NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DIGITALIZED DARK ART: RUSSIA'S INFORMATION OPERATIONS AGAINST GEORGIA

by

Sandro Bzishvili

December 2020

Thesis Advisor: Ryan Maness
Second Reader: Anne L. Clunan

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
DIGITALIZED DARK ART: RUSSIA'S INFORMATION OPERATIONS AGAINST GEORGIA

5. FUNDING NUMBERS

6. AUTHOR(S) Sandro Bzishvili

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

In this age of asymmetric warfare, cyberspace provides new opportunities and vulnerabilities for achieving strategic effects. As a revisionist power, Russia has embraced cyberspace as a key tool and a force multiplier to achieve its geopolitical objectives and target perceived adversaries. Since the Russia-Georgia war in 2008, the Kremlin has continued a full spectrum of information warfare as a part of coercive attempts to alter Georgia's pro-Western orientation and undermine its national security apparatus.

Based on the four distinct cases of cyber incidents from 2008 to 2020, this thesis explores Russia's information warfare against Georgia and the role of the cyber component within it. The purpose of this thesis is twofold: First, it highlights the importance of understanding the Russia's threat stemming from cyberspace, as it appears to be characterized by certain ambiguities. Second, as a result of examining the patterns of Russia's hostile actions in this new domain, this thesis provides foundations for potential countermeasures by referring to existing best practices and experiences, which are built on the robust cybersecurity and cyberdefense strategy models developed by Israel and Estonia.

14. SUBJECT TERMS
Georgia, Russia, Estonia, Israel, information warfare, political warfare, active measures, disinformation, propaganda, cyber operations, cyber-attacks, cyberdefense, cybersecurity, strategy

15. NUMBER OF PAGES
75

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

DIGITALIZED DARK ART: RUSSIA'S INFORMATION OPERATIONS AGAINST GEORGIA

Sandro Bzishvili
Civilian, Other, Georgia
B, Caucasus University, 2009
LL.M., Georgian Technical University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(INFORMATION OPERATIONS)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2020**

Approved by: Ryan Maness
Advisor

Anne L. Clunan
Second Reader

Douglas A. Borer
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this age of asymmetric warfare, cyberspace provides new opportunities and vulnerabilities for achieving strategic effects. As a revisionist power, Russia has embraced cyberspace as a key tool and a force multiplier to achieve its geopolitical objectives and target perceived adversaries. Since the Russia-Georgia war in 2008, the Kremlin has continued a full spectrum of information warfare as a part of coercive attempts to alter Georgia's pro-Western orientation and undermine its national security apparatus.

Based on the four distinct cases of cyber incidents from 2008 to 2020, this thesis explores Russia's information warfare against Georgia and the role of the cyber component within it. The purpose of this thesis is twofold: First, it highlights the importance of understanding the Russia's threat stemming from cyberspace, as it appears to be characterized by certain ambiguities. Second, as a result of examining the patterns of Russia's hostile actions in this new domain, this thesis provides foundations for potential countermeasures by referring to existing best practices and experiences, which are built on the robust cybersecurity and cyberdefense strategy models developed by Israel and Estonia.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C4I	Command, Control, Computers, Communication, and Intelligence
CDU	Cyber Defense Unit of Estonia
CERT	Georgian Computer Emergency Response Team
CERT-IL	Israeli Computer Emergency Response Team
DCID	Dyadic Cyber Incident and Dispute Dataset
DDoS	distributed denial of service
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDF	Israel Defense Forces
INCB	Israeli National Cyber Bureau
INCD	Israel National Cyber Directorate
IRA	Internet Research Agency (Kremlin)
NATO	North Atlantic Treaty Organization
NCSA	National Cyber Security Authority
NIS	New Israeli Shekel
NISA	Israeli National Information Security Agency
R&D	Research & Development
SDR	State Security Service of Georgia
SSSG	State Security Service of Georgia

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CONTEXT

Since declaring national independence in 1991, Georgia has been in asymmetrical power relationship with Russia.[1] Russia has tried to exploit Georgia's defense and security vulnerabilities from the very beginning of its independent statehood by fomenting regional conflicts, encouraging political extremism, and, as in 2008, even invading militarily.[2] Nonetheless, despite Russia's occupation of a significant and strategically important part of Georgian territory, Georgia managed to build effective state institutions and democratic structures.[3]

The focus of this thesis is how Russia employs cyber strategies against Georgia and what countermeasures Georgia can use to contain Russia's encroachment on its sovereignty, independence, and territorial integrity in terms of information warfare and, in particular, in the cyber security domain.

Cyber strategies as a part of twenty-first century political warfare is an emerging pattern for the new technological era. In the last two decades, there have been four distinct cases of Russia's use of information warfare and its cyber capabilities to disrupt Georgia's information security systems. These happened during the Russian invasion of Georgia in August 2008; twice when Russia hacked Georgia's government agencies in 2011 and 2019; and the latest—a combined cyber and disinformation campaign against Georgia's critical infrastructure and medical facility in the midst of the COVID-19 crisis.

These four cases were part of Russia's relatively newly established arsenal of information warfare that has gained significance in Russia's foreign and security policy in

[1] Georgia's population is 3.7 mln while Russia's population exceeds 142 mln. Militarily, the imbalance is even more striking, see "Chapter Five: Russia and Eurasia," *The Military Balance 120,* no.1 (February 14, 2020).

[2] Stephen F. Jones, *Georgia: A Political History since Independence* (New York, NY: I.B. Tauris, 2012).

[3] Stephen F. Jones and Neil S. MacFarlane, *Georgia: From Autocracy to Democracy* (Toronto, University of Toronto Press: 2020).

the last decade. For Russia, cyberspace has become integral to the information space and cyber activity has emerged as a subcategory of the information warfare. Given the decline in Russia's defense resources in comparison with the times of USSR, and the asymmetry relative to the capabilities of the United States and its NATO allies, information warfare has become a relatively affordable option for waging political warfare abroad, especially in Russia's so-called "near abroad," which encompasses the countries that had been part of the former Soviet Union prior to 1991.

Such operations have been deployed against Estonia, Georgia, and Ukraine at different times in the last two decades. Russia's activity in these countries displayed a discernable pattern, which presumes deployment of soft power means for winning the local populations' sympathy, and, in case of failure of such, continues to coerce and intimidate the target audiences. Manipulation of target audiences' perceptions has become the primary objective of Russia's information operations, while the purpose of cyber activity has been short-term critical disruption of the target's state institutions and/or support for Russia's on-ground military operations.

However, the record of Russia's use of cyber strategies as a part of political warfare indicates that the Kremlin has not been very effective in relation to its purported political objectives and has failed when countered by the target states with appropriate political and technological tools in systematic and consistent ways. This record also shows that Russia's cyber operations may not have succeeded even in conditions of significant power asymmetry in Russia's favor. This is particularly evident when countermeasures are taken both in terms of international and informational domains, by aggregating political and technological tools against Russia's activities.

This thesis has both analytical and prescriptive purposes as it seeks to describe and analyze Russia's approach to information warfare, discuss a case study of Russia's cyber operations against Georgia, and, finally, identify potential countermeasures to Russian activities, as developed by other countries in similar or comparable circumstances.

As historical tendencies demonstrate, Russia is likely to continue to pose an existential threat to Georgia's national security. Therefore, the primary focus of this paper

is to analyze Russia's cyber operations against Georgia as an integral part of Russia's information warfare and seek successful models of countermeasures, as created by Israel and Estonia in particular.

B. RESEARCH QUESTION AND HYPOTHESIS

The more specific question this thesis seeks to answer is what the most appropriate defense and security systems may be for countering Russia's information warfare and in conditions of power asymmetry.

For answers, the thesis relies on deductive logic, inferring conclusions from Russia's doctrinal and conceptual documents; analyzing the patterns of Russia's historically documented activities in cyber domain; and by comparing the experiences of countries with similar international standing and adequate systems for coping with malicious cyber activities by asymmetrically superior powers. These comparative cases include successful cybersecurity models based on technologies, science, and cyberspace but also on political and diplomatic effectiveness. While answering the question, regional and infrastructural similarities as well as power asymmetry and some other factors, including international involvement will also be considered.

The lead hypothesis for this paper is that a rigorous model of information warfare management can work even in a case of power asymmetry, when based on both technological as well as political efficacy, and long-term vision of cybersecurity and cyber defense strategy. Employing cyber capabilities to support national security is essential for the security strategy for Georgia and some other regional countries, and can be force multiplier, given the fact that Russian cyber operations are normally an accompanying element to more conventional operations rather than stand-alone attacks against the target countries. Strategic communications, as part of political measures, are also a crucial element in countering Russian information warfare.

C. METHODOLOGY AND SOURCES

This thesis uses case study as a method for answering the research question and validating the hypothesis. The case is Russian aggression against Georgia, which includes the information warfare aspect. The thesis draws practical recommendations based on comparative study of information warfare systems in Georgia, Estonia, and Israel, all of which exist and operate in conditions of power asymmetry with regional powers.

In the first chapter of the thesis, analysis of Russia's doctrinal and conceptual documents is given, complemented with anecdotal historical experiences in Russia's information warfare in the past two decades. This chapter aims at identifying patterns in Russia's cyber activities, with potential implications for smaller neighboring countries, such as Georgia.

The second chapter analyzes the historical record of Russia's actions in Georgia in four distinct cases, ranging from the cyberattacks accompanying ground offensive in 2008 to the 2020 disinformation campaign and cyberattack against the so-called Lugar Lab, established in close partnership with the United States Government.

The third chapter analyzes the cybersecurity systems created by Israel and Estonia, two countries that are similar to Georgia in a sense that they cope with power asymmetries with neighbors and also face information warfare challenges from multiple sources, including state and private entities.

The major method of researching the case study is deductive reasoning, which draws inferences from Russian doctrines and conceptual documents pertaining to information warfare. A comparative method is also used, which juxtaposes Georgian experiences with those of Israel and Estonia, inferring recommendations for Georgia's future cybersecurity system from the analysis of Israeli and Estonian experiences.

In the final, concluding part of the thesis, recommendations for Georgia's information security are presented.

II. UNDERSTANDING RUSSIA'S INFORMATION WARFARE

A. INTRODUCTION

The Kremlin has a long history of executing well-coordinated influence operations against its perceived adversaries in order to subvert and undermine them indirectly. With the advent of the information age, Moscow has realized new cyber domain opportunities and started to exploit this domain as a force multiplier for their political-military campaigns, thus, making specific operations more feasible and cost-effective as well. In other words, it has provided additional means for Russia to bolster its influence campaigns by employing a combination of cyber intrusions and propaganda. In retrospect, Russia's activities primarily against its neighbors—Estonia, Georgia, and Ukraine—demonstrated that it perceives cyberspace as an effective domain for employing their tactics successfully. Georgia was the first country that Russia targeted with a combination of kinetic and cyber means during the international conflict in 2008. Some of the similar cyber techniques Russia employed against Estonia in 2007, but tensions never escalated to a full-scale war. Since then, the Kremlin has only become more active in waging information warfare against its perceived adversaries while demonstrating interest in reclaiming its sphere of influence.

This chapter reviews the literature on Russia's information warfare and examines how cyberspace has been utilized by Russia within the broader information warfare concept. Also, it explores Russia's perspective on cyberspace as a fifth domain of strategic confrontation. The purpose of this chapter is to extract and highlight the major aspects of Russia's understanding of employing cyber ways and means based on existing studies and observations.

B. RUSSIA'S VIEW OF THE INFORMATION SPACE

Over the past decade, there has been a considerable amount of study and analysis with Russia's "new" way of war. It can be said that in the twenty-first century, the Russian Federation has successfully revived the Soviet tactics of "active measures" using modern technology and information space. According to Shultz and Godson, active measures,

which is an analogue for Western political warfare, during the Cold War era was an important tool to support Soviet foreign objectives.[4] Soviet diplomatic and intelligence services employed covert and overt techniques that included "setting up and funding front groups, covert broadcasting, media manipulation, disinformation and forgeries, and buying agents of influence."[5] In this light, Russia has utilized the internet and social media networks to stage hostile information campaigns as well as cyber-maneuvers to expose societal vulnerabilities of its perceived adversarial states. According to Benjamin Jensen, Russia uses this method as a "covert psychological warfare … designed to undermine a rival population's morale or faith in their political leaders."[6]

Many different scholars and pundits have discussed Russia's information warfare in cyberspace in order to explain how and why it became one of the main instruments for Moscow. Before examining the Kremlin novelties from different perspectives, it is important to emphasize that the modern Russian doctrines and policy consider cyberspace as an integral part of the information space and view information and cyber operations as a unified concept. Terms like cyberspace (*kiberprostranstvo)* or cyber warfare *(kibervoyna)* are used only in translations of foreign texts.[7] In other words, Russia sees cyber as a subset of information warfare and as an enabler for gaining superiority in the information landscape.[8] This thought is conceptualized in the Russian military doctrine of 2014, which views information as a cornerstone for national security and as an additional instrument of power in combination with conventional and nonconventional ones. Moreover,

---

[4] Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy.* Washington, DC: Pergamon-Brassey's International Publishers. 1984, 2.

[5] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," Strategic Perspectives, no. 11(Washington, DC: National Defense University Press, Institute for National Strategic Studies, 2012), 8. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.

[6] Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* 24, no. 1(October 1, 2017): 166, https://drive.google.com/file/d/1quiULILaIvSSQsOzQed0D1lgu1i38mQs/view.

[7] Scott Jasper and Keith Alexander, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington: Georgetown University Press, 2020), 71.

[8] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: Center for Naval Analyses, 2017), 3, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

information warfare is conceived as a means that could be employed both during both peacetime and wartime.[9] Simply, it is a continuous malign action targeting the opponent.

