REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
04/30/2020

2. REPORT TYPE
Technical Report

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Lithuania Reacts: Confronting Russian Manipulation Techniques

5a. CONTRACT NUMBER
W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Timothy Thomas

5d. PROJECT NUMBER
0719S120J3

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-19-3194

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Army (ACC-APG)

10. SPONSOR/MONITOR'S ACRONYM(S)
ACC-APG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This report will examine the information and cyber-attacks that Lithuania has experienced and what lessons its analysts have learned and applied. The first part of the analysis focuses mainly on the propaganda of influence, while the second part focuses more on cyber issues (at times, in both periods, information and cyber issues are mixed). The time period under examination is 2017-2019 and where specific templates are addressed, they are boldened.

15. SUBJECT TERMS
Information Warfare; Computer Security; Russia; cybersecurity; trolls; Lithuania; propaganda; manipulation

16. SECURITY CLASSIFICATION OF:
a. REPORT
b. ABSTRACT
c. THIS PAGE

17. LIMITATION OF ABSTRACT

18. NUMBER OF PAGES
14

19a. NAME OF RESPONSIBLE PERSON
Susan Carpenito

19b. TELEPHONE NUMBER *(Include area code)*
781-271-7646

Sponsor: USEUCOM ECJ39
Dept. No.: P663
Contract No.: W56KGU-18-D-0004-S120
Project No.: 0719S120-J3

The views expressed in this document are those of the author and do not reflect the official policy or position of MITRE, the Department of Defense, or the US government.

Approved for Public Release, Distribution Unlimited. Public Release Case Number 19-3194.

McLean, VA

Lithuania Reacts: Confronting Russian Manipulation Techniques

Timothy Thomas

April 2020

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

1 Introduction

For several years now Lithuania's government has complained about numerous information and cyber-attacks aimed at not only the government but also its population. In the majority of the cases under investigation, Russian propaganda vessels (*Russia Today* or *RT*, *Sputnik*, etc.), trolls, or secret operatives have been singled out as being responsible for the incursions or attempts at manipulation.

As a result of Lithuania's constant attention to this topic, the nation has developed several templates that are of interest to the U.S. and other nations. These templates describe Russian propaganda targets, dissemination techniques, and information themes, among other issues. The nation has developed a new National Cyber Security Strategy as well and is regarded as the fifth best country in the world regarding cybersecurity issues according to the national cyber security index.[1]

This report will examine the information and cyber-attacks that Lithuania has experienced and what lessons its analysts have learned and applied. The first part of the analysis focuses mainly on the propaganda of influence, while the second part focuses more on cyber issues (at times, in both periods, information and cyber issues are mixed). The time period under examination is 2017-2019 and where specific templates are addressed, they are boldened.

2 Information

2017

Russian V. N. Remarchuk, writing in the *Journal of the Academy of Military Science* in 2017, noted that "if society and the people are affected, then all the state power institutions, even with every technological perfection, will be doomed."[2] Soft power's importance thus lies in its ability to influence the behavior of the masses.[3]

It thus comes as no surprise that the main information activity of Russia is to try to influence Lithuanian society's will to resist. This is done, for example, by continuously pointing out fake NATO shortcomings and representations, such as that it will not come to rescue or defend Lithuania if Russia attacks it. The **ten targets of the propaganda** designed to reduce society's will were stated to be:

1. Lithuanian history
2. Foreign policy
3. Domestic policy
4. Lithuanian military
5. Defense capabilities
6. Ethnic communities (abused Russians and Poles)
7. NATO and the EU

[1] See, for example, https://ncsi.ega.ee/ncsi-index.
[2] V. N. Remarchuk, "The Destruction of the Modern State System by Means of 'Social Technologies,'" *Journal of the Academy of Military Science*, No. 2 2017, p. 48.
[3] Ibid., p. 47.

