disabling Industry Control Systems (ICS)**. According to the US intelligence data[1], since at least 2015, Russia has possessed the ability to have remote access over the software controlling critical information systems of the adversary.[2] According to the same data, cyber actors affiliated with Russia successfully managed to compromise the supply chain of the products of several vendors in a way that after downloading legal updates, Russian malware[3] was ending up in their user systems. Despite the fact that the use of ICS in Georgia is not frequent, the production cycle of large producers in the industry is still automated.
- **Cyber Espionage**. Several years ago, Georgian agencies revealed a large-scale cyber espionage operation – GEORBOT. According to the data in the report of the US cyber security organization, Fire Eye, there was non-sanctioned access to the resources of government and law enforcement structures, offices of military attaches, documentation regarding the relations between NATO and Georgia and other sensitive material for years. Various categories of information were constantly

outflowing through remotely installed malware.[4] The operation was run by a hacker group controlled by the Russian Special Forces called APT28, or Fancy Bear, later becoming a case of concern for the international community on multiple occasions. The aim of the organization is to gather information about the issues related to defense and geopolitics by using spy programs which could only be interesting to a state. APT28, which has existed from at least 2007, was, in this case, carrying out attacks for obtaining intelligence information in accordance with Russia's international interests, mainly in three directions which included: the Caucasus region, more specifically – Georgia; the Eastern European region, more specifically Hungary and Poland, and European and Euro-Atlantic security organizations: NATO and OSCE.

- **Cyber Attacks through sophisticated Malware**. In the Ukrainian conflict, Russia used the influence of sophisticated viruses with kinetic effect (BlackEnergy and Ouroboros) on critical infrastructure. Such malware "was being prepared for almost ten years and is highly difficult for an individual or a non-state actor to design."[5] Such actions create a feeling that during the future conflict, Russia will not limit itself to low-tech attacks and temporary disruptions of infrastructure.

- **Various Levels of Disruption or Disablement of Critical Infrastructure Functioning through Ddos or Defacement[6]** type attacks. It is known that in terms of a weakly protected infrastructure, even low-tech Ddos or Defacement attacks could result in disproportionately high damage.

- **Compromising Supply Chain[7] –** means infiltration through a product supplier or flaws in production or logistics. Recently, such infiltration has been frequently used by various states, especially Russia.

- **Insider Threats:** one of the simplest ways of gaining access to a system is infiltration through an insider. Insiders are considered to be former or current employees, contractors and all subjects who could have legal access to information systems. This channel is often used by the Russian Special Services. Recently, the renowned US cyber scandals connected to Russia were caused by insider threats. Apart from motivated insider threats, insider cyber incidents caused by the low awareness of users are also noteworthy. For installing malware, Russian cyber actors often use a common method such as phishing[8] and in Georgia the overall percentage of victims of phishing varies from 40% to 50% which is a

rather risky statistic. It was through phishing that the networks of the US Democratic Party, German Bundestag and other state institutions or businesses were compromised by cyber actors connected to the Russian Special Services.

- **Cyber Operations with Information Psychological Effect.** Propagandist content disseminated through cyber channels could cause the information-psychological effect: an altered perception in the Kremlin's favor, the reduction of pro-Western sentiments and the formation and strengthening of the pro-Russian elite which could be a prerequisite for conventional action.

The implementation of cyber operations by Russia during war or conflict, as well as peacetime, could be connected to addressing various strategic or tactical tasks. An incomplete list of such tasks is as follows:

- Punitive measures for actions inconsistent with Russian interests or a leverage of pressure for performing political tasks.
- Actions integrated with, preceding or accompanying conventional actions for simplifying the implementation of military tasks.
- Long-term disablement of critical infrastructure through a cyber operation with kinetic effects in order to cause economic collapse, financial damage or mass discord.
- Hindering the proper functioning of state institutions by limiting access to critical services.
- Reducing pro-Western sentiments and altering perception in the Kremlin's favor through information-psychological influencing.
- Manipulation of election results with the aim of discrediting the reputation of an unwanted candidate, weakening democratic order or undermining trust towards state institutions.
- Obtaining intelligence information through cyber espionage acts, other intelligence actions for the formation of antagonized ethnic, religious or political groups, undermining neighborly inter-state relations.
- Mining of fabrication of online data for discrediting, intimidating or blackmailing political figures, military officials, social groups or decision-making circles.

For Georgia, given the destructive and severely aggressive nature of its northern neighbor, this trend will be more-or-less dangerous. The existing situation requires a high level of awareness and concrete steps from government structures as well as representatives of critical infrastructure on strategic as well as tactical and operational levels.

Given the pace of the growth of threats in cyberspace as well as the area of their dissemination, it is important to analyze how Georgia is countering these trends. The steps taken by state cyber actors in the field of cyber security for the past decade have caused the reality where in the UN ITU Cyber Security Index, Georgia has entered the top ten worldwide. In order to calculate this Index, the study is conducted in five main directions of cyber security: legislative base, technical equipment, organizational structure, development of capacities and cooperation. Clearly, advancement in such an authoritative ranking means recognition for the national cyber security system. It must be pointed out that Georgia was assessed to be the leading country in the CIS area.[9] Despite these successes, the strategic and conceptual documentation of cyber security, as well as the legislative base, requires fundamental renewal as without effective cyber defense our country cannot become a reliable partner for the North Atlantic Treaty Organization.

