Vilnius University

INSTITUTE OF INTERNATIONAL RELATIONS AND POLITICAL SCIENCE

Eastern European and Russian Studies Programme

Hugh Cook

BALTIC RESPONSES: COUNTERING RUSSIAN INFORMATION WARFARE OPERATIONS IN THE 21st CENTURY INFORMATION, CYBER, AND PSYCHOLOGICAL SPACES

MASTER'S THESIS

10 January 2021

Vilnius, Lithuania

TABLE OF CONTENTS

Page

INTRODUCTION……...1

Methodology……...……3

Research Question……...5

Theory…….5

CHAPTER 1

ESTONIA

Background…….8

The Estonian Information Space in the 21st Century…….17

The Estonian Cyber Space in the 21st Century……..19

The Estonian Psychological Space in the 21st Century…….29

Estonia Summary…… 35

CHAPTER 2

LATVIA

Background……..37

The Latvian Information Space in the 21st Century…….38

The Latvian Cyber Space in the 21st Century……..50

The Latvian Psychological Space in the 21st Century……..57

Latvia Summary……...66

CHAPTER 3

LITHUANIA

Background……..67

The Lithuanian Information Space in the 21st Century……73

The Lithuanian Cyber Space in the 21st Century…….89
The Lithuanian Psychological Space in the 21st Century……97
Lithuania Summary……103

RECOMMENDATIONS……105

CONCLUSION……...108

SUMMARY……110

LIST OF LITERATURE……112

ACRONYMS……..121

Introduction

Russian interference in the elections and government affairs of foreign nations has become a well-documented phenomenon in the previous two decades and has been thoroughly analyzed by politicians, academics, and journalists throughout the world. Many of these high-profile interventions have occurred within the last fifteen years under the increasingly autocratic presidency of Vladimir Putin, who has capitalized on the technological shifts of the digital age by adapting Soviet-era information warfare tactics for a 21st century digital environment. A major staple of Russian foreign policy in the Putin-era has been that of interfering with other nations, a policy which is not confined to Europe or other Western countries. Since 2004, there have been at least 27 recorded attempts by Russia to interfere in elections in Europe and North America.[1] While cases differ, there are many similarities between them, with the Russian approach often being a multi-faceted one, which may include cyber-attacks and disinformation campaigns.[2]

Nowhere have these incursions been more noticeable than in the Baltic states, which once formed the three westernmost republics of the Soviet Union. Their capitals of Tallinn, Riga, and Vilnius lie within a few hundred kilometers or less of the Russian border, which makes the reality of hybrid warfare a serious concern. The Baltic States are the most vulnerable countries that NATO is obligated to defend.[3] Due to their close geographic proximity and shared political history, Estonia, Latvia, and Lithuania are keenly aware of the methodologies and intentions of the Russians and the consequences of being on the receiving end of their information warfare efforts. Their existence is strongly tied to NATO and the EU, which have not only provided security assistance, but economic aid, institutional support, and a shared sense of European identity.

The 2007 Bronze Night events in Estonia showcased Russian and its affiliated actors' offensive capabilities to wreak havoc on a country that prided itself on its technological

---

[1] Laurinavicius, Marius. "A Guide to the Russian Tool Box of Election Meddling: A Platform to Analyse the Long Term Comprehensive Kremlin Strategy of Malign Influence." International Elections Study Center. p. 5. 4 December 2018. Retrieved 17 October 2020. http://iesc.lt/app/uploads/2018/10/IESC_Guide_ToolBox_2018_FINAL.pdf

[2] Ibid

[3] Marler, Scott W. "Russian Weaponization of Information and Influence in the Baltic States." Master's thesis, U.S. Army Command and General Staff College, 2016. P. 11. Leavenworth, Kansas: U.S. Published: Army Command and General Staff College. Retrieved 17 October 2020. www.apps.dtic.mil/dtic/tr/fulltext/u2/1038780.pdf.

achievements. Protests that occurred in Latvia concerning the use of the Russian language in education and in the public and private spheres drew the ire of Russia, and thus mass protests against this policy. The financial influence Russia has had in Lithuania's media environment has been noted and has only spread, keeping Russian cultural initiatives in the public eye for years. These, among countless other hard- and soft-power initiatives, are methods which Russia has used to dictate policy and spread its influence in the region, all with the objective of weakening the Baltic states and making them more dependent on Russia. Despite these events, Western attention would not be focused on the region, nor would the full extent and consequences of Russia's information operations be fully understood for several more years by Western observers, until Russian separatists began efforts to take eastern Ukraine and Russian troops annexed the Crimean Peninsula.