In order to discuss the Kremlin's refined information warfare, it is important to have an understanding of the main concepts that underpin Russia's holistic approach. Jolanta Darczewska from the Centre for Eastern Studies notes that Moscow's information warfare has a long history and follows the same approach as the preceding Soviet period *spetspropaganda* (special propaganda), which under President Vladimir Putin has obtained additional value in a "battlefield" against the West and its "near abroad" countries.[10] She also suggests that,

> most Russian authors understand 'information warfare' as influencing the consciousness of the masses and as part of the rivalry between the different civilizational systems adopted by different countries in the information space by use of special means to control information resources as information weapons.[11]

Darczewska further describes the logic behind the Russian conduct of information warfare and argues that,

> The theory of information warfare is part of Russia's strategic culture. It is characterised by, among other features: the 'besieged fortress' syndrome; the desire to guarantee their own security without respect for the security of other countries; the authoritarian regime's fear of revolt; mythologising its own army and special forces; the desire to regulate all aspects of security, including the use of force beyond the letter of the law; imposing the principle of limited sovereignty upon its allies and neighbours; the militarisation of social and political life; and forcing an ideological image of the world upon other countries (now being presented as a confrontation between the 'American world' and the 'Russian world.'[12]

---

9 Ulrik Franke, *War by Non-Military Means: Understanding Russian Information Warfare*, FOI-R-4065-SE (Stockholm: Swedish Defense Research Agency, 2015), 14, http://dataspace.princeton.edu/jspui/handle/88435/dsp019c67wq22q.

10 Jolanta Darczewska, *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study*, no. 42 (Warsaw: Centre for Eastern Studies, 2014), 9, https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study.

11 Jolanta Darczewska, The Anatomy of Russian Information Warfare, 12.

12 Jolanta Darczewska, *The Devil is in the Details: Information Warfare in the Light of Russia's Military Doctrine*, no. 50 (Warsaw: Centre for Eastern Studies, 2015), 7–8, https://www.files.ethz.ch/isn/191967/pw_50_ang_the-devil-is-in_net.pdf.

A Russian official document, the *Conceptual* Views *on The Activity of The Armed Forces of The Russian Federation in Information Space*, defines information war as,

> confrontation between two or more states in the information space with the purpose of inflicting a damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force.[13]

"Informational confrontation," or *informatsionnoye protivoborstvo*, is another Russian government term for conflict in the information sphere, which entails two forms of influence: information-technical and information-psychological.[14] According to Timothy L. Thomas, today these two aspects are more integrated in Russian understanding of information warfare theory than ever before. He further explains how they work together,

> For example, an information-technical cyber-attack against another nation's banking industry exposes or manipulates data about the banking industry that causes fear or even information-psychological panic in the general population. Or consider how the exposure of an information-technical achievement such as the Status-6 torpedo (now known as Poseidon), which can be nuclear armed, could have an enormous impact on the information-psychological stability of a U.S. coastal region that could be a target of such a torpedo.[15]

The technical-information part of the Russian information warfare consists of information computer, intelligence systems and electronic warfare equipment. The psychological information primarily includes propaganda, disinformation and deception (*maskirovka*). Ulrik Franke also emphasizes that Russian military theorists suggest a

---

[13] Ministry of Defense of the Russian Federation. *Russian Federation Armed Forces' Information Space Activities Concept* (Moscow: Ministry of Defense of the Russian Federation, 2011), https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

[14] Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations*, DIA-11-1704-161 (Washington, DC: Defense Intelligence Agency, 2017), 38, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf.

[15] Timothy Thomas, *Russian Military Thought: Concepts and Elements*, MP190451V1 (Bedford, MA: The MITRE Corporation, 2019), 8–14, https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf.

combination of employment of psychological attack and computer attack simultaneously during a confrontation.[16] Keir Giles regarding Russian recent campaigns in the information domain suggests that,

> [Russian] information warfare can cover a vast range of different activities and processes seeking to steal, plant, interdict, manipulate, distort or destroy information. The channels and methods available for doing this cover an equally broad range, including computers, smartphones, real or invented news media, statements by leaders or celebrities, online troll campaigns, text messages, vox pops by concerned citizens, YouTube videos, or direct approaches to individual human targets.[17]

The innovative aspect in Russian information warfare today is that Russia started to implement subversive actions in cyberspace in order to pursue the military strategy while staying below the threshold of armed escalation. This is because uncertain and ambiguous features of cyberspace allow Moscow to maintain plausible deniability. For instance, taking into consideration the problem of attribution of cyberattacks the Kremlin can target an adversary's military and civilian information systems and critical infrastructure.[18] Moreover, cyberspace has enabled Russia to identify its targets, both efficiently and economically.

C. THE NEW TYPE OF WARFARE AND INITIAL PERIOD OF WAR

The reinvented "dark art" of Russia is largely based on a military concept published in 2013 by the Chief of the General Staff, General Valery Gerasimov; this concept was later dubbed the Gerasimov Doctrine or New Generation Warfare (New-Type of War). The new-type warfare concept is a set of ideas about the changing character of war that has been adopted by the Russian strategic community. Dimitry Adamsky notes that it is "an amalgamation of hard and soft power across various domains, through skillful application

---

16 Ulrik Franke, *War by Non-Military Means*, 23.

17 Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016), 4, https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook%2C%20Russian%20Information%20Warfare.pdf.

18 Kevin N. McCauley, *Russian Influence Campaigns Against the West: From the Cold War to Putin* (North Charleston, SC: CreateSpace Independent Publishing Platform, 2016), 347.

of coordinated military, diplomatic, and economic tools."[19] Robinson et al. argue that it is a Russian response to the West: "description of how warfare has evolved in general, implying an intent both to understand the threat to Russia and also to adapt and utilize the Russian state to achieve its political objectives in the future."[20] According to Gerasimov, there is a need to create a holistic theory of asymmetric operations. He discussed a new approach of employing information warfare in combination with other means. According to this concept, two innovations have been observed: The first is that the ratio of non-military and military measures is 4 to 1.[21] The second, the informational domain is considered to be added to the space-aerial, naval, and ground ones. Gerasimov argued that in contemporary military operations at strategic, operational, and tactical levels are being less differed. Furthermore, he emphasized that in modern days, wars are no longer declared, and the critical component is the role of non-military tools and their utilization during the initial period of the operation (war), which itself is a critical phase and has a direct impact on the outcome of the whole campaign. For this reason, Russia's main tactical objective is to maintain the information and situational superiority and rely on it.

In 2016, the Russian Ministry of Defense, which is mostly responsible for performing cyber-attacks, propaganda-oriented actions and inserting malware in the command and control systems of opponents, established "information operations troops."[22] Since then, observed military exercises have involved "psychological warfare and information confrontation subunits," which also reflect a shift in Russian thinking about the potential power of information warfare, which "goes to the heart of how wars are

[19] Dmitry (Dima) Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Papers 54 (Paris*:* Institut Français des Relations Internationales, November 2015), 23, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

[20] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, RR-1772-A (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1772.html.

[21] Adamsky, "Cross-Domain Coercion," 24.

[22] Keir Giles, *The Next Phase of Russian Information Warfare* (Riga: NATO StratCom COE, 2016), 4, https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

won—whether by destroying the enemy or by rendering the enemy unable to fight."[23] According to Stephen Blank, who is an expert on Russia and the former Soviet Union, "Russia has integrated cyber and information warfare organically into its planning and capabilities to project power."[24]

D. REFLEXIVE CONTROL

Russia's contemporary "informational confrontation" against its perceived adversaries is based upon Soviet era methods and is a core of psychological warfare. Hence, exploring the theory of reflexive control can facilitate in further analysis of the Russian perspective on information warfare. The concept of reflexive control originated in the Soviet Union in the 1960s and has been more or less continuously developed ever since. According to one study, "the ultimate goal of reflexive control is that the object of control will not be aware of the manipulation."[25] Hence, methods of reflexive control are similar to the deception concept and also include spreading false information to influence the decision-making process. Reflexive control can be defined as "a means of conveying to a partner or an adversary specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[26] It should be noted that Thomas sees this concept as a subset of information warfare and suggests that Russia used it extensively in Ukraine when it employed influence operations in information space.[27]

---

[23] Keir Giles, *Assessing Russia's Reorganized and Rearmed Military*, Task Force on U.S. Policy Toward Russia, Ukraine, and Eurasia (Washington, DC: Carnegie Endowment for International Peace, 2017), 9, https://carnegieendowment.org/files/5.4.2017_Keir_Giles_RussiaMilitary.pdf.

[24] Stephen Blank, "Cyber War and Information War à La Russe," in *Understanding Cyber Conflict: 14 Analogies*, ed. George Perkovich and Ariel E. Levite (Washington, DC: Carnegie Endowment for International Peace, 2017), 81, https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_FullText.pdf.

[25] Aki-Mauri Huhtinen, Noora Kotilanen, Saara Särmä and Mikko Streng, "Information Influence in Hybrid Environment: Reflexive Control as an Analytical Tool for Understanding Warfare in Social Media," International Journal of Cyber Warfare and Terrorism 9, no3. (July-September)2019: 12. https://doi.org/10.4018/IJCWT.2019070101.

[26] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," The Journal of Slavic Military Studies 17, no. 2 (June 2004):237, https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

[27] Timothy Thomas, "Russia's 21st Century Information War: Working to undermine and destabilize populations," *Defense Strategic Communications*, no.1 (January 2015): 15, https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations.

Thomas also argues that even an e-mail phishing attempt might be considered as an operation that entails reflexive control elements, because it aims to influence a target's action, which will allow a virus to penetrate into the system.[28] Valeriano, Jensen, and Maness emphasize that especially, Russia's multimedia propaganda efforts are designed according to the abovementioned concept.[29]

As reflected during the crisis in Ukraine, in order to avoid attribution, the military operations were highly deceptive. They were characterized by mixed coercive and subversive elements and included both military and non-military components in order to create confusion and influence effective decision-making. Rod Thornton further suggests that the Russian "new approach" was designed to generate defeatism—the adversary is passively persuaded to accept Russian occupation or they becomes convinced that confrontation will lead to destruction.[30] Hence, the idea is to win "hearts and minds" first and, if that is not possible, then pursue tactics of coercion and intimidation. The Ukraine conflict is a vivid example of how Russia sees cyber activity as a subcategory and enabler of information warfare.[31] The cyber features enable information operations for reflexive control because the target audience does not apprehend that its manipulation process is ongoing. Moreover, cyberspace provides more probability to mask the identity and source of the attack and also, maintain plausible deniability.

Posard, Marrone, and Helmus from RAND Corporation argue that the reflexive control theory "assumes that people live in a polarized world of cooperation versus conflict."[32] They further note that, "the end goal for these efforts is to trigger emotional reactions and drive people to ideological extremes, making it nearly impossible to build a

---

[28] Thomas, "Russian Military Thought: Concepts and Elements," 7–7.

[29] Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Coercion: The Evolving Character of Cyber Power and Strategy* (New York, NY: Oxford University Press, 2018), 111.

[30] Rod Thornton, "The Changing Nature of Modern Warfare," *The RUSI Journal* 160, no. 4 (September 2015): 42, https://doi.org/10.1080/03071847.2015.1079047.

[31] Keir Giles, "The Next Phase of Russian Information Warfare," 4.

[32] Marek N. Posard, James V. Marrone, and Todd C. Helmus, "How You can Fight Russia's Plans to Troll Americans During Campaign 2020," *The RAND Blog,* July 14, 2020. https://www.rand.org/blog/2020/07/how-you-can-fight-russias-plans-to-troll-americans.html.

consensus. The Russians also hope those who are not driven to extreme positions will throw up their hands in frustration and check out. The result is political paralysis."[33]

E. RUSSIA'S ACTIVITIES IN CYBERSPACE

Emerging cyber capabilities create new opportunities and challenges for the various actors in the world to engage in a new type of interaction for social and political reasons. Ryan Maness and Brandon Valeriano support the claim that cyber is a tactic and one of the instruments of a threat in diplomacy and international relations available at states' disposal.[34] Also, Jensen et al. note that cyber operations "represent a weak form of coercive diplomacy" and "digital intrusions are meant to be used with other sticks and carrots to shape an adversary's decision-making."[35]

Dyadic Cyber Incident and Dispute Dataset (DCID), Version 1.1, which covers publicly attributed cyber incidents between states from 2000 and 2014, examined and analyzed 45 instances of Russian engagement.[36] Valeriano et al. contend that "more often than not, Russia fails, doubles down, and fails again."[37] Data on cyber coercive exchanges between Russia and its rivals suggest that short-term disruptions and espionage activities were the most prevalent options. In general, Russian cyber actions include the amplification of state propaganda through different online media; also, using cyber disruptions, espionage, and degradation.

---

[33] Marek N. Posard, James V. Marrone, and Todd C. Helmus, "How You can Fight Russia's Plans to Troll Americans During Campaign 2020."

[34] Ryan Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society* 42, no.2 (March 2015): 302, https://journals-sagepub-com.libproxy.nps.edu/doi/pdf/10.1177/0095327X15572997?casa_token=oPwlt0xH3m4AAAAA:BiSfCl3MTmXBPU7PzQ1XQIJma6W9Of-Dss_5bvHwGAYIAZXHhw-HS7_CUoKIQ3nie9pDhqcp9q5b.

[35] Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* 42, no. 2 (January 2019): 215, https://www-tandfonline-com.libproxy.nps.edu/doi/full/10.1080/01402390.2018.1559152.

[36] Valeriano, Jensen, and Maness, *Cyber Coercion*,117-118.

[37] Valeriano, Jensen, and Maness, 110.

Valeriano et al. view cyber disruptions as a modern means for sending signals to rival states regarding its capabilities and intentions.[38] Benjamin Jensen et al. define cyber disruptions as "a low-cost, low-payoff form of cyber strategy designed to shape the larger bargaining context … pressure a rival, through either signaling the risk of crisis escalation or, in combination with propaganda efforts, undermining public confidence in existing policy preferences."[39]

Russia predominantly employs distributed denial of service (DDoS) attacks and web defacements against adversarial states. As Valeriano et al. argue, "Russia employs cyber disruption as a low-cost form of signaling escalation risks when they have a limited ability to achieve concessions through conventional means."[40] This way Moscow seeks to demonstrate the ability to inflict damage of the target's network. The first precedent occurred when the websites of the Estonian government were targeted by DDoS attacks and were defaced but had a limited coercive impact.

The Russian cyber espionage is more complex than short term cyber disruption. Cyber espionage is planned to "steal critical information or manipulate information asymmetries in a manner that produces bargaining benefits between rival states engaged in long-term competition."[41] It is perceived as a potential tool and an enabler for a long-term influence operation.