8. Ties between Lithuania and Poland
9. Culture
10. The energy sector [4]

The Center for East European Studies further developed the goal of Kremlin propaganda, stated to be the creation of an image of a temporary Baltic state that will eventually side with Russia. This will help Russia create neutral space between Europe and itself. The **five layers of this propaganda image** are: creating an image of a failing state; creating the myth that the nation is a neo-fascist state; creating mistrust in Western allies and stressing the need to agree with Russia; stimulating the fragmentation of Lithuanian society; and setting society against European ideas. The idea is to fuel nostalgia for the Soviet regime and to demonstrate that Lithuania had fueled tension in the region with artificial threats about Russia.[5]

The same source noted that **Russia's propaganda dissemination network** includes the Internet and public space; political and public organizations, informal movements, and defenders of minority rights; and history, historical heritage groups, and occurrences directed toward higher education and culture. Facebook pages, media outlets in either the Lithuanian or Russian languages, human rights defenses, public political organizations and information movements, historical heritage groups, and intellectual forums or other forms of activities are also part of the dissemination process. Television controlled by the Kremlin is the main dissemination channel along with *RT* and *Sputnik*.[6]

Propaganda has a further goal of regime change and the ability to falsify history. A Lithuanian Army representative noted that there is a **Russian information campaign** designed to do just that. The main narrative supporting regime change is that NATO is weak and detrimental to Lithuania. Russian citizens back home, on the other hand, are told NATO is strong and growing rapidly and is almost equal to the threat of fascism. Thus, Russia's propaganda is designed to fit the targeted population. Propagandists also note that everything is getting worse in Lithuania and that families are departing the country. The main narratives used to falsify or influence history are attempts to discredit Lithuanian partisans from World War II who fought against Russia by trying to convince people that they were shooting and killing their own people.

The Russian *RT* budget appears well-funded to conduct reconnaissance. According to one report, in 2016 its budget was 600 million Euros, while the entire Lithuanian defense budget was 650 million Euros. There appears to be an information reconnaissance campaign underway against Lithuanian networks, which is designed to test how long it takes to access and hack into channels and post false news. Such posting of fake news must be countered immediately, as one cannot afford to be reactive[7] when Russia is so proactive. Another 2017 article also noted that Russia likes to darken the image of people who are dead and cannot defend themselves. This is particularly true in regard to anniversaries designed to honor people who stood up to the Soviet Union, such as

[4] Ruta Latvenaite, "Information War with Russia Not to End for the Next Ten Years," *Lietuvos Zinios*, 24 April 2017.

[5] Center for Eastern European Studies Monograph, "Russian Propaganda: Analysis, Assessment, Recommendations," *EESC,* 18 July 2017, pp. 57-64.

[6] Ibid., pp. 72-76.

[7] Jurate Zuolyte, "Lithuanian Army Representative: In Information War, a Battle Over Hearts, Minds is Waged," *Delfi*, 17 October 2017.

World War II partisans (who are a continuous Russian target). Discrediting individuals is even more effective when done by people who would speak on behalf of Russians.[8]

Another source, in line with attempts to change the regime, noted that Russia tries to lower trust in the nation's institutions and in NATO and to create antagonism against liberal values. To counter such propaganda, Lithuania's Education and Science Ministry is trying to educate children about the threat of propaganda and the Culture Ministry has ordered a study of residents' ability to critically assess the media.[9]

2018

Lithuanian Foreign Minister Linas Linkevicius noted in 2018 that Russia often uses European platforms for its operations against Europe. *Russia Today* is registered in London, *RTR Planeta* in Stockholm, and *Yandex* in Amsterdam. Programmers, however, are in Moscow. Linkevicius states that, at times, some Lithuanian politicians are thinking that all is good with Russia. These people are naïve, he noted, and the hope is that they are not subject to the Stockholm syndrome, where a lack of experience or something else is causing them to make an incorrect analysis. Naturally not everything Russian should be rejected as there are very different people in different places there. But official propagandists will continue to try to divide Lithuania's population.[10]

In June 2018 a conference titled "Fake News Impact on Media Institutions: Poland's Experience and other Countries' Practices" was held in Kraków, Poland. Lithuanian LRT Director General Monika Garbaciauskaite-Budriene attended the session and made several important statements. She noted that the most important items on which to focus are 1) media literacy 2) the ability to distinguish reliable sources from unreliable ones, and 3) a need for better ethics, not legal regulation or better algorithms. She went on to discuss how truth is both a basic European tradition and value and they must be honored. Subjective opinions can skew the truth. Information can only be true or false, not subjective. Journalists too often feel pressure regarding promptness and let this feeling rule instead of taking the time to check information thoroughly. The authenticity of images must be also be checked and verified. Finally, she stated that journalists must continue to be trained in their profession as new digital devices appear often these days.[11]