Given all of the aforementioned facts, special attention must be paid to documenting the intentions, capacities or actions of Russia as a destructive cyber actor in the strategic documentation for cyber security. The new National Strategy and the legislation formulated on its basis must ensure the full integration of cyber security into all spheres of wider security and state life.

Problems with the Existing Strategy and Main Directions of the New Conceptual Base

Given the ever-changing nature of cyberspace, it is vitally important to clearly underline the problems accompanying the development of the cyber dimension of Georgia. Let us discuss several of them:

After the abolition of the State Security and Crisis Management Council, **there has been no coordinating structure in the cyber security architecture of Georgia** for over a year that would ensure the coordinated work of state cyber actors as well as cooperation with private actors and joint work on strategic documents. The absence of a coordinating structure is probably

one of the reasons why **Georgia, unfortunately, met 2019 without a National Cyber Security Strategy**. The previous strategy was functional by 2018 and the work for creating a new one started in 2019 is still at an initial stage and will likely last several months. By the way, the fact itself that Georgia is already working on a third generation strategy is very positively perceived by the international community and cyber experts which does indeed cause leading positions in international ratings.

- **The paradigm for the determination of critical infrastructure must be fundamentally reviewed.** In a democratic state, the majority of critically important services are located in the private sector and consequently, according to best practices, the private sector represents much of the critical infrastructure.[10] These fields include energy and water supply, the banking and financial sector, the food, chemical and military industries; the medical segment and others. According to the current Georgian legislation, critical infrastructure covers only a part of state networks and does not extend over the business fields critically important for the state.

- The current legislation considers the system of the Ministry of Defense of Georgia to be the only critical infrastructure in the defense field, ignoring the objects in the private sector, the functioning of which are vitally important for the field of defense (for example: the food industry, military industry, private actors within the logistical chain). The best practices include discussing the threat to the defense capacities of the country based on the scale of attack on the critical infrastructure objects of the country. **The division of the existing critical infrastructure into the defense field and the rest of the public sector itself must be reviewed. The state must have a unified list of the critical infrastructure whose protection will be the competence of various state actors including, in certain cases, the Ministry of Defense depending on the source of the aggression and the scale of the attack.**

- Despite more-or-less developed mechanisms of network defense, there is a risk of a hostile state accessing the industry control systems remotely through hacking and planting compromised technical machinery and software through supply chain operations which, given the current legislation, puts almost all information and communication networks existing in the state at risk. To put it simply, through the existing legislation regarding acquisitions, it is possible to buy critical

infrastructure or computer technologies,[11] services and software designated for state institutions from Russian companies or Russian branches of other foreign companies. Unfortunately, such cases have taken place recently as well when a fiber optical communications network was nearly bought by a Russian company while a certain part of government institutions currently receive their mobile communication services from a Russian company, among others. The same legislation also makes it possible for business organizations of the occupant country to implement internetization processes and other large projects connected to information technologies and also provide mobile communication services to state structures.[12] Of course, for these reasons, it should be quite unimaginable for the company of the occupant state to provide communications to government structures when the abovementioned occupant state successfully uses cyberspace in multi-dimensional hybrid warfare. On a conceptual level, the management of supply chain risks must be integrated into the acquisitions process or risk management system in order to ensure the security and reliability of equipment and technologies used by the state sector. Specific rules for the purchases of cyber technologies, as specialized goods and services, must be formulated where the product reliability and security will become one of the determining factors. A prohibition must be instituted on buying Russian-made or Russian imported information technologies or services.[13]

- The existing conceptual and normative base fails to address the increasing importance of insider threats. In terms of a market economy, the private sector is often a provider of critical services and hence information data of the state sector often end up in the hands of contractors which increases the scale of insider threats. In the Georgian reality, protecting sensitive information transferred by the state sector to the business sector within a business partnership is completely dependent on the good will of the company. Businesses, by their nature, are oriented on getting maximum profits with minimum expenditure; hence, they avoid additional expenses for security. This issue requires immediate regulation as no one knows what amount and type of non-classified yet sensitive information of state structures is accumulated in defenseless private networks. Large sets of personal information of public servants and military servicemen transferred to insurance companies are a good enough example of this. Such information is especially valuable on the Darknet which makes

respective systems a lucrative target for both financially motivated cyber criminals as well as cyber actors of a hostile state. It is necessary to strictly define standards for protecting data that will be obligatory for contractors to meet in order to participate in state acquisitions. In addition, the state must help private companies and contractors to process important information in an acceptable level of cyber security.

