RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

RUSSIA'S CYBER ACTIVITIES – A GROWING THREAT FOR GEORGIA

ANDRO GOTSIRIDZE

EXPERT OPINION 95

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

EXPERT OPINION

ANDRO GOTSIRIDZE

RUSSIA'S CYBER ACTIVITIES – A GROWING THREAT FOR GEORGIA

95

2018

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

All rights reserved and belong to Georgian Foundation for Strategic and International Studies. No part of this publication may be reproduced in any form, including electronic and mechanical, without the prior written permission of the publisher. The opinions and conclusions expressed are those of the author/s and do not necessarily reflect the views of the Georgian Foundation for Strategic and International Studies.

Copyright © 2018 Georgian Foundation for Strategic and International Studies

ISSN 1512-4835
ISBN 978-9941-27-873-0

Operations taking place in cyber space represent a purposeful attempt to compromise the integrity and availability of computer networks and the confidentiality of electronic services. Such actions may be aimed at damaging or impeding service, or at using a computer network as an attack tool in order to attain non-sanctioned access to certain databases or information. During the past decade, cyber operations have been used not only for actions designed to produce a technical effect, but also for changing the perceptions of a target actor through open or covert channels.

The cyber domain has established itself as a fifth field of confrontation – apart from the air, land, maritime and space fields. The use of cyber elements in order to achieve political, economic, and/or military goals, as well as geopolitical superiority, is a reality in the contemporary world. According to existing data, up to 40 states already have offensive cyber capabilities and are successfully developing it further. The cyber element today has already become an important part of any war, conflict or confrontation.

For Georgia, as an object of Russia's constant interest, securing the cyber space from its usage against Georgia's national security and defense is a priority field. The Kremlin considers Georgia to be within its sphere of influence, which is why our country is a target for Russian hybrid warfare. The hybrid activities taken by Russia consist of diplomatic, economic, military, political, cultural, social and religious information fields, bringing together the cyber operation designed for technical, as well as psychological purposes.

The increasing intensity with which cyber elements were used during conflicts with Estonia, Georgia and Ukraine – especially during the annexation of Crimea – personifies the recent Russian activities and its tactics of hybrid warfare as successful examples of the strategic integration of informational operations, provocations and cyber-attacks with conventional military operations. The analysis of the conflicts involving Russia makes it clear that it uses the conflict territories as a sort of a training ground for testing its own cyber-attack potential.

If the 2007 cyber-attack against Estonia – a punitive operation for the "bronze soldier" and a political message – was aimed to spur public unrest and mass turmoil and was the first attempt at using cyber elements to influence political processes, the following year, the use of cyber elements

in the Russia-Georgia War was a well-organized complementary process to conventional military actions, aiming at creating an information vacuum, spreading disinformation and closing the channels of international support for Georgia. In the war with Ukraine, the Russian cyber-attack had developed even further and apart from traditional results, Russia managed to utilize the capacities of large telecommunication companies in order to secretly eavesdrop on their clients, determine their locations and acquire other sorts of information which was later used for both psychological influence and information grabs as well as for the determination of locations and provision of coordinates for artillery strikes. In addition, in the conflict with Ukraine, for the first time, Russia performed an attack and disabled part of the Ukrainian energy system.[1]

For the past two years, Russia's destructive cyber activities have left the confines of the Post-Soviet area and hackers connected with Russian government structures have upon numerous occasions, targeted election processes in Europe and the United States.

The cyber units of the Ministry of Defense of the Russian Federation, which are responsible for performing cyber-attacks, propaganda-oriented actions and inserting malware in the command and control systems of opponents, represent a very real and highly serious danger for Georgia. According to high-ranking Russian military officials, these information operation units participated in the command staff exercise „Кавказ-2016"for the first time in September 2016, which once again confirms Russia's intention to control the field of information through military means.

According to existing information, Russia is actively developing remote access mechanisms for Industrial Control Systems (ICS) of critical infrastructure units. According to data provided by experts, unknown Russian actors successfully managed to compromise the product supply chains of several producers of the ICS by installing malware codes in software updates designed to facilitate exploitation.[2] The cyber-attacks on the Ukrainian energy system created a sense that in future conflicts, Russia will not limit its activities to simple DDoS and Defacement attacks or cyber espionage operations and that there is no guarantee it will not take action against critical infrastructure, which might be followed by destruction and perhaps even casualties. It should be taken into account that in cases of infrastructures with weak defenses, even DDoS and Defacement attacks could cause disproportionate damage.

As already pointed out at the beginning, apart from the attacks aimed at disabling or using the network of an adversary, Russia also uses cyber space for producing psychological effects, which means attempting to alter the behavior or perception of the target demographic in favor of the Kremlin.