Although the populations of the Baltic states are relatively small compared with other European and post-Soviet countries (the populations of Estonia, Latvia, and Lithuania combined equal less than 10% of Russia's population),[4] the resilience and understanding that the Baltic states possess can provide other nations facing Russian warfare efforts with the necessary tools and strategies to implement policies and protocols that may assist them in warding off information operations.

The problems that the Baltic states face are many and multifaceted. They require countermeasures, planning, and proactive efforts to ward off Russia's incursions and influence. Challenges currently posed in the information, cyber, and psychological environments necessitate responses by the entire society and are often asymmetric to Russia's offensive measures. A lack of understanding, a strong desire to adopt Western media economic models, the lack of adequate training or educational opportunities for technical specialties, as well as complacency, have all been factors in the Baltic state's difficulties in preparing for, and responding to, outside interference.

This thesis focuses on efforts that have been made in the Baltic countries to secure the information, cyber, and psychological spaces. Emphasis is focused on the last two decades,

[4] Marler, Scott W. "Russian Weaponization of Information and Influence in the Baltic States." Master's thesis, U.S. Army Command and General Staff College, 2016. pp. 8-11. Leavenworth, Kansas: U.S. Published: Army Command and General Staff College. Retrieved 17 October 2020. www.apps.dtic.mil/dtic/tr/fulltext/u2/1038780.pdf.

which includes the rapid progression and adoption of digital technologies throughout these societies. These developments ultimately provide resources and methods to protect these environments, but also pose new challenges that must be met. State efforts alone are insufficient and unable to provide for the security environments that are necessary in this era, which ultimately require preparation and responses by the entire society. Educational initiatives, implemented at the state level and by non-governmental organizations, the private sector, and by institutes of higher education provide further coverage of the gaps that one sector alone cannot.

Methodology

The methodologies used in this thesis include the qualitative analysis of academic and professional publications, academic journal articles, media and information warfare reports, working papers, official government publications, strategy briefs, and published analysis by multi- and supra-national security organizations. I also interviewed professional media scholars, professional journalists, and directors of policy institutes. Information gathered from these sources was chosen for several reasons, which included the analysis, expertise, and peer review process by scholars in the fields of information, cyber, and psychological security. Qualitative data was more useful than quantitative data as the necessary information sources were explanatory in nature and not usually numerical. Thematic analysis, a sub-context of qualitative analysis, was also utilized in analyzing content, both regarding primary and secondary sources. Thematic analysis enabled the identification of cross-data themes and contexts, which was useful in gaining clarity when comparing textual and interview content.

Documents were chosen for their theoretical and practical applicability, as well as for their explanatory and definitional content, which helped to interpret and contextualize information sources. Interviews were conducted to provide additional information that was not included in printed sources or could not be found or clarified in publications. Interviewees were chosen because of their level of expertise, breadth of career experiences, diversity of professions, and willingness to participate in the research process. Ideally, more than one interview was conducted with experts in each of the three Baltic states. I chose this approach for several reasons. It allowed me to ask the same questions to different interviewees so that I could compare and analyze their responses. Questions were provided to interviewees in advance so

they could familiarize themselves with the questions and conduct possible research to provide answers. Data content was taken from different sources, many of which were academic journal or professional organization websites. Traditional print sources, namely books and newspaper articles, were also utilized in the writing process.