Her commentary is important because Lithuania confronts fake report after fake report. For example, a fake hacker report out of St. Petersburg, Russia claimed that Lithuanian Defense Minister Raimundas Karobils had harassed a journalist and admitted to being gay. The fake story stated that eight current or former diplomats also had spoken up about harassment. Lithuanian intelligence agencies had warned a year ago that Russia would be trying to discredit not only such official personas but also NATO forces through information and cyber-attacks. The aim is to spread provocative information.[12]

Based on a different type of reporting, on 14 February 2018 the Lithuanian Radio and Television commission took the Russian-language channel *RTR Planeta* off the air for a year for inciting war and hatred in their programming. However, in a dissenting opinion, a European Broadcasting

[8] Pumprickaite interview with Aukse Usiene, "Army Analyst: Ruta Vanagaite is Standing on the Frontlines of Information War," *LRT.lt*, 29 October 2017.

[9] Monika Kasnikovskyte, "Representatives of Academia Revealed Who Is Hurt Most by Russian Propaganda in Lithuania," *Balsas.lt*, 22 November 2017.

[10] Rita Miliute interview with Linas Linkevicius, "It is Dangerous When tolerance Turns into Naivety," *LRT.lt*, 1 August 2018.

[11] Eliminate Jursenaite interview with Moniak Garbaciauskaite-Budriene, "Journalists Must Seek Truth. This is the Best Antidote Against Fake News," *LRT.lt*, 23 June 2018.

[12] No author provided, "Fake News on Lithuanian Defense Minister Planted on News Portal," *BNS* (in English) 19 January 2018.

Union representative stated that responding to Russian information with creative alternatives such as providing more profound information of higher quality would be more efficient than taking TV channels off the air.[13]

Thus fake reporting, references to war and hatred, and means to create tension and confusion in society are all being used by Russia's propaganda outlets. Darius Jauniskis, Head of the State Security Department (VSD) of Lithuania, noted that Russia prepares information operations in peacetime in order to get the future battlefield prepared for action. Russia demonizes Lithuania as part of NATO and belittles it as a state. Such information actions are conducted constantly.[14] Propagandistic portals such as *Sputnik* and *Baltnews* employ the use of topics such as the presence and deployment of weapons as part of their information warfare strategy, which is reminiscent of the use of Soviet-era reflexive control measures (getting someone to do something for themselves that they are actually doing for you), according to a lecturer at Vilnius University.[15] Another report stated that *Baltnews* was engaged in "destructive activities in all three Baltic States; also, [it] cooperates with other companies, organizations, and persons…"[16]

Russia continues to ignore reality and historical truth. In 2018 the Baltic nations requested compensation for the Soviet occupation of their country during the last century. The Russian response was to state that Russia may decide to take Vilnius and Klaipeda back as part of its compensation. To Lithuanian analysts, this is another historical manipulation that Russia uses as it continues, in its own way, to ignore its occupation of the Baltic countries. When a demand is made for compensation for its occupation, Russia demands territory as its compensation.[17]

Based on this background, Lithuania's national security strategy has listed several **information themes** that Russia invokes. They are: attempts to skew historical memory; the spread of unfounded and misleading information about the democratic regime and the country's defense; attempts to pit ethnic and cultural groups one against another; attempts to weaken the national identity; information intended to discredit the country's membership in NATO; and information that weakens the citizens' resolve to defend Lithuania. It is necessary for Lithuanians to improve one's "information radar" as to what is real and fake; improve one's understanding of what is a fact, what is an interpretation, and what is simply a lie; and improve the ability to select information sources and their reliability. Critical thinking must be improved, investment in education must grow, and a reliance on more than one source is needed. News spread by social networks needs to be viewed in a critical way. Discord may be sewn in electoral processes, in relation to increased defense spending and the nation's socio-economic situation. A citizen's socio-economic situation can make them more vulnerable to propaganda. [18]

Finally, Lithuania has learned military lessons from the ongoing war in Ukraine. In an interview with a Ukrainian hybrid warfare expert, it was noted that Russia had used propaganda to attack army commanders by calling them unpatriotic, corrupt, and talentless. Soldiers received such messages directly to their cell phones in the field and were encouraged to rebel. The August 2014 battle of Ilovaysk was critical, as Russia's initial assault had caused some panic in Ukrainian

[13] No author provided, "European Broadcasting Union Representative Doubts Efficiency of Lithuania's Sanctions on Russian TV Channels," *BNS* (in English) 14 February 2018.

[14] Audrius Matonis interview with Darius Jauniskis, "VSK Head: Russia Tends to Cross Lines," *LRT.lt*, 3 April 2018.