The main effect of the "information confrontation" concept well known in Russian military circles is to manipulate the perceptions of the target audience and influence their behavior. Russia considers the field of information to be a strategically decisive and critically important domain of the new type of military conflict, which could be used to both exert control over its own population as well as to acquire influence over opposing countries. Information warfare for the Kremlin is a key tool for establishing dominance in the international arena. The military circles consider it to be their priority to develop forces and means for gaining informational superiority during periods of war, crisis and peace, meaning control over the content of information, as well as over the technical means of its dissemination. "Informational Confrontation" against Western societies is based upon the Soviet era tactics of psychological warfare and is one of the main aspects of the Russian strategy. In general, informational-psychological influence represents the initial phase of the conflicts inspired by Russia, consisting of non-conventional operations aimed at manipulating the public opinion inside the target country, as well as through the international media. The annexation of Crimea showed us that in parallel to intensive actions, Russian military units accessed the target territory under the cover of local armed formations. The phase of non-conventional operations ends there. If the operation turns out to be successful, then actions aimed at legitimizing the intervention are taken, and justified with the mythical pretext of "protecting the rights of minorities". The second phase already involves conventional actions; however, again in the case of Crimea, the success of the first, non-conventional phase simplified the conventional phase of the conflict in Russia's favor.

One of the most serious instruments for acquiring informational superiority in the Russian arsenal is the cyber support for psychological operations aimed at implementing the strategic and tactical tasks of information warfare. The cyber elements of such operations include compromising the networks of the objects of interest with the aim of acquiring information that could be used for intimidation, blackmail, discrediting and falsification, as well as for controlled dissemination in mass media.

Russia uses various tools to gain dominance in the process of informational confrontation: due to the difficulty of attribution, Russian intelligence services establish highly secretive hacktivist groups or act under the cover of already established ones. Hacktivist attacks were one of the components in the cyber-attacks supported by the Russian government in 2007 in Estonia and in 2008 in Georgia. They were also heavily involved in the Russia-Ukraine conflict during the events of Maidan and annexation of Crimea.

Lately, open sources and data from friendly special services are dominated by the idea that Russia was behind the hacktivists attack on the French TV channel TV5 Monde in April 2015, allegedly performed by the Cyber Caliphate associated with Daesh.[3] The same group is responsible for hacking the Twitter account of the United States Central Command. The attack on the French TV channel was well organized and started back in January by sending phishing letters to its employees. Three months later, this enabled the cyber-criminals to gain control of up to ten information channels and their social media channels, spread jihadi propaganda and publish the personal data of the French military personnel serving in Syria.

There are numerous pieces of technical evidence that this well-known attack by cyber terrorists was a cyber-attack conducted/supported by the Russian state – a so-called false flag operation under the cover of the Cyber Caliphate. Despite the difficulties of attribution, this opinion is reinforced by the *modus operandi* of the attack as well as the existence of elements of Cyrillic script in malware codes, identical to the M.O. of the APT28 (an organization affiliated with the Russian Special services that is responsible for multiple cyber espionage or other sorts of cyber-attacks against Georgia, Ukraine, EU member states and the USA) hacker group operating under Kremlin's control. An additional argument is that the timing of the attack coincides with the worsening of relations between France and Russia (the Mistral matter, the refusal of then President of France to participate in the 9 May events in Moscow and so on).

As of today, the likelihood of a cyber-attack by terrorist organizations that would cause mass damage or casualties is very low. Their cyber capabilities are only sufficient for temporary, local damage to electronic services and websites; however, the threat will be much more serious if the terrorist organizations cooperate with any state with advanced cyber capabilities in

order to essentially improve their own cyber capacities. It should be noted, that Russia has provided the first example of such cooperation, despite the fact that cooperating with terrorist organizations contains political risks for states.

The flagship of cyber activities run by Moscow – group CyberBerkut – is in charge of cyber support for Russian military operations and strategic tasks. The group undertakes both technical, as well as propaganda attacks. CyberBerkut has been actively involved in cyber espionage or DDoS attacks against NATO, Ukraine and German government websites since 2014. The focus is on the online publishing of documentation acquired through hacking, which mainly serves the purpose of discrediting governments, reducing trust towards elected bodies, and the demoralization and intimidation of the adversary.

In order to change or manipulate information, Russia widely uses a paid commentator army –so-called Trolls. The largest grouping of hired Trolls – the Internet Research Agency (IRA), a.k.a. Trolls from Olgino, is a state funded organization, which acts on the Kremlin's orders and mainly publishes pro-government content or engages in online discussions in favor of the Kremlin. The task of the organization is to combat "Western influence" and media sources that have a negative stance towards Russia. Additionally, the function of some of these trolls is also to spread false content.