To give credibility to my analysis, primary sources were sought, if possible, to ascertain information directly from policymakers, academics, or professionals with direct knowledge of information warfare and security issues. For the most part, primary sources were readily available digitally and provided access to their websites or databases. Secondary sources were also utilized, though not as regularly as their primary counterparts. Secondary sources primarily consisted of news articles that included information cited from primary documents or was obtained through informational interviews. Several secondary sources reiterated content that was found in other secondary sources, though the analytical and informational content value was still useful, and often provided additional information not found in earlier secondary sources. In analyzing content, several approaches were used to ensure that I understood the information presented, and to further investigate conflicting sources. Analysis for conducting interviews was somewhat more difficult, though the same general approach was taken to ensure that what was stated in the interview(s) was in line with primary or secondary sources gathered from databases, websites, or physical sources.

Several major problems were also encountered in the research and writing process. These included, but were not limited to, a lack of responsiveness for interview requests, the non-specific nature of the content presented in secondary sources, the lack of public availability of some academic sources, and occasional technical problems with videoconferencing platforms.

Interviews were conducted using Skype or Zoom over a period of several months during the spring, summer, and fall of 2020. Interviews consisted of a short introduction and declaration of intent for the use of written and verbally communicated information. The timeline and length of the interviews varied, but an average timespan was approximately forty-five minutes to one hour and fifteen minutes. Audio was transcribed using an online transcription service, providing a textual transcript of the interview. Interviewees were chosen for their knowledge of the subject area and their ability to fill in information gaps that were not adequately addressed or were not available in the literature review.

Research Question

In this thesis, I focus primarily on measures to protect against Russian information warfare operations in the Baltic states, implemented at the state level, in the private sector, through non-governmental organizations (NGOs), and efforts made by these states with multi-national alliances, such as the North Atlantic Treaty Organization (NATO) and the European Union (EU). Attention is also focused on the cooperating partners and future measures in this fight.

My primary research question is, "How are the Baltic societies responding to Russian information warfare operations in terms of their methodologies, asymmetric approaches, cyber policies and technology?" A secondary focus is centered on the effectiveness, problems, and future outcomes of these measures. My research questions are intended to guide critical analysis and to analyze existing scholarship on these aspects of security as well as to provide original perspectives and recommendations for the enhancement of the information, cyber and psychological security environment in the Baltic states.

There are several assumptions that I make throughout this paper. First, it is assumed that with experience and greater resources, the Baltic societies will be able to create policies and countermeasures that will counteract Russian information warfare efforts. Secondly, it is assumed that Russian propaganda and disinformation will continue to advance technologically, so the Baltic states must maintain and increase their activities in the coming years.

Theory

For this thesis, I have utilized Barry Buzan's concept of an expanded security construct applied to the protection of the information, cyber, and psychological spaces of the Baltic states. The widespread availability and adoption of digital technologies and the increased presence of interconnected media sources, including social media platforms, have transformed how societies worldwide function and interact with one another as well as how citizens interact with each other. While the concepts of traditional security are still very prevalent and applicable in the modern era, the development and expansion of non-traditional warfare methodologies has increased exponentially as well. Technological advances, in addition to improvements in

weapons systems, has allowed for an intellectualizing of this environment and the digitizing of war. As global events have shown, it just as advantageous, if not more so, to weaken an adversary from within than to resort to kinetic warfare.

Traditional security concepts, though necessary, are not adequate for the technologies and electronic infrastructures that have come to define the 21st century. The threats that face modern states and societies have grown so significantly that they raise questions as to what can, or may, constitute a threat. The traditional concepts of security, based on hard power, need to be expanded to include these new threats and technologies. This thesis uses an idea advanced by Barry Buzan that the security field be reconceptualized - broadened - to include "a substantial range of concerns about the conditions of existence."[5] Buzan's expansion of the traditional security field allowed for the concept of societal security to enter the theory realm. This paper is concerned with the Baltic states which continue to face serious pressures from societal fissures, manifesting themselves in ethnic and linguistic divides. The multitude of threats to the Baltic states and their survival goes beyond political debates and the politicization of issues. It is as a reality that impacts real people and real societies. Buzan states that, "Security is taken to be about the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change, which they see as hostile. The bottom line of security is survival, but it also reasonably includes a substantial range of concerns about the conditions of existence."[6]