[15] No author or title provided, *BBC Monitoring* (in English), 13 February 2018.

[16] No author provided, "Conservative MP Addresses Authorities Over Kremlin Propaganda Channels Operating in Lithuania," *ELTA* (in English), 31 August 2018.

[17] Zygintas Abromaitis, "Russian Propaganda Returns to Territorial Disputes with Lithuania," *LRT.lt*, 13 September 2018.

[18] No author provided, "Are We Resilient Enough Against Information Threats," *15min.lt*, 31 October 2018.

society, with mothers, wives, and sisters calling soldiers and persuading them to save themselves and come home (the force had been surrounded by Russian forces and Ukrainian President Petro Poroshenko had called President Putin and requested a cease fire in order to get his forces home). It wasn't until army commanders could explain why things were done in certain ways that feelings began to change.[19]

2019

For some time, Lithuanian intelligence agencies have been stating that Russia's aggressive policy was the main threat to the nation's national security. The presence of Allied troops in the region in 2018 helped reduce the likelihood of Russia's use of military force against the region. To increase its ability to manipulate Lithuanian society, Russia increased its investment in what might be termed Lithuanian language propaganda, further indicating that it is reviewing strategies and the quality of its work to achieve its goals.[20]

In January 2019 Facebook announced that it had removed hundreds of pages and accounts in Lithuania that were linked to the Russian Sputnik channel or its employees. While the pages presented themselves as independent, they were spreading posts about anti-NATO sentiment. Some were in Lithuanian and some targeted divisive political issues.[21]

In a similar manner, Russian TV continued their propaganda assault of hatred with more fake news about Lithuanian partisans who were awarded the Freedom Prize in January 2019. Channel Russia 24 deemed the partisans to be criminals and offered fake statistics to create tension and distrust in Lithuania as part of Russia's information war,[22] which attempts to use propaganda to divide Lithuanians, undermine mutual trust, and influence democratic and decision-making processes. Lithuania's Deputy Minister of Foreign Affairs noted that disinformation presents a serious challenge for Western unity and security.[23] Character assassination, threatening letters to the Lithuanian embassy in Moscow, and defamation, fake news, intimidation, and various forms of pressure are the usual instruments that the Russian government uses to achieve its goals.[24] Any issue that calls out Russian wrongdoing is severely chastised. For example, on 13 January Lithuania ruled against Russia and indicted its military for injuring and killing Lithuanians involved in that nation's 1991 demonstration for independence. Naturally, Russia strongly condemned the ruling without providing any proof that it's military had not conducted such actions.[25]

It was also noted that in addition to the traditional tools of fake news, cyber-attacks, hacking, and disinformation campaigns, Russia also uses shadow money, corrupt influence, and other past tools to create useful political movements or to propose candidates that support Kremlin policies.

[19] Aidanas Praleika, interview with Lyubov Tsybulskaya, "Ukrainian Expert: Moscow's Propaganda Hits Where It is Most Painful," *Lietuvos Zinios*, 20 November 2018.

[20] Milena Andrukaityte, "NSGK Chairman: Russia is Increasing Investments in Propaganda in the Lithuanian Language," *15min.lt*, 30 January 2019.

[21] No author provided, "Facebook Removes Hundreds of Accounts Linked to Sputnik Employees," *Baltic News Service* (in English), 17 January 2019.

[22] No author or title provided, *ELTA* (in English), 15 January 2019.

[23] No author or title provided, *ELTA* (in English), 11 April 2019.

[24] No author or title provided, *Lietuvos Zinios*, 15 April 2019.

[25] No author or title provided, *ELTA* (in English), 23 April 2019

Russia’s long-term, traditional way of influence is a complex mixture of issues across the entire spectrum of activities, making it hard to recognize in its entirety.[26]

In summation, the three-year period under examination has found that some Russian information incursions have met with success while most have been singled out as outright slander or disinformation. Perhaps more importantly Lithuania has uncovered the most important Russian propaganda themes and dissemination techniques, as outlined above, for which they must be prepared to defend themselves.