One of the means of manipulation for Russia are the numerous internet-bots controlled by the Kremlin, which are essentially applications that automatically spread content throughout social media. A bot can tank unwanted information, make it impossible to access real content, spread a specific message or undertake other tasks of various difficulty and content.

The content itself – the spreading of which serves all of the means stated above – represents *a mix of false and true information aimed at confusing, demoralizing and gaining influence over the target audience. The target audience is the population of Russia, certain groups within the populations of other countries, the internal Russian political elite or those of the target countries. The channels of spreading propaganda are various: including TV and radio channels, bots and social media Trolls, optimized search engines, bribed journalists in foreign media and more.*

The spreading of desired informational content, the development of technical capacities or control of already existing ones for the means listed above happens at least in three different ways:

- Creation of a manageable communication space in the country of interest, creating broadcasting channels and domination in the social media with the aim of sowing a feeling of political or economic instability.
- Creating cyber channels of informational support for pro-Russian political parties or groupings, aimed at establishing a pro-Russian elite; establishing a mood that the pro-Russian forces could end up in a Parliament or participate in the formation of a government.
- Using other segments of social media and cyber space for undermining purposes, especially in the context of the relations with neighbors which could possibly damage relations with a strategic partner or neighboring states and in the case of aggression make it more difficult to get political or other types of support.

According to the data of leading intelligence services, by using the aforementioned channels and spreading desirable content, the Russian propaganda machine is mainly trying to promote several ideas:

- The bankrupt Western Liberal order must be changed with an Eurasian Neo-Conservative Post-Liberal world order, which protects traditions, conservative values and true freedoms.
- The West is demonizing Russia, whilst the latter is merely trying to protect its interests and sovereignty.
- The United States is interfering with the domestic politics of sovereign states and changes government all over the world.

The scale of the cyber threats coming from Russia is growing in terms of both complexity as well as variation. An informational-technical effect-oriented cyber-attack performed or supported by Russia against Georgia could cause serious damage and even casualties whilst the propaganda content spread through cyber channels could cause the alteration of perceptions in favor of the Kremlin, reduce pro-Western sentiments and form/strengthen the pro-Russian elite; all of which could be a prerequisite to conventional actions. Hence, **it is necessary to allocate sufficient attention to creating a mechanism for acquiring and analyzing information about the intentions,**

capabilities and actions of Russia as a destructive cyber actor, as well as to conduct active work in this regard.

It is vitally important to focus not only on network protection operations, but to also **integrate cyber capabilities with other military operations.** Cyber elements – as the recent events have made clear – hold one of the key roles in hybrid warfare tactics and are used for solving more and more tasks. It is important to constantly involve cyber elements in military exercises taking place on the territory of our country as well as to ensure participation of Georgian structures, the private sector and the academia in international cyber exercises. The main work in this regard is yet to be done and the challenge itself, according to the common assessment, is more intellectual, than technical.

An approach must be established that **cyber security is a common responsibility and that without effective international or intra-structure cooperation on information exchange, our country cannot play the role of a reliable partner in cyber space.** In this context, the **actions aimed towards raising the awareness of users** are of utmost importance.

Despite the fact that the difference between our adversary and us is enormous in terms of military potential, cyber space is actually a domain where a small country can truly resist a much more powerful aggressor. Cyber space can become a successful element of an asymmetric response to threatening actions or a sort of on-going front of resistance.

References

1. The usage of cyber elements in the Ukrainian conflict is discussed at length in the compilation published by NATO CCD COE: Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn, 2015.

2. The intelligence community of the United States of America marked this information, as well as the statement of the Minister of Defense of Russian Federation about the creation of Cyber-Command as a serious threat. For example, Statement for the Record. Hearing: Worldwide Cyber Threat. House Permanent Select Committee on Intelligence. James R. Clapper, Director of National Intelligence. “Computer security studies assert that Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software (“malware”) designed to facilitate exploitation directly from the vendors’ websites along with legitimate software updates, according to private sector cyber security experts.”

3. The terroristic nature of Daesh and the cyber structures associated with it are under no doubt and by its actions, Russia created a precedent of cooperating with the terrorists, which, in itself, contains danger, even in terms of basic improvement of the cyber abilities of the terrorist organizations. Despite the fact that this action was a typical false flag operation from the side of the Russian Special Forces, it can still be qualified as an operation conducted under the cover of hacktivism. See, for example the US Defence Intelligence Agency report RUSSIA MILITARY POWER - Building a Military to Support Great Power Aspirations “Under the guise of hacktivism, a group called “Cyber Caliphate,” seemingly ISIS associated, conducted a hack against French station TV5 Monde in January 2015. The Cyber Caliphate group was later linked to Russian military hackers. The same group hijacked the Twitter feed of the U.S. Central Command”. www.dia.mil/Military-Power-Publications