Identifying threats is a major problem modern states must contend with, which has only proven more challenging in the digital age. Lines that once clearly existed between the threatening and non-threatening have become increasingly blurred, with almost anyone having the capability to carry out harmful acts against people, places, and systems. As an example, then-National Defense Minister Juozas Olekas noted that the 2002 *National Security Strategy* was outdated and added that, "New challenges, including hybrid warfare, cyber and informational challenges, and a changed geopolitical situation have emerged."[7]

---

[5] Buzan, Barry, "New Patterns of Global Security in the Twenty-first Century" *International Affairs,* 673 (1991), pp. 432-433. Retrieved 26 December, 2020.
[6] Ibid
[7] "Lithuania to draft new National Security strategy." (2015, 27 October). baltictimes.com. Retrieved 29 December 2020. https://www.baltictimes.com/lithuania_to_draft_new_national_security_strategy/

Buzan's widened concept of security allows for societies to focus on the many ways in which hostile actors can adversely affect them. This paper broadly groups these concerns into three categories: information, cyber, and psychology security. For information security, concerns include the dissemination of media content, the economics of media ownership, and the effects of media on consumers. All these aspects of the information environment are subject to manipulation by outside actors, especially by Russian information warfare operations aimed at, and within, the Baltic states. For cyber security, concerns are about everything from securing school records to securing NATO's communication and command systems. For psychological security, concerns are center on the ethnic and linguistic divides in the Baltic countries that Russia exploits. Because of the demographic composition of the region, security efforts have long been identified, but often not implemented, or the necessary security measures were not implemented until the psychological environment had been placed in Russia's favor. Further securing the psychological space includes providing media literacy classes throughout society and providing adequate minority language programming options and opportunities, furthering integration efforts to homogenize ethnic and linguistic minorities and shift media consumption habits and enhance critical thinking skills.

CHAPTER 1

Estonia

Background

Since declaring independence from the Soviet Union in 1990, the security environment that initially greeted the re-established republic has changed significantly. Both regionally and globally, great strides in technological progress, a revisionist and autocratic Russia, and democratic fatigue throughout the Western world have allowed Estonia's adversaries to engage in hybrid and information warfare operations that have caused much concern among policymakers and throughout Estonian society. Despite these changes, Estonia, the least populous and northernmost Baltic state is one of the most technologically advanced countries worldwide and recognized by many countries throughout the world as a successful example of a technologically advanced society.

The Estonian information space can be regarded in one of two major conceptions, depending on what perspective is applied. The first one is an open and independent media environment that largely follows democratic norms and allows for freedom of speech, media

consumption, and media ownership. The media environment is regarded as free and open[8], where censorship is officially prohibited. This perspective is the most prevalent both within Estonia and to external observers. However, it is also important to consider the contrasting perspective, which focuses on the ethnic and linguistic divide that exists between Estonians and ethnic Russians. Significant changes that took place in the first several years after gaining independence could be considered protective measures, as they were a psychological and cultural cleansing of the Soviet period-a time that many Estonians would like to forget.

Although the ethnic Russian minority has been more adequately integrated into Estonian society than in some post-Soviet countries, they continue to consume Russian-based media that largely centers on propagating Russia-friendly perspectives. These perspectives negatively portray Estonia using a number of false and misleading narratives. These include Estonia being dependent on NATO and its Western allies for its survival, that Estonians are fascist and/or Nazi sympathizers due to their support of the Nazi forces in the region during World War II, and that the quality of life in Estonia is substandard in comparison to Russia. Protecting the information and cyber space has been a major priority in the 21st century. Russia showcased its offensive capabilities by crippling Estonian society during the Bronze Night and by mobilizing Russian-speakers and sympathizers in Ukraine in 2014. Countering Russian information warfare operations requires a multifaceted response; asymmetrical approaches have been more reactionary than proactive in nature. Sharing a political and geographic history, and a cultural and linguistic one, Estonians understand Russia's capability to carry out information operations, and are dedicated to take appropriate measures as the country approaches its third decade as an independent nation.