Furthermore, Jensen et al. draw attention to two aspects. First, cyber espionage, in the event of network penetration, has a potential to prepare the ground for future operations. As explained, "not only do you access critical networks and steal information altering the balance of information in a crisis, but even if the intrusion is revealed, the target is left wondering what else was stolen and what other networks are compromised."[42] Second, cyber espionage can be a low-cost tool for manipulation of a target audience's perceptions.

---

[38] Valeriano, Jensen, and Maness, 36.

[39] Jensen, Valeriano, and Maness, "Fancy Bears and Digital Trolls," 216.

[40] Valeriano, Jensen, and Maness, 124.

[41] Jensen, Valeriano, and Maness, "Fancy Bears and Digital Trolls," 216.

[42] Jensen, Valeriano, and Maness, 219.

However, as examined by Valeriano et al., cyber degradation, which is a costlier signaling option than cyber disruption or espionage, "is more likely to have a compellent effect than disruptions or espionage."[43]

On February 26, 2015, the U.S. director of National Intelligence Gen. James Clapper stated that Russia was ready to conduct offensive cyber operations with engagement of newly established cyber command.[44] He further emphasized,

> Computer security studies assert that unspecified Russian cyber actors are developing means to access industrial control systems (ICS) remotely. These systems manage critical infrastructures such as electric power grids, urban mass transit systems, air traffic control, and oil and gas distribution networks. These unspecified Russian actors have successfully compromised the product supply chains of three ICS vendors so that customers download exploitative malware directly from the vendors' websites along with routine software updates, according to private sector cybersecurity experts.[45]

On December 23, 2015, more than 230,000 people in the region of Ivano-Frankivsk, Ukraine lost electricity for 6 hours as result of the cyber-attack. The perpetrators also carried out a coordinated telephone DDoS attack against the company itself, thus, crashing communication with the customers. However, it should be mentioned that clear attribution of the attack to the Russian Federation has not been committed.

The Kremlin uses cyber means for waging a modern form of political warfare. As mentioned earlier, Russia's actions in cyberspace have a similar patterns both in peacetime and in wartime—Russia uses low-cost, unsophisticated cyber techniques to disseminate malign propaganda and sows discontent within the targeted country, "while signaling the risk of escalation."[46] Moreover, despite having moderate cyber power, Russia is one of the most determined and active players in terms of conducting offensive operations in cyberspace.[47] This is due to the modern information ecosystem, which is characterized by

---

[43] Jensen, Valeriano, and Maness, 216.

[44] Stephen Blank, "Cyber War and Information War à La Russe," 81.

[45] Statement for the Record: Worldwide Cyber Threats, House Permanent Select Committee on Intelligence (2015), https://fas.org/irp/congress/2015_hr/091015clapper.pdf.

[46] Valeriano, Jensen, and Maness, *Cyber Coercion,* 111.

[47] Valeriano, Jensen, and Maness, *Cyber Coercion,* 74.

non-existing entry barriers that have given Moscow the opportunity to design less sophisticated and low-cost operations "to shape public opinion and signal resolve."[48] However, it should be noted that Russia rarely employs sophisticated cyber methods and preferred to strike on non-governmental and non-military institutions. Also, Russia's coercive actions have never caused any escalation beside diplomatic and economic sanctions, which actually coincided with the use of military power from Russia's side as well.

There is another aspect of Russia's hostile campaign in cyberspace, which should be emphasized, and which makes Russia exclusively notorious—the Kremlin and cyber proxies. After the fall of the Soviet Union, the grave economic situation caused by mass unemployment and the unstable political environment turned many computer-savvy citizens into criminal-minded hackers. Russia as a rogue actor has established relationships with cyber-criminal organizations and individuals who can act as proxies and conduct various types of cyber operations against other states without leaving conspicuous traces.[49]

Russia utilizes formal and informal resources to implement its malign influence campaigns. Russian Special Forces, Federal Security Service, and Main Directorate of the General Staff of the Armed Forces often are engaged in the aforementioned activities as well. The Russian law enforcement agencies indirectly sanction cyber-criminals to target third parties outside Russian territory. They do not respond to international requests to cooperate in investigation processes where Russian citizens are allegedly in connection with the crime. Moreover, they monitor cyber-criminals and enter into a proxy relationship that allows the latter to avoid arrest and stay under state "protection." In return, the system gets individuals who in particular circumstances serve the Kremlin's interests.

There are four distinct patterns of relationship between the Russian state and cyber proxies.

---

[48] Valeriano, Jensen, and Maness, *Cyber Coercion*, 110.

[49] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom: Cambridge University Press, 2018), 94.

1. **Sanctioning in peacetime**. The 2007 DDoS attack on Estonia was the first example of a peacetime period attack by the Kremlin-affiliated group, which conducted a sophisticated attack on Estonian government and business websites.

2. **Sanctioning in wartime**. Since the start of hostilities in Ukraine, offensive cyber operations have been conducted concurrently against Ukrainian private and state organizations, that entailed attacks on critical infrastructure and governmental agencies. Alongside the Russian government, CyberBerkut and other pro-Russian actors that have carried out several cyber operations.

3. **Blitz orchestration**. According to the various studies, in the Russo-Georgian war of 2008, close cooperation was observed between Russian military and civilian cyber attackers because the timing of the cyber operation coincided with military maneuvers.

4. **Sanctioning and mobilizing**. FSB representatives organized a criminal group to hack Yahoo network and gain access to sensitive information. Moreover, the Russian government did not comply with Interpol and ignored the Red Notice on one of the members of the group.[50]

Apart from Russian governmental agencies, Russian state-sponsored media is also engaged in disinformation and influence campaigns. For instance, falsified information is disseminated to mislead target audiences by presenting them biased information that serves Russian foreign policy goals. For instance, one of the state-sponsored media outlets, Russia Today, rebranded later as RT, was founded in December 2005 for the purpose of promoting a positive image of Russia abroad. Today it reaches "over 644 million people in more than 100 countries and available in more than 2.7 million hotel rooms."[51] As Lithuanian

[50] Tim Maurer, *Cyber Mercenaries*, 97–106.

[51] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, 66.

Minister for Foreign Affairs Linas Linkevicus noted, "Russia Today's propaganda machine is no less destructive than the military machine in Crimea."[52]

"Informational Confrontation" is based upon psychological warfare and is one of the main aspects of the Russian approach. In general, the 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. In order to change or manipulate information, Russia widely uses a group of controlled internet users who have been identified to attack social media posts and news pieces countering the pro-Russian narrative. In fact, it is a paid commentator army of so-called trolls, which is the innovative instrument at Putin's disposal.[53] The largest grouping of hired trolls is the infamous the Internet Research Agency (IRA), which is funded by the Kremlin. According to Robinson et. al. "these groups regularly post information to websites in Russia and abroad to reflect the regime's point of view, cast doubt on Western narratives, or otherwise influence public opinion."[54] 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 is the numerous internet bots controlled by the Kremlin, which essentially applications that automatically spread content throughout social media.[55]

Putin sees the information space as a lever for advancing his core interests, whereas cyber capabilities are additional enablers to it. Informational dominance is pivotal for the Kremlin. Moreover, patterns of an evolving media environment and the modern

---

[52] Bret Perry, "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations," *Small Wars Journal*, August 14, 2015, https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera.

[53] Krishnadev Calamur, "What Is the Internet Research Agency," *Atlantic*, February 16, 2018, https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/.

[54] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, 64.

[55] Adrian Chen, "What Mueller's Indictment Reveals About Russia's Internet Research Agency," *New Yorker*, February 17, 2018, https://www.newyorker.com/news/news-desk/what-muellers-indictment-reveals-about-russias-internet-research-agency.

information ecosystem have bolstered Russia's perspective in achieving its strategic goals by utilizing cyber-enabled information operations as well. According to Scott Jasper, these capabilities give Moscow a covert means to achieve its objectives and at the same time maintain plausible deniability.[56] Moreover, Janis Berzins from Latvian National Defense Academy notes that some of Russia's new guidelines for building military capabilities in the nearest future envisages a focus more on direct influence rather than on direct destruction and champion contactless war instead of direct clash.[57]

F. CONCLUSION

Within the last 20 years, the Kremlin had an attempt to use technology and the internet in pursuit of its broader political goals. This was motivated by the belief that character of war has changed and with the advent of the information revolution the future battlefield would require totally new approaches. As a result, the Kremlin decided to focus on outweighing its own shortcomings and disadvantages through digitalized subversive and covert actions. This Russian political warfare tactics has a focus on division and deception of the enemy that is similar to the old Soviet methods. However, modern technologies allowed Russia to refine its signature moves and adjust them to adjust contemporary environment. Russia has excelled in framing discussions in a way that serves Russian interests. This becomes extremely dangerous in times of crisis, because Moscow can dominate and transmit another reality. Having this in mind, Russia most likely will continue to develop and expand its information tools of influence with the same success. However, the empirical analysis based on the most well-known cases suggest that the Kremlin has not received any significant gains as a result of its hostile cyber actions so far.[58] Russia's cyber coercion efforts have not been effective and signaling escalation risks have not been communicated successfully.

---

[56] Scott Jasper and Keith Alexander, *Russian Cyber Operations,* 71.

[57] Janis Berzins, *Russia's New Generation Warfare in Ukraine*, №02 (Riga: National Defense Academy of Latvia, 2014), 5, https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf.

[58] Valeriano, Jensen, and Maness, *Cyber Coercion,* 110.

Russia's cyber strategy resemble concepts of active measures and reflexive control from the Soviet period that entailed deception, information manipulation and disinformation as integral parts of the state policy. These days, one of the main objectives for Moscow is to utilize the information domain to its maximum extent and shape the target population's opinion both within Russia and beyond its borders as well.

Undoubtedly, Georgia is not and will not be an exception in the near future. The Kremlin will continue to undermine Georgia's development and democratization process by attempts to sow chaos and facilitate destabilization. Georgia's official document, Strategic Defense Review 2017–2020 emphasizes that Russia seeks "to limit international political support for Georgia and weaken cooperation directed at strengthening of defense capabilities."[59] Presumably, Moscow will predominantly rely on the elements of its soft power "to ensure the weakening of state institutions, strengthening of pro-Russian civil and political movements and discredit pro-Western foreign policy agenda."[60]

It appears that information warfare has become the *modus operandi* of Putin's regime.[61] The next chapter will discuss the major cyber incidents that targeted Georgia and has been attributed to the Russian Federation.

[59] Ministry of Defense, *Strategic Defense Review 2017–2020* (Tbilisi, Georgia: Ministry of Defense, 2017), 54, https://mod.gov.ge/en/page/73/strategic-defence-review.

[60] Ministry of Defense, Strategic Defense Review 2017–2020, 54.

[61] Deborah Yarsike Ball, *Protecting Falsehoods with a Bodyguard of Lies: Putin's Use of Information Warfare*, No.136 (Rome: Research Division-NATO Defense College, 2017), 2, https://www.ndc.nato.int/news/news.php?icode=1017.

III. GEORGIA'S RUSSIAN THREAT IN CYBERSPACE

A. INTRODUCTION

After the end of the August War 2008, it soon became clear that Moscow would use all types of instruments in the future to continue pressuring pro-Western Georgia in order to coerce and convince Tbilisi to accept the so-called "new geopolitical reality"—the loss of its two historic regions of Abkhazia and Tshkhinvali ("South Ossetia").[62] One of the main objectives of invasion was to cement Russia's military presence in the country and thereby hinder Georgia's Western orientation. Since then, Russia has become more aggressive and has stressed its interest in reclaiming the sphere of influence over the so-called "near abroad." Moscow has utilized cyberspace to conduct cyberattacks and information operations to expose Georgia's vulnerability and upset the country's national security frameworks. In response to these subversions, Tbilisi continues to develop and strives to join European Union and NATO. For this reason, Russia sees Georgia's pro-Western policy as a threat and the country itself as one of the battlegrounds in its confrontation with the West.

This chapter will demonstrate the threats that Georgia faces from Russia in the cyber domain by looking at various Georgian official documents pertaining to its cyber posture and four cyberattacks on the state from 2008 to 2020, which have been attributed to the Russian Federation.

B. SECURING CYBERSPACE IN GEORGIA

For Georgia, as an object of Russia's constant targeting, securing and defending its cyberspace is a national security priority. According to the annual report of 2018 of the State Security Service of Georgia (SSSG),

> it has been established that foreign countries and their special services have been using cyber capabilities more and more actively, in their own interests. Conducting cyberattacks and cyber intelligence operations against government and critical infrastructure objects by special services of foreign

[62] Alexander Rondeli, *Georgia—Russia: From Negative to Positive Uncertainty*, #3 (Tbilisi, Georgia: GFSIS, 2013), 3, https://www.gfsis.org/files/library/opinion-papers/3-expert-opinion-eng.pdf.

countries and hacker groups controlled by them also represent a major risk to the security of the country.[63]

Georgia has acknowledged the cyberthreats and has sought to address them in its policy documents. According to the National Security Concept of Georgia, strengthening the security of the cyberspace and ensuring safety of electronic information is one of the main interests for Georgia. Moreover, lessons from the cyberattacks during the 2008 Russian-Georgian war and the subsequent evolving cyber threats have invigorated cybersecurity policy of Georgia.

Today, threats stemming from the Russian Federation remain among the top security challenges for Georgia, according to Georgia's Strategic Defense Review (SDR) of 2017–2020, which was published in April 2017. The SDR describes the future priorities of the Ministry of Defense and the Georgian Armed Forces, and also outlines the new structure that the armed forces hope to achieve by 2020. According to the SDR, Russia has an aggressive foreign policy, which is "a special threat for Georgia's security environment."[64] The authors of the SDR also note that Russia seeks to strengthen its satellite groups, weaken state institutions and discredit Georgia's pro-Western foreign policy.

It should be noted that, these undermining activities are in line with the Russia's perception on soft power, which is the integral part of Russia's "new way of war." For instance, Vladimir Putin in 2012 stated that soft power is "a matrix of tools and methods to reach foreign policy goals without the use of arms but exerting information and other levers of influence."[65] However, it diametrically differs from the Western conceptualization. Alexander Dolinsky makes an interesting observation and argues that

---

[63] State Security Service of Georgia, *The Report of the State Security Service of Georgia*, (Tbilisi: State Security Service of Georgia, 2019), 11, https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/SSSG%20Report%202018.pdf.

[64] Government of Georgia, Strategic Defense Review 2017–2020, 48.