3 Cyber

2017-2019

In late 2017 the Lithuanian Defense Ministry stated that Kaspersky Lab software products posed a potential threat to Lithuania’s national security, especially since several critical infrastructures (not named) were using it. Government agencies were told to stop using the product while businesses will have to assess the risk of using Kaspersky products on an individual basis.[27] Another report stated that five percent of public bodies and agencies were using the software, according to the National Cyber Security Center (NCSC). Kaspersky Lab, the report noted, stated that it does not have inappropriate ties with any government.[28] The Lithuanian government noted that it had collected information carefully and did not jump to conclusions. Rather, specific evidence was collected about the software. Defense Deputy Edvinas Kerza noted that “at least two criminal groups linked with Russia’s special services” were distributing malware.[29]

In addition to Kaspersky products, the NCSC recommended against using the Yandex Taxi ride-sharing app. The app is registered in Amsterdam, but its information technology specialists are in Moscow. The device collects and stores personal data and requests permission to activate a device’s camera or microphone or manage its wireless network access.[30]

Simultaneously, hacking incidents are increasing against Lithuania. Some have been coordinated with information attacks. Subjects of the attacks have included figures such as Lithuania’s National Defense Minister Raimundas Karoblis and Lithuanian troops participating in NATO exercises; and some have included energy or other specific agencies. Russia has been identified as a major culprit behind the attacks, and in many cases criminal groups or trolls were singled out as responsible for the incursions. Lithuania’s Deputy Defense Minister Edvinas Kerza noted in one interview that 27 percent of incidents were directed at the energy sector, 22 percent toward the public sector, and 21 percent toward the foreign affairs and security policy sectors. The result is a hybrid threat.[31]

[26] Viktorija Rimaite, “Lithuania Will Not Manage to Escape Kremlin Tentacles: Old Weapons Pose Danger as Well,” *Irytas.lt*, 9 May 2019.

[27] No author provided, “Russian Kaspersky Lab Software Poses Threat to Lithuania’s Security—Government,” *BNS* (in English), 21 December 2017.

[28] No author provided, “Lithuanian Critical System Managers Scrap Kaspersky Lab Software,” *BNS* (in English), 27 January 2018.

[29] No author provided, “Lithuania’s Government Ready for Litigation with Kaspersky Lab—Deputy Defense Minister,” *BNS* (in English), 1 March 2018.

[30] No author provided, “Lithuania’s Cyber Security Center Recommends Against Using Yandex.Taxi App,” *BNS* (in English), 30 July 2018.

[31] Audrius Matonis interview with Edvinas Kerza and Rytis Rainis, “Criminal Groups Have Been Identified That Are Financed by Russian Authorities,” *LRT.lt*, 13 August 2018.

Lithuania has a host of "virtual elves" that try to act as a counterbalance against the efforts of pro-Kremlin trolls to control virtual information space. The elves' aim is to unmask Russian disinformation and fight those who spread it. In response, a Russian search system listed Lithuanian activists who are contesting Russian propaganda. The Russian goal was to organize attacks against the elves and create obstacles that prevent virtual space from supporting Lithuania.[32]

In response to Russia's expanded use of cyber activities, on 13 August 2018 Lithuania approved a new **national cyber security strategy**, which has replaced the existing Electronic Information Safety Development Program for 2011-2019. This was due to new cyber security challenges, especially cyber-attacks against public and energy sectors, airports, media outlets, and infrastructure for national security. Five goals were identified: bolstering cyber resistance and defense capabilities; fighting online crime; promoting innovations and a cyber security culture; promoting private-public cooperation; and strengthening international cooperation.[33]

The threat of cyber-attacks from Russia involves specific criminal groups funded by Russian authorities. They can create viruses undetectable by commercial measures with a goal of taking control of computer networks and systems.[34] Cyber-attacks appear most often on Lithuanian national holidays, when Russia is being accused of some wrongdoing, or when Russian citizens are banned from entering Lithuania. Russia then observes how Lithuania responds to such provocations and it tests Lithuania's level of cybersecurity at the same time. Media outlets are used to spread disinformation (lies about the situation) and panic (lies about shutting down infrastructure) through intrusions.[35]

Defense Minister Karoblis, in another interview, discussed the danger of two Russian programs designated as 1C and ABBYY. A cyber-attack in Ukraine used 1C, an accounting program that was then banned in Ukraine immediately but not in Lithuania. However, the system is being used in Vilnius in a proportional manner until a new program can be constructed. Interim measures are in place until fully secured software is installed. This helps Lithuania continue to pay, for example, the police in the meantime.[36]