The dissolution of the Soviet Union brought about the demographic reality that nearly a third of the newly formed republic's population was ethnically Russian or were Russian speakers. Strong feelings of nationalism and a desire to resurrect the previous Estonian Republic created a stark divide between Estonians and ethnic Russians in nearly all aspects of society. Although the Estonian constitution provides for the "right to freely disseminate ideas, opinions,

[8] Loit, Urmas, & Harro-Loit, Halliki. "Media Pluralism Monitor 2016 Monitoring Risks for Media Pluralism in the EU and Beyond." Report. pp. 4-12. December 2016. Retrieved 18 November 2020. Centre for Media Pluralism and Media Freedom. https://cadmus.eui.eu/bitstream/handle/1814/46794/Estonia_EN.pdf?sequence=1&isAllowed=y.

beliefs and other information by word, print, picture or other means,"[9] media policy was primarily modeled on a liberal, market-based approach that significantly favored Estonians and the Estonian language. The 1990's saw the dramatic shift from Soviet media and broadcasting standards to a Western model, in which, "All production, transmission and receiving equipment was replaced."[10] A fresh generation of journalists in the newly established independence era gravitated towards an Anglo-Saxon model of media commercialization[11], which has been the most prevalent source of information in Estonia ever since. This free-market ideology changed media content and brought about the combining of information and entertainment[12], a process known to journalists and media scholars as "infotainment"; this led to obstacles in properly contextualizing and analyzing news events and has impeded integration efforts.[13] However, public broadcasting services often cover stories with greater contextual clarity and also provide an alternative to commercial media outlets. Trust in national media remains higher than in many Western nations, where faith in media and institutions is waning.

Efforts to provide Estonian-based Russian-language media have increased in the 21st century, but these endeavors have been less enthusiastic than for Estonian-language content. The changes that took place in the Russian-language media landscape in the early independence era were significant and disadvantageous to its audience. The number of hours of Russian-language broadcasts declined dramatically on television and no effort was made to replace them on programming schedules, nor were any efforts made to reestablish national Russian-language TV channels.[14] Estonian media policy in the early 1990's placed a low emphasis on media targeted towards the Russian minority and was based on two assumptions. The first was the belief that Russian-language media did not need government support because the demographic situation

---

[9] Ibid, p. 11.

[10] Joesaar, Andres, Rannu, Salme, & Jufereva, Maria. (2013). "Media for the Minorities: Russian Language Media in Estonia 1990-2012." Media Transformations. p. 122. Retrieved 22 November 2020. https://www.vdu.lt/cris/handle/20.500.12259/31465

[11] Vihalemm, Peeter. (2006) "Media Use in Estonia: Trends and Patterns." Nordicom Review. p. 18. Retrieved 18 November 2020. https://www.researchgate.net/publication/47502946_Media_Use_in_Estonia_Trends_and_Patterns

[12] Ibid

[13] Ibid

[14] Joesaar, Andres. "Day After: The Impact of the Launch of the Russian-Language Television Channel ETV+ on Estonian Public Broadcasting's Viewing Trends." 2017. Vol. 2, p. 40. Report. Tallinn University. Retrieved 18 November 2020. https://www.researchgate.net/publication/318984136_DAY_AFTER_THE_IMPACT_OF_THE_LAUNCH_OF_THE_RUSSIAN-LANGUAGE_TELEVISION_CHANNEL_ETV_ON_ESTONIAN_PUBLIC_BROADCASTING'S_VIEWING_TRENDS

would come to disfavor minority media and that emigration, and assimilation for those Russian-speakers who remained, would be adequately satisfied by Estonian-language media.[15] The second assumption centered on the idea that newly instituted free market principles in the media sector would allow for the creation of minority language media opportunities and that linguistic integration would not need state intervention or regulation.[16]

Russian-language programming did not disappear from Estonian television entirely, however, as cable providers filled the void and began to rebroadcast these channels and expand their networks to the Russian-speaking audience.[17] The new TV linguistic divide came into being in a far more noticeable way after this rearrangement, and has contributed to a schism that persists to the present day in the Estonian television audience.[18] Television has been the main source of information for both Estonians and the Russian minority, even with the increased prevalence and popularity of social media. However, by 2000, the budget for Russian language programming had been drastically reduced[19], thus severely limiting Russian language media and providing no viable domestic television alternative. Entertainment and news programming for Russian-speakers almost exclusively emanates from inside Russia. A 2014 Saar poll indicated that 72% of the Russian-speaking audience named Russian state TV channels PBK, RTR, Planeta Baltic, NTV Mir, and Ren TV Estonia as their most important sources of information, with more than half of all viewing time dedicated to these outlets.[20] In contrast, the Estonian-language TV channels Kanal 2 and TV3 had a majority Estonian audience but had low viewership among Russian-speakers. The poll also indicated that Estonians were highly tuned in to the public Estonian Television, with 81% of those polled listing it as their main information source.[21]