[65] Peter Pomerantsev and Michael Weiss, *How the Kremlin Weaponizes Information, Culture and Money* (New York, NY: The Institute of Modern Russia, 2014), 12, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

"if the Western vision is based on building attractiveness, the Kremlin believes soft power to be a set of tools for manipulation."[66]

Prior to the SDR, the government of Georgia published its second cybersecurity strategy for the period 2017 to 2018.[67] The strategy identified the Russian Federation as a key threat to Georgia's critical infrastructure for the following reasons: the Russian Federation has not changed its aggressive cyber-policies, the Russian Federation has significantly enhanced its capabilities in the area of cyberattacks, and finally, the Russian Federation has significantly improved technical cyber applications in the areas of psychological influence. Since 2008, the dependence of Georgia on informational and communication technologies has significantly increased its exposure to cyberattacks. With this in mind and with cyberattacks on the rise, the threat landscape is constantly evolving. Indeed, these massive cyberattacks against Georgia, which are discussed below, are unsettling and highlight Georgia's deep security vulnerabilities.

C. THE AUGUST WAR 2008

The Russian-Georgia war of 2008 was the first time that Russia used combination of coordinated cyber and information operations in support of its military campaign.[68] It was conducted by the so-called patriotic hackers and resembled the same method that Russia used in Estonia in 2007, when numerous financial and governmental institution networks became victims of cyberattacks. In particular, webpages became defaced and targeted by distributed denial of service (DDoS) attacks and website defacements.[69] The computer network operations have several objectives that entail the disruption, degradation or collection of information from the enemy. However, in the 2008 war, Russia pioneered in the utilization of cyberspace in order to create informational and psychological

66 Peter Pomerantsev and Michael Weiss, 12.

67 Government of Georgia, *National Cybersecurity Strategy of Georgia 2017–2018* (Tbilisi, Georgia: Government of Georgia, 2017), 7, http://gov.ge/files/469_59439_212523_14.pdf.

68 Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle, PA: U.S. Army War College, 2011), 44.

69 Sarah P. White, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War* (West Point, NY: Modern War Institute, 2018), 1, https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.

superiority for shaping the favorable narrative during the initial period of war. Moreover, Russia engaged cyber proxies in the conflict, which "ranged from the citizen hackers who perpetrated the attacks to the private companies who were relied on to defend against them."[70] This could be conceived as a part of a very organic relationships between criminals and government agencies that have emerged in post-Soviet Russia. Also, for several experts, such ties provide additional grounds to argue that the offensive cyber operations against Georgia were carried out by Russian criminals but orchestrated by the Russian government.[71]

Reports suggest that about two weeks prior to the active phase of the conflict, Georgian government webpages were already targeted by malicious activities.[72] The initial cyberattack at the end of July did not caused significant damage and served as a reconnaissance for the major attacks. However, as the Russian military advanced into Georgian territory, the cyberattacks intensified and became more sophisticated. The most active period was synchronized with the Russian major military offensive of Georgia from August 7 to 12. At the same time, it coincided with "rapid mobilization of non-state actors to project coercive (cyber) power, in the form of a DDoS attack."[73] Most analysts agree that command-and-control servers for these operation were located in Russia and the DDoS attack was coordinated through Russian hacker forums. Instructions for the attack were posted on different Russian sites so that every random visitor could have participated. As a result, a series of coordinated cyberattacks were carried out on the web pages of the Ministries of Internal and Foreign Affairs of Georgia, media outlets and National Bank. These DDoS attacks on average lasted approximately two hours and fifteen minutes, and the longest lasted six hours.[74] Some even argue that despite the fact that "internet

---

[70] Sarah P. White, "Understanding Cyberwarfare," 2.

[71] Tim Maurer, Cyber Mercenaries, 102.

[72] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1.

[73] Tim Maurer, Cyber Mercenaries, 101.

[74] Ronald J. Deibert, Rafael Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (February 1, 2012), 10, https://doi.org/10.1177/0967010611431079

penetration in Georgia was low, and the area of conflict was not fully plugged in to the global information environment," the cyber component "played a significant, if not decisive role in the conflict—as an object of contestation and as a vector for generating strategic effects and outcomes."[75] However, it is less likely that DDoS attacks and web defacements could have affected military decision making and Georgian conventional force capabilities.[76] What Russia really achieved was the psychological impact, that it was able to hinder central government of Georgia to interact with its own population.

It is noteworthy that the August War in 2008 served as a harbinger for future contingencies, which should have been a wakeup call for the West. However, as the Ukrainian crisis showed, still there was a huge surprise component in Russia's tactics. The Russia's military campaign in Georgia demonstrated that a similar type of cyberattack and information campaign had the potential to develop further and also, to bring more severe consequences for a target country, that is more dependent on modern information technologies. As noted by Ronald Heickerö,

> The new modus operandi gives deniability for actors in combination with strategic benefits such as obtaining political goals. The possibility to deny any involvement could be a tempting driver for an aggressor. The implication is that the IW weapon will be used more in future conflicts both as a stand-alone method and in conjunction with military operations.[77]

Also, it should be mentioned that compared to previous experiences in Chechnya, Russia acted significantly savvier in 2008 in dealing with the media.[78] The Kremlin appeared to have taken into account the way how the U.S. used to hold briefings during the Iraq and Afghanistan campaigns and tried to mimic them. The Russians had a narrative prepared and tried to effectively spread it during the initial period of war. It should be emphasized, that the Kremlin had such an enormous desire to cooperate with the Russian

---

[75] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace," 4.

[76] White, "Understanding Cyberwarfare," 1.

[77] Roland Heickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, FOI-R-2970-SE (Stockholm: Swedish Defense Research Agency, 2010), 54, http://www.highseclabs.com/data/foir2970.pdf.

[78] Ariel Cohen and Robert E. Hamilton, The Russian Military and the Georgia War, 47.

media that it flew about fifty media representatives to Tskhinvali ("South Ossetia") several days prior to the invasion. This fact is another clear indication how Russia prepared the military operation.

D. GEORBOT CASE

The GEORBOT case took place in March 2011. The Georgian Computer Emergency Response Team (CERT) and computer experts discovered that the hackers, who allegedly were affiliated with Russian intelligence agencies, had infected between 300 and 400 computers across six Georgian government agencies.[79] This compromised botnet was nicknamed "GEORBOT" and it executed a specific task,

> The malicious software was programmed to search for specific keywords—such as USA, Russia, NATO and CIA—in Microsoft Word documents and PDFs, and was eventually modified to record audio and take screenshots. The documents were deleted within a few minutes from the drop servers, after the hacker had copied the files to his own PC.[80]

As a first step the CERT disconnected the command-and-control servers. This made hackers aware that they had been discovered, but still they decided to continue and increase the stealthiness of the operation.[81] However, they failed, and the Georgian CERT managed to identify them as a possible Russian intelligence affiliated group. The Georgians decided to "hack back" and designed a honeypot for that. As a result, the Russian hackers stole a compromised "Georgian-NATO Agreement" file that allowed the Georgians to take control over the hacker's computer, collect information regarding further targets and even film a short video of the hacker. Obviously, Georgian CERT did not receive any cooperation from Moscow's law enforcement authorities in order to proceed with this case.

---

79 Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013), 151.

80 Jeremy Kirk, "Georgian Cyber Counterattack Exposes Russian Hacker Seeking NATO Document," *Atlantic Council*, November 4, 2012, https://www.atlanticcouncil.org/blogs/natosource/georgian-cyber-counterattack-exposes-russian-hacker-seeking-nato-document/.

81 Thomas Rid, Cyber War Will Not Take Place, 151.

Apart from another example of Russia's cyber espionage, this case addresses the problem of attribution. Thomas Rid makes a very interesting observation regarding the GEORBOT case,

> The GEORBOT incident is probably the only detailed example of a successful case of active attribution on the public domain. But perhaps its most unusual feature is the fact that the Georgian government made the information public. Most intelligence agencies and their governments are highly reluctant to publicize such operations, for that could reveal vulnerabilities, tactics, skills, and create potential political blowback. Yet, if a small and technologically limited agency like Georgia's Ministry of Justice can pull off an active attribution operation in a legally grey area, then the assumption is reasonable that mighty and highly specialized intelligence agencies of the world's most technologically sophisticated powers can achieve a much higher degree of attribution.[82]

This assumption dates from 2011 to 2013. The next incident, which took place in 2019 basically echoes what Thomas Rid suggested here.

E. THE OCTOBER CASE

On October 28, 2019, the cyberattacks were launched on the websites and servers of Georgian governmental agencies and private organizations. As a result, almost fifty thousand webpages were defaced and attacked through a distributed denial of service (DDoS). For "website defacement" the hackers used an image of the former president of Georgia, Mikhail Saakashvili, to replace the original content. Presumably, the hacker sought to add a political ground to an attack and a had an attempt of a political trolling that aimed to cause unrest in Georgian society.[83] Meanwhile, some of the fringe Georgian media outlets and Russian *Sputnik* attributed the cyberattack to Saakashvili. It should be noted that this time the attack was not very sophisticated, which in fact, is a Russian pattern too. The negative psychological effect, which is a growing perception of insecurity and obfuscation in public is what the Kremlin predominantly expects to achieve from this type

[82] Thomas Rid, Cyber War Will Not Take Place, 152.

[83] Givi Gogitashvili, "Russia's 2019 Cyber Attack against Georgia Followed by Full-Spectrum Propaganda Effort," *Medium*, April 23, 2020, https://medium.com/dfrlab/russias-2019-cyber-attack-against-georgia-followed-by-full-spectrum-propaganda-effort-4460673cb3e9.

of incidents. To this end, Moscow does not require to invest more and design costly cyber operations that can paralyze the critical infrastructure and have more destructive effect.

On February 20, 2020, as a result of investigation and cooperation with Georgia, the United Kingdom and the United States published the statement, which said that the cyber actor behind the October attack was the Main Center for Special Technologies, also known as "Unit 74455" of the Russian General Staff Main Intelligence Directorate, namely, the Russian military intelligence service.[84] The UK government once again underscored in its statement that this group was responsible for the cyberattack on Ukraine's electricity grid in December 2015 and the NotPetya cyberattack in June 2017. The United Kingdom assessed the correctness of its attribution as "almost certain" (95 percent + probability).[85]

It should be mentioned that on October 15, 2020, Department of Justice has reinforced the allegations and announced that six officers of the unit were charged in connection with destabilizing various computer attacks for "the strategic benefit of Russia."[86] The illegal activities among others also included NotPetya and the on Georgian networks.

Prior to the attack, on October 22, 2019, the U.S. House of Representatives unanimously passed the Georgia Support Act (H.R.598), once again underscoring U.S. support for the independence and sovereignty of Georgia.[87] It deals with several topics related to Georgia's general security and cybersecurity theme as well. The cooperation section regarding cyber portion stipulates that the United States will do the following,

---

[84] Ryan Browne, "US and UK Accuse Russia of Major Cyber Attack on Georgia," *CNN*, February 20, 2020, https://www.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html.

[85] "UK Condemns Russia's GRU over Georgia Cyber-Attacks," UK Government, February 20, 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

[86] "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Department of Justice, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[87] George Tsereteli, "Russian Cyberattack on Georgia Shows Why the U.S. Should Pass the Georgia Support Act," *Atlantic Council*, June 9, 2020), https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-cyberattack-on-georgia-shows-why-the-us-should-pass-the-georgia-support-act/.

> (1) Provide Georgia such support as may be necessary to secure government computer networks from malicious cyber intrusions, particularly such networks that defend the critical infrastructure; (2) Provide Georgia support in reducing reliance on Russian information and communications technology; (3) Assist Georgia to build its capacity, expand cybersecurity information sharing, and cooperate on international cyberspace efforts.[88]

While scrutinizing the Georgia Support Act, it is difficult not to see connections between this initiative, which focused on cybersecurity cooperation, and the October cyberattack. Furthermore, this operation had been carried out shortly after Georgia's Defense Minister held a bilateral meeting with NATO Secretary General at NATO headquarters in Brussels.[89]

F. THE LUGAR LAB CASE

Apart from cyber intrusions, Russia's "crown jewel" in the twenty-first century political warfare is a dissemination of propaganda and disinformation by employing state-sponsored media, infamous Internet Research Agency (IRA), and agents of influence. It should be mentioned that the IRA is a Kremlin-backed organization, also known as the "troll farm," which is a cornerstone of the modern Russian information warfare. It operates thousands of fake twitter and Facebook accounts to run different types influence operations. For instance, according to a study conducted by RAND corporation,

> In October 2017, news broke that Russia had exploited Facebook as part of its information campaign. The Internet Research Agency created dozens of Facebook pages that sought to exploit and expand various social division created dozens of Facebook pages that sought to exploit and expand various social divisions within the United States that included race, religion, political affiliation, and class. These pages used Facebook advertising algorithms to target the ads to populations most vulnerable to the intended message.[90]

---

88 Georgia Support Act, H.R.598, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/598/text.

89 "Bilateral Meeting with the Minister of Defense of Georgia," *NATO*, October 25, 2019, http://www.nato.int/cps/en/natohq/photos_169927.htm.

90 Christian Bills, "The Internet Research Agency: Spreading Disinformation," *Small Wars Journal*, October 30, 2020, https://smallwarsjournal.com/jrnl/art/internet-research-agency-spreading-disinformation.

In this light, it is noteworthy that the some of the most vulnerable members of Georgian society live within the occupied regions of Georgia that have been targeted by the Kremlin's information warfare. For instance, in 2017, a massive disinformation campaign was launched against Central Public Health Reference Laboratory (Lugar Lab, named after U.S. senator Richard Lugar). Russian-controlled de facto Tskhinvali (South Ossetia) representatives accused the central government of Georgia for outbreaks of pandemic diseases of humans and animals in Georgia.