The public is not the only target of Russian cyber-attacks. NATO troops in Estonia, Latvia, Lithuania, and Poland have been told that cyber-attacks are being aimed at their cellphones. As a result, soldiers are surrendering their cellphone service cards and communicating only via safe channels.[37] One 2017 report referenced a Wall Street Journal article that "cited troops, officials, and government representatives of NATO member-states" as stating that Russia had planned to hack mobile phones in order to obtain information about capacities and the ability to intimidate troops. The campaign was targeting 4,000 NATO troops in Poland and the Baltics.[38] Fake news stories have apparently been trying to use soldiers to cause problems in Lithuanian-Polish relations. In one such fake report, a Lithuanian soldier had reportedly said some Polish soldiers

[32] Rasa Pakalkiene, "Lithuanian Elves Have Gotten on the Kremlin's Last Nerve: Their Lists Have Been Published," *Lietuvos Zinios*, 8 January 2018.

[33] No author provided," Lithuanian Government Approves New Cyber Security Strategy," *BNS* (in English), 13 August 2018.

[34] No author provided, "Russia Poses Biggest Cyber Threat for Lithuania, Vice Minister Says (Media)," *BNS* (in English), 14 August 2018,

[35] Egle Kristopaityte, "Expert about Attack Against Karoblis: There Will Be More Such Campaigns Before Presidential Election," *15min.lt*, 19 January 2018.

[36] Indre Makaraityte interview with Raimundas Karoblis and Marius Laurinavicius, "We Have Not Realized Yet That We Are at War with Russia," *LRT.lt*, 26 September 2018.

[37] Julija Petrosiute and Vykintas Pugaciauskas, "NATO Troops in Baltic States Will Have to Get Used to Life Without Unsafe Internet, Mobile Applications," *LRT.lt*, 6 January 2018.

[38] Vaidotas Beniusis, "NATO Troops Warned About Phone Hacking Threat Upon Arrival in Lithuania," *BNS* (in English), 6 October 2017.

look like pigs due to their poor physical preparedness. Of interest is that the author of the fake story is apparently also a made-up character. The domain name that was spreading these stories was registered in Poland, but it is not known who controls it.[39] In a 2019 story about military exercises, it was reported that news portals were hacked. As a result, fake news was inserted into the portal, to include reporting about water shortages near Kaunas and the testing of weapons of mass destruction. Kremlin trolls were cited as the source of the news, aimed to cause panic among the population.[40]

The outlook for the future is not completely negative, in fact the Russian activity is driving positive change. Deputy Defense Minister Kerza said there is more than one plan under consideration for what the state would do if a mass cyber-attack occurred. Lithuania has invested in underground infrastructure and the network connections are known and who would ensure the systems function. Opponents will not know who our technicians are or where our cables are located. They are not announced. Lithuania is preparing not only for cyber defense but also for cyber-attacks. As Kerza warned "We do not aim to claim that we would be trying only to defend ourselves,"[41] a clear statement of the preparation of offensive operations if required.

Further, the July 2019 issue of Defense News had an article on Lithuania's cybersecurity posture, which is already, according to the 2018 Global Cybersecurity Index, the fourth best prepared country in cyberspace, behind only the UK, U.S., and France. The article noted that the Ministry of National Defense now has sole responsibility for setting cyber policy; that a Cyber Security Center was established in Kaunas in 2018; and that Lithuania participated at the international level by leading the European Union's permanent structured cooperation (PESCO) project on rapid response teams for cyber issues.[42]

Finally, political commentator Marius Laurinavicius noted that Lithuania's problem is that it does not realize yet that it is at war with Russia. The current government "is not creating an anti-hybrid strategy" and it does not prioritize issues as it should. For example, the chairman of the ruling party, LVZS leader Ramunas Karbauskis, has a business with a person funding a Russian troll factory and no one seems to worry about this.[43] Another report stated that Lithuania's NCSC warned in June 2019 about a risk posed by some Wi-Fi equipment as it uses Russian technology.[44]

4 Conclusions

One insightful commentary noted that Russian foreign policy creates political wedges by creating problems, violating international law, and creating geopolitical tensions.[45] Russian propaganda creates similar information wedges. Lithuania's continued information and cyber diligence directed at Russia's propaganda assault helps everyone better picture what these wedges are and their shape as well as where the Kremlin is directing its efforts.

[39] Andrius Vaitkevicius, "Liars from Poland Who Slandered Lithuanian Soldier Hiding under Picture of Doctor from Druskininkai," *Irytas.lt,* 12 November 2018.