The launch of ETV+ by Estonian Public Broadcasting in September 2015 marked the first major state effort to market Estonian-based Russian-language television news and

---

[15] Ibid, p. 43.
[16] Ibid
[17] Ibid
[18] Ibid
[19] Joesaar, Andres, Rannu, Salme, & Jufereva, Maria. (2013). "Media for the Minorities: Russian Language Media in Estonia 1990-2012." Media Transformations. p. 142. Retrieved 22 November 2020. https://www.vdu.lt/cris/handle/20.500.12259/31465
[20] Ibid, p. 41.
[21] Ibid

entertainment programming to Russian-speakers since declaring independence. This was due, in part, to potential security concerns Estonian officials had regarding Russia's actions in Ukraine in 2014. Proposals to provide a publicly funded Russian-language channel were discussed regularly in the first 25 years of independence, but remained only in the theoretical phase as they were met with criticism from politicians and political elites with fears that such channel(s) could undermine the Estonian language and pave the way for Russian to become a second official state language.[22] Reasons against creating a national channel were more numerous and influential than were the reasons to create Russian-language programming. Some of these concerns claimed:

- that creating high-quality programming would be too costly and would require resources that were unavailable to Estonia[23]
- that competition from other countries would compete for the Estonian audience[24]
- that assimilation, through time, would integrate Russian-speakers well enough so they would not need Russian-language media[25]
- that there would be an inadequate workforce to staff new programs[26]

Arguments to create Russian-language programming include:

- bridging the gap between the two ethnic groups[27]
- providing quality sources of information to all Estonian residents[28]
- hoping that minority-language programming would ease tensions that existed in society[29]

[22] Joesaar, Andres. "Day After: The Impact of the Launch of the Russian-Language Television Channel ETV+ on Estonian Public Broadcasting's Viewing Trends." 2017. Vol. 2, p. 44. Report. Tallinn University. Retrieved 18 November 2020. https://www.researchgate.net/publication/318984136_DAY_AFTER_THE_IMPACT_OF_THE_LAUNCH_OF_THE_RUSSIAN-LANGUAGE_TELEVISION_CHANNEL_ETV_ON_ESTONIAN_PUBLIC_BROADCASTING'S_VIEWING_TRENDS
[23] Ibid
[24] Ibid
[25] Ibid
[26] Ibid
[27] Ibid
[28] Ibid
[29] Ibid

- balancing or counteracting Russia's influence with an Estonian narrative, thereby decreasing the risk of Russian information warfare operations[30]

The launch of ETV+ is one of the latest examples in Estonia's attempts to further secure its information space. The channel's promise to viewers is that it provides a voice for those who consider Estonia home and to discuss issues and people that matter to them.[31] ETV+ also offers viewers a chance to be active participants in its programming, which includes video blogs, social media, apps, events, and a website, in addition to its television and radio programs.[32] Studies indicate that the viewing habits of Russian-speakers did not change significantly after the ETV+'s launch; the anticipated audience did not materialize.[33] A major challenge for Estonian media officials has been getting a Russian-speaking audience to tune in to programming, which has continually lagged behind its Russian-based counterparts. A significant increase in viewership, however, occurred in 2020 during the coronavirus pandemic. The increase in audience size has been attributed to local coverage of the virus, which Russian-based outlets do not cover.[34] Additionally, the spread of the virus is nearly impossible to cover with fake news, as vital information is necessary to maintain the health and safety of the public.[35] Local information and knowledge of government actions are a necessary component to this objective.