Later, in October 2018, the misleading narrative had been amplified by Russian Maj. Gen. Igor Kirilov, who stated that "it's highly likely that the U.S. is building up its military biological potential under the cover of studying protective means and conducting other peaceful research, flouting international agreements."[91] He also claimed that these activities might have been the reason to the spread of viral infections in the southern part of Russia. According to him, "the near simultaneous deaths of a large number of volunteers give reason to believe that the Lugar Center was researching a highly toxic and highly lethal chemical or biological agent."[92]

In December 2018, a known Russian-sponsored media source, *Sputnik News*, released an article entitled "Russia Concerned over U.S. Biological Activities in Georgia."[93] The article freely drew conclusions without sufficient information and was based on an interview with the former Georgian Minister of State Security, Igor Giorgadze (affiliated with the Russian secret service), who has been accused of plotting to overthrow the Georgian leadership and now resides in Russia. In response to the article, then-Deputy Foreign Minister of Russia, Grigory Karasin, stated that "the U.S.-funded Richard Lugar Laboratory in Georgia allegedly runs biological weapons tests and expects the U.S. and Georgian authorities to provide sufficient clarification on the center's activities."[94]

---

[91] Vladimir Isachenkov, "Russia Claims U.S. Running Secret Bio Weapons Lab in Georgia," *AP*, October 4, 2018, https://apnews.com/article/0cf158200e674f41bd3026133e5e043d.

[92] Vladimir Isachekov.

[93] "Russia Concerned Over U.S. Biological Activities in Georgia - Deputy Minister," *Sputnik International*, December 19, 2018, https://sputniknews.com/world/201812191070814362-russia-us-lab/.

[94] "Russia Concerned Over U.S. Biological Activities in Georgia - Deputy Minister."

Over the course of the COVID-19 pandemic, the Kremlin has continued assaults on the Tbilisi-based Lugar Lab and intensified the spread of disinformation by making statements implicitly blaming Georgia and the United States for the severe outbreak of the coronavirus in Russia.[95] These accusations were "proactively backed by the Russian defense and foreign ministries, which released tersely worded statements that Russia would not allow the production of biological weapons near its borders."[96]

On September 4, 2020, the Ministry of Internal Affairs of Georgia stated that a malicious cyberattack had been directed to the computer systems of the Ministry of Health and Social Affairs of Georgia and on its subordinate agency, the Public Health Research Center, which operates the Lugar Lab, by one of the foreign special services. According to their statement, "part of the documentation obtained as a result of illegal entry into the system is currently uploaded on a foreign webpage and is available to the public. At the same time, these pages are loaded with obviously falsified information, deliberately forged documents aimed at intimidating the public and generating distrust."[97]

Russia's overarching objective is to undermine the West and Georgia internationally, to sow distrust between people living in the occupied regions of Georgia and people living in the rest of the country. It uses the network of propaganda distributors which is broad and interconnected. Such a network might be comprised from non-governmental organizations, political parties, media outlets, and of course the internet and social media platforms. Today, Russia relies significantly on the use of various media elements for its agents of influence. This, coupled with its cyber capabilities, represent Russia's primary tool for disrupting Georgia's Western-leaning attitudes and agenda. Thus, the Kremlin will intensify its activities below the threshold of military aggression and

95 "US Labs in Third Countries May Be Developing Pathogenic Agents - Diplomat," *TASS*, April 17, 2020, https://tass.com/politics/1146327.

96 Zaal Anjaparidze, "Russia Dusts Off Conspiracy Theories about Georgia's Lugar Center Laboratory in Midst of COVID-19 Crisis," *Eurasia Daily Monitor 17*, no.62 (May 2020), https://jamestown.org/program/russia-dusts-off-conspiracy-theories-about-georgias-lugar-center-laboratory-in-midst-of-covid-19-crisis/.

97 "Statement of The Ministry of Internal Affairs of Georgia," Ministry of Internal Affairs, September 3, 2020, https://police.ge/en/saqartvelos-shinagan-saqmeta-saministros-gantskhadeba/13926.

amplify its propaganda. More likely, the number of cyberattacks on critical infrastructure will grow as well.

G. CONCLUSION

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 to exert control over its own population and also, to acquire influence over opposing countries.

Russia's holistic approach to information warfare encompasses disinformation, propaganda, DDoS attacks and espionage. These components of information warfare technique are continuously utilized on a daily basis by the recently established cyber units of the Russian Ministry of Defense. Many other Kremlin affiliated groups are also engaged in performing "cyberattacks, propaganda-oriented actions and inserting malware in the command and control systems of opponents."[98] Russia is becoming more assertive "to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny."[99]

Furthermore, it is most likely that Moscow will continue to be opportunistic and exploit the existing environment in order to advance its strategic interests as seen during the Covid-19 pandemic situation. The global crisis caused by the virus gave impetus for Russia to intensify its political warfare agenda. This again reinforces the assumption that there are blurred lines between war and peace in the Russian understanding. As witnessed with regard the Lugar case, subversive actions in cyberspace will continue to pose critical threats to Georgia's security architecture. In particular, Russia's hostile operations in cyberspace will continue to undermine Georgia's credibility as a modern European country that can be a part of NATO or the European Union. Therefore, the Western partner

98 Andro Gotsiridze, *Russia's Cyber Activities—A Growing Threat for Georgia*, #95 (Tbilisi, Georgia: GFSIS, 2018), 4, https://www.gfsis.org/files/library/opinion-papers/95-expert-opinion-eng.pdf.

99 Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare*, 2.

countries need to focus on collaboration with Georgia in order to develop joint informational and diplomatic response measures. For instance, attribution and globally coordinated “name and shame” campaigns could limit the effectiveness of Russia’s malign information operations, because it would be harder for Russia to deny its actions and would also, raise awareness in society with regard to the problem itself.

Bearing in mind that Georgia is not the only country being affected with misleading and hostile narratives, a coordinated international approach should be a basic silver bullet for tackling the problem. Therefore, in response to the Russian threat, which is a critical threat for the West as well, Georgia needs to seek solutions on the domestic and international levels. It is important to create a cyber defense mechanism that can prevent the cognitive outcome of destructive cyber operations, in addition to the technical effects of computer network attacks. In order to counter Russian threats in cyberspace, Georgia should design and enforce an effective platform to counter fake news, disinformation and propaganda dissemination.

For finding a way forward for Georgia, the next chapter will examine how Israel and Estonia approach to their national cybersecurity and cyberdefense. Like Georgia, these two small states face security threats from much bigger and power neighboring states, which try to coerce and intimidate them. However, Israel and Estonia continue to move forward in a challenging geopolitical environment. Moreover, they timely noticed what opportunities would cyber bring and started to invest in development of cyber capacities in order to respond to some of the existing challenges for the national security and also, to outweigh their shortcomings. In addition, Georgia has historical ties with both countries and has been in close cooperation in terms of developing defensive capabilities, including cyber field as well.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CYBERSECURITY AND CYBERDEFENSE IN ISRAEL AND ESTONIA

A. INTRODUCTION

Israel and Estonia have aggregated vast experiences in mitigating risks in cyberspace and addressing modern cyber challenges. Moreover, in the past few years, they have developed a long-term vision of cyber security and cyber defense strategy and have excelled in using cyber capabilities to support their national security and conventional military operations as well. Therefore, as different countries in the world that strive to develop their cyber capabilities in order to meet the challenges related to the information age and the cyber era, advanced Israeli and Estonian models can serve as a source of learning. Furthermore, Israel and Estonia have been selected for analysis due to their special relations with Georgia, including cooperation in military and cyber spheres, which primarily focuses on sharing best practices, experiences and lessons learned.

This chapter examines two case studies of the Israeli and Estonian approaches to cybersecurity and cyber defense. Due to an unstable geopolitical environment, both Israel and Estonia perceive advanced technologies, science, and cyberspace as avenues to gain a qualitative edge over their adversaries. This aspiration stems from a severe reality that is created by existential security threats posed by rogue and powerful actors that claim the status of regional hegemon.

Israel faces a wide range of challenges in the Middle East region, which has been involved in a never-ending conflict since the end of the World War II. The current unstable security environment for Israel is largely caused by the Iran and its network of allies in the region. Moreover, Iran seeks to expand its cyber capabilities an also cooperates with foreign hacktivists as well, including the Syrian Electronic Army, Shi'a Islamist hacker groups, and Lebanese Hizballah.[100] In addition, apart from being capable of conducting series of destructive cyber-attacks—such as on Saudi ARAMCO, or on Israeli critical

[100] Quentin E. Hodson, Logan Ma, Krystina Marcinek, and Karen Schwindt, *Fighting Shadows in the Dark*, RR2961(Santa Monica, CA: RAND Corporation, 2019), 24. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf.

infrastructure—Iran has started to utilize information domain to implement "international influence campaigns promoting news and stories aligned with Iranian interests."[101] Marie Baezner argues, that Iran tries to duplicate Russia's way of waging information warfare and have built a "complex networks of fake websites and social media personas to promote anti-Saudi Arabia, anti-Israel, pro-Palestinian stories and news on U.S policies in favor of Iran."[102] It is noteworthy that, according to the cybersecurity firm FireEye, a Russian lab might be involved in developing a malware used during the Saudi ARAMCO incident.[103]

Similar to Georgia, Israel is confronted by a larger power that perceives cyber-attacks as part of a continuum of asymmetric warfare. Moreover, the strategic, tactical, and operational logic behind the Russian and Iran cyber operations appear to be similar. Both states collaborate with proxy groups and prefer less sophisticated cyber efforts to coerce, gain access to sensitive information (espionage), retaliate or signal resolve. They seek to exert influence in cyberspace by amplifying state narrative to obfuscate the target audience and attain the informational superiority. On the other hand, Israel still remains a successful model of resistance and resilience, and the nation continues to advance its interests and build a robust framework of security and defense, and in particular cyber capacity. To this reason, examining the Israeli approach with regard to addressing the cyber threats appears to be a compelling effort for Georgia, which is in the process of shaping its cyber posture.

Georgia and Estonia, both as post-Soviet states, are still perceived as a sphere of privileged interest by Russia. In addition, Estonia has a significant Russian-speaking minority. According to 2011 data, almost 30 percent of Estonia's citizens are Russian speakers, of which 25 percent perceive and identify themselves as Russians. This factor gives the Kremlin the leverage to undermine the Baltic state by internally disrupting it. For instance, in 2007, "the state's banking and public administration systems" were attacked as a result of the DDoS attack, "following a dispute with Russia over the movement of a

---

101 Marie Baezner, *Hotspot Analysis: Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions* (Zurich: Center for Security Studies, 2019), 17, https://doi.org/10.3929/ethz-b-000344841.

102 Marie Baezner, *Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions*, 17.

103 Quentin E. Hodson, Logan Ma, Krystina Marcinek, and Karen Schwindt, 26.

Soviet-era statue."[104] As Heickero notes, this incident has been "a wake-up call to highlight the risks, threats and vulnerabilities on information warfare. The operation directed against Estonia was one of the first official and publicly known cyber-attacks against a country using large-scale botnets and DDoS by nationalist-driven civilians."[105]

Despite the fact that Estonia is a member of NATOs alliance, Russia still poses a significant threat to the national security of the small Baltic state. Moreover, between 2014 and 2015, the RAND Corporation assessed the probable outcome of a Russian invasion of Estonia, Latvia, and Lithuania, concluding that the time required for "Russian forces to reach the outskirts of the Estonian and/or Latvian capitals of Tallinn and Riga, respectively, is 60 hours."[106] Russia seeks to exploit the existing weak spots use them at their advantage. Therefore, it resorts to "strategic information operations and propaganda activities that are part of campaigns designed to undermine trust in their institutions, foment ethnic and social tensions, and erode confidence in North Atlantic Treaty Organization (NATO) collective defense commitments."[107]

B. EVOLUTION OF MODERN ISRAELI CYBERSECURITY

Israel has constantly faced existential threats from state and non-state actors since its foundation. Yet the country has been coping with this complex geopolitical situation, and today, it has a reputation as a democratic state with a highly technological army. The responsibility for implementing and conducting Israel's cybersecurity and defense cyber strategy is assigned to two organizations: The Israeli National Cyber Directorate (INCD) and the Israel Defense Forces (IDF). Despite the fact that the strategy has not been

---

[104] Ronald J. Deibert, Rafael Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War,"

[105] Roland Heickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, 5.

[106] David A. Shlapak and Michael W. Johnson, *Reinforcing Deterrence NATO's Eastern Flank*, RR-1253-A(Santa Monica, CA: RAND Corporation, 2016). https://www.rand.org/pubs/research_reports/RR1253.html.

[107] Stephen J. Flanagan, Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin, *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance*, RR-2779-OSD(Santa Monica, CA: RAND Corporation, 2016), 5. https://www.rand.org/pubs/research_reports/RR2779.html.

published as a unified document, some aspects and approaches are given in different national regulations and activities.[108]

The first key event in the evolutionary ladder of Israel's national cyber security and defense policy was the establishment of a special regulatory body: The National Information Security Agency (NISA). Since its founding in 2003, NISA has worked to ensure the safety of critical infrastructure and was mandated to coordinate and supervise the implementation of governmental instructions.

The next milestone was the launch of the National Cyber Initiative, which in 2010 incentivized the first cyber-strategy design and facilitated the adoption of the Government Resolution 3611 "Promoting national capacity in cyberspace." The document noted,

> To work towards advancing national capabilities in cyberspace and improving management of current and future challenges in cyberspace. To improve the defense of national infrastructures essential for maintaining a stable and productive life in the State of Israel, and to strengthen those infrastructures, as much as possible, against cyberattack by advancing Israel's status as a center for the development of information technologies while encouraging cooperation among academia, industry, and the private sector, government ministries and special bodies.[109]

This initiative resulted in two main outcomes: first, foundation of the Israeli National Cyber Bureau (INCB), which was established in 2012 and mandated to lead and coordinate national cyber policy across the public and private sectors; and second, the promotion of research and development (R&D) in cyberspace.[110] In fact, it became the main advising body for the government in both crafting and implementation of national policy in the cyber field.

In 2015, a new operational agency—the National Cyber Security Authority (NCSA)—was established by the Israeli government to cooperate with INCB and ensure

---

[108] Deborah Housen-Couriel, *National Cyber Security Organization in Israel* (Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2017), 8, https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf.