- Another vital topic is the proper perception of cyber security problems by top managers in the state and private sectors. The level of perception that allows for the use of non-licensed software or Russian anti-virus programs and e-mail providers by state structures remains an unfortunate reality. Such cases are not at all rare. For comparison, let us remember that due to cyber risks (data collection, tracking), the appropriate Lithuanian state structure recommended that public servants do not use the services of Yandex-Taxi. It is necessary to formulate a complex of measures for heightening awareness with regard to cyber security and implement it on all levels of state governance.
- If the existing strategy and normative base at least partially regulates the technical effects of destructive cyber operations, the conceptual document does not even discuss the negative influence of propaganda and disinformation disseminated through cyber channels. It is necessary to identify the structures responsible for preventing the information-psychological effects of Russian cyber operations in the cyber security architecture as well as defining their roles – study the sources of threats and organize events for informing target groups about possible threats and destructive actors.
- Results of cyber attacks, types of discovered malware and risky activities are closed information due to reputational risks, even though it would be much easier and effective to manage risks in the case of the proper sharing of this information. The formulation of a policy for transparency and a timely sharing of the results of cyber attacks must be decided at a strategic level – also creating inter-structure and public-private platforms for exchanging information about threats and risks.

Therefore, in terms of the new national strategy, it is necessary to move cyber security to a higher level and integrate cyber security requirements into various fields of state life.

References

1. Hearing: World Wide Cyber Threats (Open),Testimony of The Honorable James Clapper, Director of National Intelligence, September 10, 2015. Accessable at: www.docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF

2. **ICS (Industrial control system) –** a collective term used for describing control systems and instruments connected to them, bringing together the machinery, systems, networks and control mechanisms used for automation and operation of industry processes. Currently widely used in almost all sorts of critical infrastructure such as industry, transport, energy, hydro-economy and others which is why it is a target for destructive cyber operations. Widely spread versions of ICS are the so-called **SCADA (Supervisory Control and Data Acquisition)** and **DCS (Distributed Control Systems) systems.**

3. **Malicious software, malware**: Computer program used for non-sanctioned access to information systems, gathering sensitive information, stealing, destroying, altering, encrypting or illegally obtaining access to a computer.

4. Fireeye special report, 2014, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? Accessible at: www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

5. Sam Jones, "Cyber Snake Plagues Ukraine Networks," Financial Times, 7 March 2014. Accessed at www.ft.com/content/615c29ba-a614-11e3-8a2a-00144feab7de www.ft.com/content/615c29ba-a614-11e3-8a2a-00144feab7de

6. A form of low-tech cyber attack which changes the appearance of a website without permission, especially the cover page. Is mainly used by hacktivists and cyber terrorists for spreading protests messages, propaganda material or other content. Such an attack was performed by Russia-affiliated hackers on the website of the Georgian President in 2008 where they placed fascist symbols.

7. The so-called **Supply Chain Threats** – threats arising in the process of supplying a product (computer technologies, software and others) which means the probability of incidents connected to flaws of the supplier when the supplying side cannot or does not ensure that security measures are followed or actively threatens the security, life or health of the client.

8. **Phishing** – a common form of cyber crime which aims to compromise the computer, install malware and get access to sensitive information by deceiving the victim. A special form of phishing is the so-called Spear-Phishing designed for narrower and more specific circles of users (management, groups carrying certain knowledge or information). It requires a well-prepared context for gaining trust. Apart from financial cyber crime, various forms of phishing are actively used in inter-state destructive cyber operations for compromising the network of the adversary.

9. The Global Cybersecurity Index (GCI) 2018, International Telecommunication Union (ITU). Accessible at: www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf?fbclid=IwAR1--Sw9bTs0N0qFHBbGcGTckqeyNryG1eBGHNP9k5Ar1oNZqFyS0yFOIXA

10. PRESIDENTIAL POLICY DIRECTIVE/PPD-21: SUBJECT: Critical Infrastructure Security and Resilience, February 12, 2013. Accessible at www.obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil and www.dhs.gov/cisa/critical-infrastructure-sectors

11. Apart from the fact that there are numerous precedents of puchasing sensitive services or products from Russian companies in the not-so-distant past, the Ministry of Defense, among other products, also bought computer technologies from a company whose leader has been tried for spying in Russia's favor. The Ministry explained this incident by a lack of appropriate legislation. Clearly, the legislative vacuum is definitely one of the problems for preventing such incidents, yet it is not the only one as in the case of an appropriate understanding of the so-called supply chain threats, an unreliable actor can absolutely be disqualified from a state acquisition process for security interests. See the July 2, 2018 statement by the Ministry of Defense of Georgia. Accessible at: www.mod.gov.ge/ge/news/read/6668/saqartvelos-tavdacvis-saministros-gancxadeba

12. From a technical standpoint, it is beyond doubt that a mobile network operator has all the means to control its clients' calls, messaging, spy on their movement, identify location and, upon necessity, use the mobile device itself (phone, tablet and others) for intelligence or other undermining purposes. In the case of the usage of mobile data, the personal or public life of any client becomes accessible. It was the abilities of a mobile network operator and metadata that Russia used for resolving military and political tasks of varying difficulty as well as blackmail, intimidation or determining coordinates for artillery strikes in the Ukrainian conflict.

13. Such a precedent was created by the Special Services of the United States where after the famous Kaspersky Scandal, the state structures were given 90 days to uninstall this software. Accessible at: www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4