Estonian-based Russian-language radio has a longer history and a greater variety of programming than Russian-language television. Like most media outlets in Estonia, the majority of radio channels are owned and operated by private companies. The public Estonian Radio has gained a respectable listenership, with a notable example being Raadio 4, a channel that is specifically targeted at the Russian-speaking community. First airing in 1993, this channel broadcasts programming that is of interest to Russophiles, including topics such as social issues

[30] Ibid, p. 45.
[31] Ibid, p. 43.
[32] Ibid
[33] Bahovski, Erkki. "First Steps towards the Estonian Media Space." 2 April 2020. Retrieved 19 November 2020. https://icds.ee/en/first-steps-towards-the-estonian-media-space/
[34] Ibid
[35] Ibid

and politics.[36] However, even with the longevity of the station and a respectable listening audience, the ethnic divide continues to showcase itself as was the case with Raadio 4's coverage of Russia's actions in Crimea in 2014.[37] Significant criticism was levied at the station's coverage of Russia's annexation of Crimea, which was seen as favoring a Western narrative, ultimately causing a sizeable segment of listeners to abandon the station.[38] Many of these listeners are thought to have migrated to Russian-based sources, even if only for these events.

The dawn of the 21st century saw the establishment of more Russian-language radio stations, although content was far more likely to come from centralized sources than from local programming, which was largely due to economic factors. Smaller regions, and local content, often consumed resources and funding that was greater than local advertising revenue.[39] Today, Russian-language radio remains a popular source of information for Russophiles. Radio does not cause as much concern to Estonian officials as television, online news sites, and social media; but licensing and content monitoring are still practiced, in attempts to ensure the freedom, legitimacy, and security of the airwaves.

Estonian Russian language print media has also been popular among Russophiles. Despite the turbulent nature of the 1990's Russian-language media market, and the effects of the 1998-2001 economic crisis when Russian-language outlets' main objective was their survival, relative stability was eventually achieved, continuing into the early years of the new millennium.[40] Due in part to media consolidation and the trend towards digitalization, the number of Russian-language newspapers decreased significantly. The late 2000's financial crisis took a major toll on minority-language media, which have never fully recovered.[41] Daily newspaper circulation has been in decline since the late 1990's, even during strong economic

---

[36] Lavrentjev, Ivan. (2020). "The Securitization of Russian-speaking Media in Estonia: Case Study of ETV+ Channel." Master's thesis, University of Helsinki. p. 19. University of Helsinki. Retrieved November 23, 2020. https://helda.helsinki.fi/bitstream/handle/10138/316401/Lavrentjev_Ivan_thesis_2020.pdf?sequence=3

[37] Ibid

[38] Meister, Stefan. (Ed.). (2018). "Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia" (ifa Edition Culture and Foreign Policy). p. 47. Stuttgart: ifa (Institut für Auslandsbeziehungen). https://nbn-resolving.org/urn:nbn:de:0168-ssoar-59979-0

[39] Joesaar, Andres, Rannu, Salme, & Jufereva, Maria. (2013). "Media for the Minorities: Russian Language Media in Estonia 1990-2012." Media Transformations. p. 131. Retrieved 22 November 2020. https://www.vdu.lt/cris/handle/20.500.12259/31465

[40] Ibid p. 123

[41] Ibid, p. 124.

times.[42] As news content began to migrate to a digital format, newspaper circulation further collapsed. By 2011, there was only one national daily Russian-language newspaper, and only one that was delivered throughout the Baltic states.[43] Today, nearly all remaining Russian-language publications are distributed only regionally or locally, and many of these are published only weekly, biweekly, or monthly.

The first online news sources appeared soon after the turn of the new millennium. By the 2010's, privately-owned Russian-language websites were the most common online information source for Russophiles while ERR hosted a small online presence.[44] Independent news sources did not have a significant presence online as financial constraints largely prevented them from achieving success even though there were numerous attempts at launching them.[45] Somewhat surprising is the situation with Russian-language sources originating in Russia. These sources, either linked directly to the Russian government, or controlled by it, have smaller audiences than Estonian-based Russian-language online portals. In May 2017, the local Sputnik website had approximately a quarter million visitors while the Russian language version of Postimees had approximately 2.6 million visitors.[46] Unlike the other sources of Russian language media in Estonia, Russian-based websites have a larger share of their audience in Russia than they do in Estonia. The issue of ensuring that media content was not unduly influenced by outside actors was a significant concern when Estonian media policy was being developed.[47] Both the legislative and executive branches were concerned that state policies should adequately provide for the needs of the Russian-speaking community, but the threat posed by Russia had to be considered, especially regarding Russian money. Establishing the "correct political undercurrent"[48] was part of the process, and government-issued licenses were a visible and practical way of providing for information security.