[109] Resolution No. 3611, 1 (2011), https://www.gov.il/he/Departments/policies/2011_des3611

[110] Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel*, (Cham: Springer International Publishing, 2015), 57, https://doi.org/10.1007/978-3-319-18986-4.

the security of Israeli civilian cyberspace. Having no law-enforcement power, its main functions included guidance of the private sector and information sharing, also, acting as a regulator, and assistance in case of cyberattacks. It is noteworthy that this model was designed to focus on cooperation, develop technology, and increase societal trust as well. In addition, NCSA has incorporated the critical infrastructure protection organization—NISA, and also, has founded the National Computer Emergency Response Team (CERT-IL). According to Tabansky, it is a "central public contact point for support for all civilian non-critical sectors" and "the central pillar in the long-term effort to secure Israel's civilian sector at large."[111]

Later, in 2017, INCB and NCSA together formed the INCD in the Prime Minister's office, which was tasked with coordinating the cyber policy and building the cyber force of Israel. As a result, the defensive component of Israel's cybersecurity was transformed into a more centralized institution with a simpler hierarchy. It should be mentioned that the INCD partners with the Israel Innovation Authority and has initiated the establishment of Cyber Research Centers in Israeli universities and different innovation programs.[112]

C. CYBERSECURITY STRATEGY OF ISRAEL

The first National Cyber Security Strategy of Israel became known to public in 2017. According to the document, Israel views cyberspace "as an engine of economic growth, social welfare and national security."[113] In the same year, Israel also adopted the Digital Israel Initiative, which seeks to benefit from information and communication technologies as a means to boost the economy, and a create smart government administration.[114] In other words, the goal is to transform Israeli society into a digital and

111 Lior Tabansky, "Israel Defense Forces and National Cyber Defense," *Connections: The Quarterly Journal* 19, no. 1 (2020): 53, https://doi.org/10.11610/Connections.19.1.05.

112 Tabansky, "Israel Defense Forces and National Cyber Defense." 53–54.

113 National Cyber Directorate, *Israeli National Cyber Security Strategy in Brief* (Tel-Aviv: National Cyber Directorate, 2017), 5, http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

114 Ministry for Social Equality of Israel, *The Digital Israel National Initiative: The National Digital Program of the Government of Israel* (Tel-Aviv: Ministry for Social Equality, 2017), 25, https://www.gov.il/BlobFolder/news/digital_israel_national_plan/en/The%20National%20Digital%20Program%20of%20the%20Government%20of%20Israel.pdf.

innovative society that is governed by an electronic government (e-government). However, this new initiative, which implies the use of information and communication technologies for various interactions, automatically poses additional challenges for Israeli national security and for its cyber security in particular. Therefore, securing cyberspace is one of the main national interests of Israel and obviously, cyber security strategy serves as a practical foundation for it.

Today, Israel's cyber security strategy is "designed to efficiently structure the national efforts and to ensure a stable, long-term solution."[115] According to Jasper Frei, this document "includes both direct state actions to confront cyber risks as well as indirect efforts, which aim at supporting and collaborating with the private sector."[116] It establishes new holistic concepts and is based on the three-layer approach: Aggregate Cyber Robustness, Systemic Cyber Resilience and National Cyber Defense. Cyber Robustness aims to prevent high-level damage through the promotion of best practices, regulations, and incentives. Also, it sets high cyber security requirements for government institutions as an exemplar for private companies.[117] Conversely, Systemic Cyber Resilience focuses on confronting a cyberattack when it happens and minimizing the damage for the nation. As mentioned above, the CERT-IL, which is under the National Cyber Directorate, works actively with the private sector to develop Systemic Cyber Resilience by encouraging information sharing and offering assistance during cyber incidents.[118] For instance, this second layer is activated in the event of incidents that "do not present an immediate threat, but may cause cumulative damage over time, or might and severe a national defense response as the understanding of the threat evolves."[119]

The third layer addresses the most critical national security threats that are posed by the resource-rich attackers and are emanated from cyberspace. As Frei notes, the third

---

115 National Cyber Directorate, 5.

116 Jasper Frei, *Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations* (Zurich: Center for Security Studies, 2020), 11, https://doi.org/10.3929/ETHZ-B-000438397.

117 National Cyber Directorate, 10.

118 National Cyber Directorate, 11.

119 National Cyber DIrectorate, 13.

layer "relies on the two preceding layers and includes not only defensive measures bust also active cyberdefense and offensive actions by national security and law enforcement organs to counter both state and non-state aggression to achieve deterrence."[120]

D. THE IDF AND NATIONAL CYBERDEFENSE STRATEGY

In 2015, Israel started to regard cyberspace as a fifth domain of warfare.[121] Today, the most fundamental body in the implementation process of cyber strategy is the Israel Defense Forces, which is a central organization and perceived as a symbol of strength of the state. Apart from prime defensive functions, it is also engaged in science and in the research and development process of different spheres, such as education, high-tech industry and cybersecurity. The IDF sees cyber as a an important qualitative force multiplier and follows the logic of Israeli grand strategy that posits the importance of "the quest for qualitative superiority to balance numerical inferiority."[122] For this reason, it has been largely interested in the development of advanced technologies used in electronic warfare, information warfare, encryption and signal intelligence.[123] As Major-General Amidror notes,

> IDF, like other militaries, is pre-occupied with working out how best to integrate cyber capabilities, for both defensive and offensive purposes. Since it is clear that cyber warfare will become hugely important in the coming years, and because there is a long road ahead, the IDF is already investing considerable sums of money and highly talented personnel in this area and is engaged in the deep and broad development of its cyber capabilities.[124]

Obviously, Israel's major national security concerns are not related to the cyber domain; there are more existential challenges. However, in April 2020, a cyberattack

---

120 Frei, *Israel's National Cybersecurity and Cyberdefense Posture*, 11.

121 Baezner and Cordey, *National Cybersecurity Strategies in Comparison - Challenges for Switzerland*, (Zurich: Center for Security Studies, 2019), 26, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf.

122 Tabansky and Ben Israel, "Cybersecurity in Israel," 11.

123 Tabansky, "Israel Defense Forces and National Cyber Defense," 57.

124 Gadi Eizenkot, "Cyberspace and the Israel Defense Forces," *Cyber, Intelligence, and Security 2*, no. 3 (December 2018): 6, https://www.inss.org.il/wp-content/uploads/2019/01/Eizenkot.pdf.

allegedly conducted by Iran targeted different water and sewage treatment facilities across Israel.[125] On May 9, a cyberattack on the system that controls Iran's Shahid Rajaee port brought the system to an abrupt and inexplicable halt.[126] The IDF Chief of Staff Aviv Kochavi did not confirm his government's involvement, but he did comment that Israel would continue to act with a mix of instruments. Israel allegedly went for "hack back" and signaled its resolve by retaliating.[127] This type of incidents and the changing nature of waging war propelled the IDF to start focusing on corresponding warfare capabilities to start addressing the threats. According to Gil Baram,

> The cyber technology used in warfare affects the way the latter is conducted. … Cyber warfare technologies have the potential for enormous advantages along with new and unfamiliar risks. Given the sweeping innovation in this field, the understanding of its nature and consequences has only begun.[128]

The IDF also actively started to participate in drills and capacity building in order to secure the state in emergencies. These drills were conducted in close cooperation with the National Cyber Directorate because it plays an integral part in "defending and protecting the national cyberspace in emergencies and wartime."[129]

In 2017, the C4I (command, control, computers, communications, and intelligence) and Cyber Defense branch was unified as a branch and established within the IDF as a central entity for Israel's cyberdefense. The given mandate is to secure the IDF's communication systems and network. Also, it holds responsibility for supporting the IDF

---

125 Gil Baram and Kevjn Lim, "Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks," *Foreign Policy*, (June 2020), https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

126 Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility," *Washington Post*, May 18, 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

127 Baram and Lim, "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks."

128 Gil Baram, "The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case," Military and Strategic Affairs 5, no. 1 (May 2013): 23, https://www.inss.org.il/wp-content/uploads/systemfiles/MASA5-1Eng4_Baram.pdf.

129 Eizenkot, "Cyberspace and the Israel Defense Forces," 103.

by training its Information and Communications Technology (ICT) professions, advancing system architecture, developing cryptographic foundations and software.[130]

Unit 8200 is a subordinate to the Military Intelligence Directorate, which itself operates under the IDF, but is "an independent service that is not part of the ground forces, the Navy, or the Air Force."[131] Unit 8200 serves primarily as a signal intelligence collector and code decryption unit. According to Sean Cordey, it is was involved with such offensive and defensive cyber operations such as: Operation Orchard (2007), Stuxnet (2010), Operation Full Disclosure (2014) and the Ogero Incident (2017).[132] Unit 8200 also is mandated to perform "Computer Network Attack (CNA) and Computer Network Exploitation (CNE)."[133] In addition, this branch is considered by many as "an incubator for future very successful cybersecurity startups, technology venture capitalists, and cybersecurity experts."[134] This fact is primarily conditioned by the Israeli compulsory conscription system, which integrates Israeli citizens into its cyber security agencies.[135] As a result, "conscripts absorb the military capital, or part of it, while in service and "export" it into the civilian sphere where it converts well, especially in the hi-tech sector."[136] In fact, military background in Israeli technological field is considered as an advantage and often equals to a University degree.[137]

---

130 Tabansky, "Israel Defense Forces and National Cyber Defense," 56.

131 Tabansky, 56.

132 Sean Cordey, *The Israeli Unit 8200: An OSINT-Based Study* (Zurich: Center for Security Studies, 2020), 9, https://css.ethz.ch/en/services/digital-library/publications/publication.html/2beaf2b8-3d47-4be9-8553-18e7a8ce7c8e.

133 Tabansky, 56.

134 Cordey, *The Israeli Unit 8200,* 3.

135 Jamie Collier, "Cyber Reserves Are Not a Silver Bullet," *War on the Rocks,* May 22, 2020. https://warontherocks.com/2020/05/cyber-reserves-are-not-a-silver-bullet/

136 Tabansky, 58.

137 Ori Swed and john Sibley Butler, "Military Capital in the Israeli Hi-Tech Industry," *Armed Forces & Society 41,* no. 1(August 2013): 131.

It should be noted that Israel had planned to establish a central cyber command, but later decided to keep its defensive and offensive military capacities manner.[138] According to Lior Tabansky, enhanced national cybersecurity can be based on the following general strategies: 1. In order to provide additional cybersecurity, the military should be permitted to operate within domestic civilian cyberspace, and 2. Conventional defense forces should be reduced and new civilian organizations established for cybersecurity. He further notes, that bearing in mind the success of Israel in civilian cybersecurity, eventually more novelties are to be foreseen.[139]

The IDF has focused on upgrading its capabilities in the cybersphere. For instance, about 10 billion New Israeli Shekel (NIS) were invested in the Digital Ground Army project, which aim to provide "better functionality and optimization in concentrating information about the enemy, the IDF, and the combined use of IDF force."[140] Moreover, overarching changes and reorganizations entailed inter-governmental cooperation among the IDF and other state agencies like Mossad or General Security Service.

The Israeli focus on building cyber capacities represents a holistic responsive mechanism to modern cyber threats. This comprehensive approach is largely premised by the Israeli total defense model, which itself is a common feature for a small state.

E. THE ESTONIAN CYBERSECURITY AND STRATEGY

Estonia is visited by thousands of delegations each year to learn about its existing digital ecosystem.[141] For instance, 46.7 percent of Estonians used internet for voting during the European Parliament Elections.[142] Major government services have been

---

138 Judah Ari Gross, "Army Beefs up Cyber-Defense Unit as It Gives up Idea of Unified Cyber Command," *Times of Israel*, May 14, 2017, http://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/.

139 Tabansky, 61.

140 Gadi Eizenkot, "Cyberspace and the Israel Defense Forces,"103.

141 Information System Authority, *Cyber Security in Estonia 2020* (Tallinn: Information System Authority, 2020) 48, https://www.ria.ee/sites/default/files/cyber_aastaraamat_eng_web_2020.pdf.

142 Juvien Galano, "i-Voting - the Future of Elections," *e-estonia*, March 19, https://e-estonia.com/i-voting-the-future-of-elections/.

digitalized, like legislation, education, justice, health care, taxes, etc.[143] Moreover, in 2017, Estonia pioneered the world's first "Data Embassy" in Luxembourg.[144] Contrary to a traditional embassy, this data center is a cloud server that backs up Estonian e-governance networks.

In 2007, Estonia became the first country to face different forms of DDoS attacks that lasted for three weeks and had a politically motivated ground.[145] This incident served as a lesson for Estonia, despite the fact that Russia never acknowledged the attack. It created a solid basis for further Estonian development and today, Estonia is the first country in the world to have adopted a third cyber security strategy. The new Cybersecurity Strategy 2019–2022 once again highlights Estonia's long-time vision, objectives, and priority areas in the cyber domain. Objectively, Estonia is regarded as the most resilient digital society; it has absolute trust in digital public services and can cope with evolving cyber threats with great success due to the vision and principles it has embraced.

Interestingly, Estonia does not differentiate between cyber and physical domains in terms of protecting and promoting fundamental rights and freedoms. Moreover, it views digital development as a basis for socioeconomic growth and focuses on establishing an Estonian digital ecosystem. For this reason, special attention is drawn to the role of innovation in security, cryptography, and the overarching principle of open communication.[146]

The Ministry of Economic Affairs and Communications is the leading body in the area of cyber security. However, the Ministry of Defense is in charge of organizing national

---

[143] Nathan Heller, "Estonia, the Digital Republic," *New Yorker*, December 18, 2017, https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

[144] Yuliya Talmazan, "Data security meets diplomacy: Why Estonia is storing its data in Luxembourg," *NBC News*, June 25, 2019, https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171.

[145] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *International Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 24, https://doi.org/10.4018/ijcwt.2011010103.

[146] Ministry of Economic Affairs and Communications, *Cybersecurity Strategy of Republic of Estonia 2019–2022*(Tallinn: Ministry of Economic Affairs and Communications, 2019), 10, https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

cyber defense, in cooperation with the Estonian Foreign Intelligence Service, Estonian Defense Forces Cyber Command, and Cyber Defense Unit.[147]

According to the National Defense Strategy of Estonia, "the Estonian Defense League is a voluntary, militarily organized, armed, national defense organization" which is under the Ministry of Defense and mandated to develop a cyberdefense capability.[148] The first cyber defense units were formed in 2009, after the notorious 2007 cyberattacks against Estonia. On January 28, 2011, the Cyber Defense Unit (CDU) was officially established within the Estonian Defense League.[149] The mission of the CDU is to protect Estonian cyberspace, including protection of information infrastructure and support of national defense objectives.

The CDU is formed from individuals who have different backgrounds and want to contribute to cyber security. CDU objectives include several interesting and important tasks. For instance, such as the development of cooperation among qualified IT specialists, the creation of public-private partnership network, participation in international cyber security training events.