[40] No author provided, "Kremlin Trolls Try to Spread Panic," *Kauno Diena Online*, 21 June 2019.

[41] Vaidas Saldziunas, "What Would Be Happening in Lithuania, If Internet Was Disconnected during a Cyber Attack: There are a Few Plans," *Delfi*, 25 November 2018.

[42] Jen Judson, "A Necessary Rise," *Defense News*, 8 July 2019, p. 9.

[43] Makaraityte interview with Raimundas Karoblis and Marius Laurinavicius.

[44] No author provided, "Lithuania's Cyber Security Center Warns About WiFi Equipment Risk," *BNS* (in English), 11 June 2018.

[45] Unidentified correspondent interview with Egidijus Motieka, "Kremlin Created System of Geopolitical Wedges in Europe; May Manipulate New Lithuanian President," *LRT.lt,* 30 March 2019.

The discussion above listed Russian propaganda targets, dissemination techniques, and information threats/themes that compose Russia's information campaign to influence Lithuania's population. Lithuania has a historical grudge with Russia,[46] which makes its focus very precise and documented. Many of these lessons can be applied to other nations that wish to counter Russian efforts to manipulate them, since other European nations also have their own grudges.

Russia, meanwhile, continues to ignore the importance of values and a quest for truth. Instead, it works to develop its own objective view of reality, one that is not shared by the European community at large. The Kremlin, from its responses to date, indicates that it is destined to ignore the realities (and there are many) that do not reflect well for actions it has committed. It is prone in many cases (MH-17, Skripal poisonings, Olympic doping, etc.) to invent its own version of reality.

5 Recommendations

The US should use Lithuania's experience as one example/guide to countering Russian techniques. While Lithuania has a different history and understanding of Russia than does the U.S., insights from Vilnius about Russian methods are beneficial and will improve the US's overall comprehension of Russian goals. To achieve its goals in Lithuania, Russia has used character assassination, threatening letters to the Lithuanian embassy in Moscow, defamation, fake news, intimidation, rewrites of history, and various forms of pressure. The US can expect that some of these methods, fine-tuned to the US experience, would be used against Washington and thus should be on a thematic watch list.

Lithuanian analysts have offered several unique perspectives on Russian propaganda that are specific to the region. Taking Lithuania's response under consideration can help NATO prepare ways and means to offset Russia's information onslaught there and in other Baltic nations. The Lithuanian response has been specific, offering ten targets of Russian propaganda; five layers of Russia's propaganda image; a look at Russia's dissemination network for propaganda; and an outline of a Russian propaganda campaign.

US adults and students, like Lithuanian citizens, should be made aware of Russian dissemination techniques, which include not just the Internet but attempts to manipulate many other organizations. Targets for the dissemination of Russian propaganda include public organizations, information movements, and social media, among others. Russia often finds elements in these groups that are receptive to its arguments, since some Russian themes, hidden in various sources and presentations, are accepted without deeper research about their potential manipulation capability. Education is important to make people aware of such techniques, not only for adults but also for high school and college students. Learning how to think critically is important, as is being a skeptic of information obtained from a potential adversary. Another important dissemination area, this time in relation to the Internet, is the sale of Russian anti-virus materials, such as the Kaspersky Anti-virus product. Such materials can later be used by Russian special services to infiltrate US systems. To date, not only Lithuania but also Ukraine and the U.S. have stopped using this product in government systems, warning citizens that if they use Kaspersky products, they do so at their own risk.

The US should pay closer attention to the problems that exist in its society, as Lithuanians do about their problems, since they are the most likely targets for Russian manipulation

[46] See, for example, Joana Lapeniene, "Year is About to End, Information Warfare Continues," *LRT.lt*, 31 December 2017.

attempts. Russia pays close attention to schisms in Lithuanian society, and it looks for US societal problems as well. One Russian PSYOP specialist told this author that the US publication *Army Times* provided themes for him to use against the US during the Cold War, since the publication listed the problems of servicemen in each issue. From the Russian perspective, problems are targets. Russian themes are designed to exploit problems and shake a citizen's resolve, skew historical memory, and discredit ties with allies. Russian themes are well-hidden, making it hard to discern what is fake and what is real, and unreliable context creates tension and confusion in society. The Russian attacks use images and myths as well to create mistrust. Following Lithuanian methods to counter such attempts in their country is instructional, as the US can learn new ways Lithuania has found to respond to Russian themes and also find out which responses do not work as well as others.