Estonia plays a key role in developing NATO's cyber defense policy. In August 2018, the Estonian Cyber Command was formed on the basis of the Headquarters Support and Signal Battalion and the Joint Headquarters. The major missions include defending the country's information systems, assisting NATO allies, and preparing for active cyber defense operations.[150]

The NATO Cooperative Cyber Defense Centre of Excellence is based in Tallinn. Its mission is to enhance capability, cooperation and information-sharing between NATO member states in cyber defense. Moreover, Estonia cooperates with NATO allies and

147 Estonian Information System Authority, *Cyber Security in Estonia 2020*, 6.

148 Estonian Ministry of Defense, *National Defense Strategy of Estonia* (Tallinn: Estonian Ministry of Defense, 2011), 13, https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

149 Information System Authority, *Cyber Security in Estonia 2020*, 36.

150 Piret Pernik, *Preparing for Cyber Conflict: Case Studies of Cyber Command* (Tallinn: International Centre For Defense and Security, 2018) 6, https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf.

partners in cyber field as well. Its primary objective is to achieve outstanding competence in conducting large-scale cyber exercises on the technical as well as strategic level. More than 1,500 cyber experts from 30 nations took part in 2019's Locked Shields exercise. Another exercise, Crossed Swords, focused on developing the tactical responsive cyber defense skills of cyber experts.[151]

The latest Estonian Cybersecurity Strategy 2019–2022 envisages four objectives along with coexisting challenges and the ways to attainment. The first objective is to address challenges posed by insufficient institutional awareness of information systems security and misperceptions about cyber threats in general in order to build a sustainable digital society. For this reason, the cybersecurity strategy aims to preserve a sustainable digital society by developing technological resilience and working towards cyber incident-related crisis prevention, preparedness, and resolution.[152]

The second objective is to support Estonian cybersecurity Research and Development (R&D), and by 2022, form a strong, innovative and globally competitive industry. The main obstacles in overcoming this are limitations in investments and the lack of Estonian cybersecurity companies in international markets.[153]

As a third strategic objective, Estonia aspires to become a top international contributor with a visible footprint, and to become a partner on cyber issues with the European Union, NATO and the United Nations. The strategy envisages regular joint exercises and information sharing within the bilateral cooperation framework.[154]

The last objective stipulated in the document is defined as the Estonian goal to build a cyber-literate society, which entails high cybersecurity awareness among its citizens, state and private sector. Estonia realized that it lacked a cyber savvy workforce and has sought to develop sufficient forward-looking human talent. Its goals are to strengthen and

---

151 Information System Authority, *Cyber Security in Estonia 2020*, 29.

152 Ministry of Economic Affairs and Communications, *Cybersecurity Strategy 2019–2022*, 14.

153 Ministry of Economic Affairs and Communications, 14.

154 Ministry of Economic Affairs and Communications, 58.

improve the skills of its mid-level officials through particular cyber defense courses and to facilitate the development of talent according to state and private demand.[155]

F. CONCLUSION

Cybersecurity remains a challenging component of broad national security and defense. Gradually, some nations have started to pursue steps similar to those taken by Estonia and Israel, focusing on digital governmental services or emerging technologies. Many countries have yet to develop an overarching cybersecurity strategy and to ensure the security of their critical infrastructure and citizens by cooperating with the private sector and the international community. The Estonian and Israeli cases demonstrate both the opportunity of the cyberspace and the threats that are related to unsecured networks and systems. They understood that investing in science, technological development, and human capital would result in a more secure cyberspace.

The Estonian and Israeli cases demonstrate both the potential severity of digital threats, and responses that states may take to safeguard against future cyberattacks. A cyber-crisis management plan at a national level is a very important element in a national cybersecurity strategy, as it focuses on the national coordination and mitigation efforts during the crisis. Many cyber-incidents occur on a daily basis and are mitigated promptly at an operational level, without necessarily leading to a crisis situation. Cyber-crisis specific procedures should explain the steps and actions that are needed during the cyber-crisis. Few countries have pursued similar steps in the direction of securing cyberspace like Estonia and Israel. Many countries have yet to develop an organization-wide cybersecurity strategy and start engaging in cooperation and information sharing globally. The use of an international engagement strategy could be considered as an instrument for fostering international cooperation.

[155] Ministry of Economic Affairs and Communications, 64.

V. CONCLUSIONS AND RECOMMENDATIONS

In the post-Soviet period, Russia continued the Soviet tradition of active measures in foreign and security policy, subverting the perceived adversaries, and extended these measures to the cyber domain. This, for Russia, was a cost-effective way of increasing its influence, especially in the so-called "near abroad" and coercing weaker powers into submission, exhausting their morale and the will to resist.

Russian defense and security doctrines consider cyberspace as part of the information space and view cyber operations as a unified concept, integral to its defense and security policy. These views are best expressed in the so-called Gerasimov doctrine, which has become a shorthand for Russia's active measures both in case of stand-alone cyber-attacks as well as when serving as accompanying part of larger, more complex military operations. The purpose of these operations is the reflexive control of perceived adversaries, winning their populations' "hearts and minds," and, in case of failure, pursuing the tactics of coercion and intimidation. Cyber disruption, spying, and the manipulation of the perceptions of the target audiences have been the major objectives of Russian information operations as evident in the cases with Georgia, Estonia, and Ukraine at different times in the last decade and half.

For cyber operations, Russia uses proxy groups, which can be deployed both in longer-term, continuous manner as well as for immediate cyber-disruption in a relatively short-term period during special and/or military ground operations. These are coupled with the means of psychological warfare in a form of "informational confrontation," which is normally the initial phase of the conflict aimed at degrading the adversary's capacity for resistance.

However, the historical record shows that Russia's active measures have certain limits. Frequently, they are isolated acts of cyber-disruption with no significant political consequences. Also, in cases when they are employed in conjunction with propagandistic measures, these acts of informational warfare are not necessarily fatal and may be

effectively countered by the opponent's consistent and coordinated efforts – both technologically and politically.

Russia's experience with the armed conflict with Georgia shows that in case of short-term military campaign of August 2008, Russia employed its cyber-warfare capabilities as a corollary to its extensive ground military operation. These cyber-measures aimed at hindering the Georgian Government's efforts to resist and retaliate the adversary's superior ground and naval forces. The major achievement of Russian cyber-operations during the war was psychological, having demonstrated Moscow's ability to disrupt Georgian Government's communication channels with its own population. However, for Russian armed forces, these cyber-measures did not bring about any qualitative advantage over Georgia.

The following two cases of Russian intrusion into Georgia's cyber-space were less effective, in terms of political objectives, as they represented isolated cases of hacking of computer networks of several agencies of the Georgian Government. And finally, in the case of the Lugar Lab, Russia attempted to use propaganda and disinformation to discredit the work of US-backed Central Public Health Reference Laboratory, but also, later in 2020, targeting the Lab's computer system so that to discredit its work in the eyes of the domestic and international public.

As Russia continues to pose critical threat to Georgia's defense and security infrastructure, it is of paramount importance to share and adopt the experiences of countries with similar infrastructural and political structures, including the power asymmetries with the opponents. Two such cases are Israel and Estonia. These small countries managed to create effective long-term cyber defense and cybersecurity systems, capable of fending off potential cyber-attacks from disproportionately superior powers.

The key elements of such effective systems that enable the smaller countries, specifically, Georgia, to counter the superior adversaries' information measures, both political and cyber-generated, include the following:

First, it is important to develop a long-term vision of cyber security and cyber defense strategy, using cyber capabilities to support both day-to-day security infrastructure

as well as military operations. Such documents help to develop coordination between various branches of authority, as well as between the center and the regions, when it comes to resisting a superior invading power. Secure communication infrastructure may become key in such cases. Coordination between the armed forces and police, as well as between the central government and local administrations, and strategic communication with own population may be key in ensuring avoidance of panic (causing various shortages in fuel and food as well as fleeing from the epicenter of the conflict toward the border areas) and other forms of civil disruption, which were widespread during the August 2008 war.

Second, a separate, yet integrated cybersecurity unit should be established and maintained in the highest civilian office of the country, the one directly responsible for the coordination of national cybersecurity strategy and operations. Normally, this is Presidential or Prime-Ministerial administration. In a hypothetical scenario, such an office would coordinate secure communication between various ministries and agencies, in case if normal communication channels have been disrupted. Such a generic system is being implemented in Georgia, known as Business Continuity Management system, under the auspices of the European Union and United Nations Development Programme. The system is implemented in various key state institutions and, yet, the system may require a separate and consolidated administrative unit, which would ensure its smooth nation-wide functioning in extraordinary circumstances.

Third, an appropriate national security strategy plan, as a single document, should be created and widely acknowledged as such a document helps to coordinate the work of all relevant bodies responsible for not only cyber but also conventional security activities throughout the nation. Such documents raise awareness about the potential dangers of information warfare both in technological as well as political terms. Also, such documents may help to endow Government's actions with more legitimacy in critical times, as political opposition in today's polarized world may deem the Government's actions arbitrary and self-serving. In the follow-up of the August 2008 war, after a brief hiatus, Georgian opposition staged large-scale demonstrations with demands to oust the Government, and the Government found itself in difficult situation as it had no legitimate

reference for explaining some of its security and diplomatic actions during and after the war to the population.

Fourth, strategic communications are of utmost importance for preparing the Government, armed forces, and general population for potential propagandistic attack, "soft power" offensive, coercion and intimidation by the adversary. Attacks against the morale of the population are usually the preparatory stage of a larger-scale military operations as well as active measures. Strategic communication blueprint is needed to counter hostile propaganda not only nationally (to prevent panic and further civilian disturbance) but also for waging international information warfare for garnering external political support. In the immediate follow-up of the August 2008 military campaign, Georgian diplomatic service found itself in difficult circumstances as it faced overwhelming worldwide disinformation coming from Russian official and unofficial sources, accusing Georgian Government of starting hostile actions and committing mass atrocities. There was little awareness or plan of what can be done in a systematic way to counter hostile propaganda in electronic mass media. This warrants development of a consistent blueprint for strategic communications action plan for averting such disruption in future.

Fifth, with the increased digitalization of Georgia, the cybersecurity threats will only gain in importance, elevating information warfare issues in the hierarchy of national security priorities. Therefore, addressing these pressing issues should be one of the major concerns of national security establishment of Georgia. As evidenced from the substantive chapters of this thesis, in 2008, Georgia was relatively spared of cyber disruption, due to the latter's underdevelopment. This is not the case anymore. With the nation-wide digitization, Georgia's governance and economy is becoming fast dependent on its digital infrastructure. Therefore, the management of its cybersecurity should be developing in anticipation of progress, not following it. Therefore, cybersecurity matters should be introduced in every sphere of public management and constitute one of the core areas of Georgia's civilian defense component of its "total defense" philosophy, which is currently under development.

Sixth, internationalization of efforts against foreign cyber-attacks is of paramount importance, as cyber-attacks and other active measures are, normally, accompanying larger and more serious political campaigns that target the country's resilience and military readiness. Therefore, domestic strategic communications should be complemented with international measures, through diplomatic and security channels with the leading strategic international partners, i.e., the United States, NATO countries, including, especially, the leading European nations, and Turkey. Georgia enjoys special strategic relations with NATO, framed in the Alliance's enhanced opportunities initiative. Since 2014, Georgia has had NATO's Substantive Cooperation Package, which was only recently updated and strengthened at the 1–2 December NATO Foreign Ministerial. The new additions to the Substantive Package include secure communications and cybersecurity elements. This indicates that the NATO-Georgia cooperation is rather well-established and coordinated in the information warfare domain. And this direction seems to be gaining more and more dynamic speed in mutual relationship. Given that Russia seems to more sensitive and apprehensive to international response to its actions, especially when it comes to sanctions, than to Georgia's (or, for that matter, Ukraine's) military capabilities, Georgia's effective coordination with international community may be a more potent (and certainly cost-effective) deterrent against Russia than the development of defense infrastructure and hardware. The point is that in some great and medium powers, especially in Europe, acuteness of Russian threat to European security is still disputed politically. Therefore, for effective international deterrent, Georgia needs more and more enhanced coordination at the international level to achieve meaningful political effectiveness for developing a persuasive political deterrent against the adversary.

Seventh, Georgia should invest more in Research and Development as cyber warfare and information domain cannot be meaningfully separated from the rest of infrastructure or body politic. Holistic development of these domains is key to successful defense of the nation. This offers yet another chance of cooperation with NATO. Since Georgian Government committed to the upgrade of its education and research capacities by increasing the general budget for education and science several-fold, the, Research and Development in cybersecurity can be listed as one of the priorities, especially given that

innovation is the common theme in Georgian Government's economic program for the next four years. Coupled with the popularity of state-sponsored start-ups, innovative research in cybersecurity field may be one of the leading directions in Georgia's defense infrastructure.

Eighth, given that cyber domain is often privately driven, Georgian Government should pay greater attention to the coordination between public institutions and private entities in ensuring that there is enough capacity for waging information campaigns both in technological as well as political terms. Technological resource can be found and integrated throughout the country, among the cutting-edge innovative private enterprises and start-ups that have been supported by Georgian Government in the last few years.

LIST OF REFERENCES

Adamsky, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Papers 54, Paris*:* Institut Français des Relations Internationales, November 2015. https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

Anjaparidze, Zaal. "Russia Dusts Off Conspiracy Theories about Georgia's Lugar Center Laboratory in Midst of COVID-19 Crisis." *Eurasia Daily Monitor 17*, no.62 (May 2020). https://jamestown.org/program/russia-dusts-off-conspiracy-theories-about-georgias-lugar-center-laboratory-in-midst-of-covid-19-crisis/.

Baezner, Marie, and Sean Cordey. *National Cybersecurity Strategies in Comparison - Challenges for Switzerland*. Zurich: Center for Security Studies, 2019. /en/center/CSS-news/2019/07/nationale-cybersicherheitsstrategien-im-vergleich--herausforderungen-fuer-die-schweiz-.html.

Ball, Deborah Yarsike. *Protecting Falsehoods with a Bodyguard of Lies: Putin's Use of Information Warfare*, No.136. Rome: Research Division-NATO Defense College, 2017), 2, https://www.ndc.nato.int/news/news.php?icode=1017.

Baram, Gil. "The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case." Military and Strategic Affairs 5, no. 1 (May 2013): 23–43. https://www.inss.org.il/wp-content/uploads/systemfiles/MASA5-1Eng4_Baram.pdf

Baram, Gil, and Kevjn Lim. "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks." *Foreign Policy*. June 2020. https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

Berzins, Janis. *Russia's New Generation Warfare in Ukraine*, №02. Riga: National Defense Academy of Latvia, 2014. https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf.

Bills, Christian. "The Internet Research Agency: Spreading Disinformation." *Small Wars Journal*, October 30, 2020. https://smallwarsjournal.com/jrnl/art/internet-research-agency-spreading-disinformation.

Blank, Stephen. “Cyber War and Information War à La Russe,” in *Understanding Cyber Conflict: 14 Analogies,* ed. George Perkovich and Ariel E. Levite. Washington, DC: Carnegie Endowment for International Peace, 2017. https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_FullText.pdf Carnegie Endowment for International Peace. Accessed October 17, 2020. https://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399.

Browne, Ryan. “US and UK Accuse Russia of Major Cyber Attack on Georgia,” *CNN*, February 20, 2020. https://www.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html.

Calamur, Krishnadev. “What Is the Internet Research Agency?” *Atlantic*, February 16, 2018. https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/.

Chen, Adrian. “What Mueller’s Indictment Reveals About Russia’s Internet Research Agency.” *New Yorker*, February 17, 2018. https://www.newyorker.com/news/news-desk/what-muellers-indictment-reveals-about-russias-internet-research-agency.

Cohen, Ariel, and Robert E. Hamilton. *The Russian Military and the Georgia War: Lessons and Implications*. Carlisle, PA: U.S. Army War College, 2011.

Connell, Michael, and Sarah Vogler. *Russia’s Approach to Cyber Warfare*, R0148. Arlington, VA: Center for Naval Analyses, 2016. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Cordey, Sean. *The Israeli Unit 8200: An OSINT-Based Study*. Zurich: Center for Security Studies, 2020. https://css.ethz.ch/en/services/digital-library/publications/publication.html/2beaf2b8-3d47-4be9-8553-18e7a8ce7c8e.

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. “Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security.” *International Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 24–34. https://doi.org/10.4018/ijcwt.2011010103.

Darczewska, Jolanta. *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*. no. 42. Warsaw: Centre for Eastern Studies, 2014. https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study.

———. *The Devil is in the Details: Information Warfare in the Light of Russia’s Military Doctrine.* no. 50. Warsaw: Centre for Eastern Studies, 2015. https://www.files.ethz.ch/isn/191967/pw_50_ang_the-devil-is-in_net.pdf.

Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations*. DIA-11-1704-161. Washington, DC: Defense Intelligence Agency, 2017. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf.

Deibert, Ronald J., Rafael Rohozinski, and Masashi Crete-Nishihata. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War." *Security Dialogue* 43, no. 1 (February 1, 2012): 3–24. https://doi.org/10.1177/0967010611431079.

Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Eizenkot, Gadi. "Cyberspace and the Israel Defense Forces." *Cyber, Intelligence, and Security 2*. no. 3 (December 2018): 99–104. https://www.inss.org.il/wp-content/uploads/2019/01/Eizenkot.pdf.

Flanagan, Stephen J., Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin. *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance.* RR-2779-OSD(Santa Monica, CA: RAND Corporation, 2016). https://www.rand.org/pubs/research_reports/RR2779.html.

Franke, Ulrik. *War by Non-Military Means: Understanding Russian Information Warfare*, FOI-R-4065-SE. Stockholm: Swedish Defense Research Agency, 2015. http://dataspace.princeton.edu/jspui/handle/88435/dsp019c67wq22q.

Frei, Jasper. *Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations*. Zurich: Center for Security Studies, 2020. https://doi.org/10.3929/ETHZ-B-000438397.

Galano, Juvien. "i-Voting - the Future of Elections," *e-estonia*, March 2019. https://e-estonia.com/i-voting-the-future-of-elections/.

Giles, Keir. *Assessing Russia's Reorganized and Rearmed Military*, Task Force on U.S. Policy Toward Russia, Ukraine, and Eurasia. Washington, DC: Carnegie Endowment for International Peace, 2017. https://carnegieendowment.org/files/5.4.2017_Keir_Giles_RussiaMilitary.pdf.

———. *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016. https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook%2C%20Russian%20Information%20Warfare.pdf.

———. *The Next Phase of Russian Information Warfare*. Riga: NATO StratCom COE, 2016. https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Gogitashvili, Givi. “Russia’s 2019 Cyber Attack against Georgia Followed by Full-Spectrum Propaganda Effort,” *Medium*, April 23, 2020. https://medium.com/dfrlab/russias-2019-cyber-attack-against-georgia-followed-by-full-spectrum-propaganda-effort-4460673cb3e9.

Gotsiridze, Andro. *Russia’s Cyber Activities—A Growing Threat for Georgia*. #95. Tbilisi, Georgia: GFSIS, 2018. https://www.gfsis.org/files/library/opinion-papers/95-expert-opinion-eng.pdf.

Government of Georgia. *National Cybersecurity Strategy of Georgia 2017–2018*. Tbilisi, Georgia: Government of Georgia, 2017. http://gov.ge/files/469_59439_212523_14.pdf.

Gross, Judah Ari. “Army Beefs up Cyber-Defense Unit as It Gives up Idea of Unified Cyber Command.” http://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/.

Heickerö, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, FOI-R-2970-SE. Stockholm: Swedish Defense Research Agency, 2010. http://www.highseclabs.com/data/foir2970.pdf.

Heller, Nathan. “Estonia, the Digital Republic.” *New Yorker*, December 18, 2017. https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

Housen-Couriel, Deborah. *National Cyber Security Organization in Israel*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2017. https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf.

Huhtinen, Aki-Mauri, Noora Kotilanen, Saara Särmä, and Mikko Streng. “Information Influence in Hybrid Environment: Reflexive Control as an Analytical Tool for Understanding Warfare in Social Media.” *International Journal of Cyber Warfare and Terrorism 9*, no3. (July-September)2019: 1–20. https://doi.org/10.4018/IJCWT.2019070101

Information Security Authority of Estonia. *Cyber Security in Estonia 2020*. Tallinn: Information System Authority of Estonia, 2020. https://www.ria.ee/sites/default/files/cyber_aastaraamat_eng_web_2020.pdf.

Isachekov, Vladimir. “Russia Claims U.S. Running Secret Bio Weapons Lab in Georgia,” *AP*, October 4, 2018. https://apnews.com/article/0cf158200e674f41bd3026133e5e043d.

Jasper, Scott, and Keith Alexander. *Russian Cyber Operations: Coding the Boundaries of Conflict.* Washington: Georgetown University Press, 2020.

Jensen, Benjamin. "The Cyber Character of Political Warfare." *Brown Journal of World Affairs* 24, no.1 (October 2017): 159–171. https://drive.google.com/file/d/1quiULILaIvSSQsOzQed0D1lgu1i38mQs/view.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." *Journal of Strategic Studies* 42, no. 2 (February 23, 2019): 212–234. https://doi.org/10.1080/01402390.2018.1559152.

Jones, Stephen F., *Georgia: A Political History since Independence.* New York, NY: I.B. Tauris, 2012.

Jones, Stephen F., and Neil S. MacFarlane. *Georgia: From Autocracy to Democracy*. Toronto: University of Toronto Press, 2020.

Kirk, Jeremy. "Georgian Cyber Counterattack Exposes Russian Hacker Seeking NATO Document," *Atlantic Council*, November 4, 2012. https://www.atlanticcouncil.org/blogs/natosource/georgian-cyber-counterattack-exposes-russian-hacker-seeking-nato-document/.

Maness, Ryan, and Brandon Valeriano. "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society* 42, no.2 (March 2015): 301–323. https://journals-sagepub-com.libproxy.nps.edu/doi/pdf/10.1177/0095327X15572997?casa_token=oPwlt0xH3m4AAAAA:BiSfCl3MTmXBPU7PzQ1XQIJma6W9Of-Dss_5bvHwGAYIAZXHhw-HS7_CUoKIQ3nie9pDhqcp9q5b.

Markoff, John. "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.

McCauley, Kevin N., *Russian Influence Campaigns Against the West: From the Cold War to Putin*. North Charleston, SC: CreateSpace Independent Publishing Platform, 2016.

Ministry of Defense of Georgia. *Strategic Defense Review 2017–2020.* Tbilisi, Georgia: Ministry of Defense, 2017. https://mod.gov.ge/en/page/73/strategic-defence-review.

Ministry of Defense of the Russian Federation. *Russian Federation Armed Forces' Information Space Activities Concept* Moscow: Ministry of Defense of the Russian Federation, 2011. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Ministry of Economic Affairs and Communications of Estonia. *Cybersecurity Strategy of Republic of Estonia 2019–2022*. Tallinn: Ministry of Economic Affairs and Communications, 2019. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

Ministry of Defense of Estonia. *National Defense Strategy of Estonia*. Tallinn: Ministry of Defense of Estonia, 2011. https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

Ministry of Internal Affairs of Georgia. "Statement of The Ministry of Internal Affairs of Georgia." September 3, 2020. https://police.ge/en/saqartvelos-shinagan-saqmeta-saministros-gantskhadeba/13926

Ministry for Social Equality of Israel. *The Digital Israel National Initiative: The National Digital Program of the Government of Israel*. Tel-Aviv: Ministry for Social Equality, 2017. https://www.gov.il/BlobFolder/news/digital_israel_national_plan/en/The%20National%20Digital%20Program%20of%20the%20Government%20of%20Israel.pdf.

National Cyber Directorate. *Israeli National Cyber Security Strategy in Brief.* Tel-Aviv: National Cyber Directorate, 2017. http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

NATO. "Bilateral Meeting with the Minister of Defense of Georgia." October 25, 2019. http://www.nato.int/cps/en/natohq/photos_169927.htm.

Pernik, Piret. *Preparing for Cyber Conflict: Case Studies of Cyber Command.* Tallinn: International Centre For Defense and Security, 2018. https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf.

Perry, Bret. "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations," *Small Wars Journal,* August 14, 2015. https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera.

Pomerantsev, Peter, and Michael Weiss. *How the Kremlin Weaponizes Information, Culture and Money.* New York, NY: The Institute of Modern Russia, 2014. https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

Posard, Marek N., James V. Marrone, and Todd C. Helmus. "How You can Fight Russia's Plans to Troll Americans During Campaign 2020." *The Rand Blog,* July 14, 2020. https://www.rand.org/blog/2020/07/how-you-can-fight-russias-plans-to-troll-americans.html.

Rid, Thomas. *Cyber War Will Not Take Place.* Oxford: Oxford University Press, 2013.

Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, RR-1772-A. Santa Monica, CA: RAND, 2018. https://www.rand.org/pubs/research_reports/RR1772.html.

Rondeli, Alexander. *Georgia—Russia: From Negative to Positive Uncertainty*. #3. Tbilisi: GFSIS, 2013. https://www.gfsis.org/files/library/opinion-papers/3-expert-opinion-eng.pdf.

Schoen, Fletcher, and Christopher J. Lamb. "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference." Strategic Perspectives, no. 11. Washington, DC: National Defense University Press, Institute for National Strategic Studies, 2012. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.

Shlapak, David A., and Michael W. Johnson. *Reinforcing Deterrence NATO's Eastern Flank.* RR-1253-A(Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1253.html

Shultz, Richard H., and Roy Godson. *Dezinformatsia: Active Measures in Soviet Strategy*. Washington, DC: Pergamon-Brassey's International Publishers, 1984.

Sputnik International. "Russia Concerned Over U.S. Biological Activities in Georgia - Deputy Minister." December 19, 2018, https://sputniknews.com/world/201812191070814362-russia-us-lab/

State Security Service of Georgia. *The Report of the State Security Service of Georgia.* Tbilisi: State Security Service of Georgia, 2019. https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/SSSG%20Report%202018.pdf.

Swed, Ori, and john Sibley Butler. "Military Capital in the Israeli Hi-Tech Industry." *Armed Forces & Society 41*, no. 1(August 2013): 123–141. DOI: 10.1177/0095327X13499562.

Tabansky, Lior. "Israel Defense Forces and National Cyber Defense." *Connections: The Quarterly Journal* 19, no. 1 (2020): 45–62. https://doi.org/10.11610/Connections.19.1.05.

Tabansky, Lior, and Isaac Ben Israel. *Cybersecurity in Israel*, (Cham: Springer International Publishing, 2015). https://doi.org/10.1007/978-3-319-18986-4.

Talmazan, Yuliya. “Data security meets diplomacy: Why Estonia is storing its data in Luxembourg.” *NBC News*, June 25, 2019, https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171.

TASS. “US Labs in Third Countries May Be Developing Pathogenic Agents - Diplomat.” April 17, 2020. https://tass.com/politics/1146327.

Thomas, Timothy. *Russian Military Thought: Concepts and Elements*. MP190451V1. Bedford, MA: The MITRE Corporation, 2019. https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf.

———. “Russia’s Reflexive Control Theory and the Military.” *The Journal of Slavic Military Studies* 17, no. 2 (June 2004): 237–56. https://doi.org/10.1080/13518040490450529.

———. “Russia’s 21st Century Information War: Working to undermine and destabilize populations,” *Defense Strategic Communications*, no.1 (January 2015). https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations.

Thornton, Rod. “The Changing Nature of Modern Warfare.” *The RUSI Journal* 160, no. 4 (July 4, 2015): 40–48. https://doi.org/10.1080/03071847.2015.1079047.

Tsereteli, George. “Russian Cyberattack on Georgia Shows Why the U.S. Should Pass the Georgia Support Act.” *Atlantic Council*, June 9, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-cyberattack-on-georgia-shows-why-the-us-should-pass-the-georgia-support-act/.

UK Government. “UK Condemns Russia’s GRU over Georgia Cyber-Attacks.” February 20, 2020. https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. *Cyber Coercion: The Evolving Character of Cyber Power and Strategy*. New York, NY: Oxford University Press, 2018.

Warrick, Joby and Ellen Nakashima. “Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility.” *Washington Post*, May 18, 2020. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

White, Sarah P., *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*. West Point, NY: Modern War Institute, 2018. https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California