---

[42] Ibid, p. 125.
[43] Ibid
[44] Lavrentjev, Ivan. (2020). "The Securitization of Russian-speaking Media in Estonia: Case Study of ETV+ Channel." Master's thesis, University of Helsinki. p. 19. University of Helsinki. Retrieved November 23, 2020. https://helda.helsinki.fi/bitstream/handle/10138/316401/Lavrentjev_Ivan_thesis_2020.pdf?sequence=3
[45] Ibid
[46] Ibid
[47] Joesaar, Andres, Rannu, Salme, & Jufereva, Maria. (2013). "Media for the Minorities: Russian Language Media in Estonia 1990-2012." Media Transformations. p. 130. Retrieved 22 November 2020. https://www.vdu.lt/cris/handle/20.500.12259/31465
[48] Ibid

Estonia, like its southern neighbor, Latvia, had a similar idea of broadening the concept of security due to its comparable demographic composition. As the first Baltic state to enter accession discussions to the EU and NATO in the late 1990's, Estonia found itself concerned with military, historical, cultural, and demographic security. After regaining independence, the Estonian parliament narrowed citizenship requirements in the new Estonian republic and reenacted a 1938 citizenship law, which declared that only those who could trace their lineage to pre-Soviet times would be granted citizenship.[49] In October 1992, the Estonian parliament ruled that the new Estonian republic was in essence a continuation of the previous Republic that existed from 1918-1940.[50] Unsurprisingly, this declaration did little to improve relations with Russia, foster feelings of unity, or quell ethnic divisions after the collapse of the Soviet Union. With feelings of intense nationalism, the historical legacy of Estonia was "defined" to celebrate and enhance what Estonia was and who or what could truly be Estonian. After European, Russian, and international criticism, citizenship and language requirements were liberalized to conform more with European and international norms, making Estonia a more attractive candidate for EU and NATO membership. With the ethnic Russian minority gradually becoming more integrated into Estonian society, the fears about the linguistic and demographic environments have eased. The political security environment has also become slightly less worrisome over time, as most ethnic Russians have voted or become party members of mainstream Estonian political parties. There are currently no major political parties in Estonia that openly advocate for pro-Russian policies. However, there are noted exceptions to this liberalizing trend, with information security being a special concern. The reforms on citizenship and language allowed Estonia eventual membership in NATO and the EU, which further antagonized Russia.

Due to several factors, which include economic, cultural, political, and security aspects, the Estonian information space is still susceptible to Russian narratives and exploitation through the content disseminated by Russia-based media outlets, the activities organized under its Compatriot Policy, in addition to other soft power initiatives. Linguistic segregation continues to plague integration efforts, although significant progress has been made in this area. There is hope among Estonian officials that increased attention and Estonian-based programming aimed at

[49] Ibid, p. 29.
[50] Ibid

Russophiles will reap benefits, though this will be a slow process that will never truly sever Russophiles from Russian media or soft power initiatives.

The Estonian Information Space in the 21st Century

Estonia has long been proud of its security and access in the digital space. The advancement and shift towards a more digital environment have led to security discussions focused on cyber security, also known as "security in the information space". Continued technological advancements and expansion of electronic services throughout Estonian society have become a major emphasis for government leaders, with access to cyber networks considered a fundamental right and freedom for all Estonians.[51] Several different cybersecurity strategies have been implemented in the 21st century, each building and expanding upon earlier strategies and practices. The "e-Estonia" initiative was established in 1997, which is a partnership between the Estonian government and Enterprise Estonia. This organization seeks to develop the national economy by exporting goods and promoting Estonian businesses, increasing revenue from tourism, and attracting foreign investment to the country.[52] Estonia has been a successful example for other countries making the transition to the digital age.[53] To provide for the vibrancy that is necessary to ensure a safe environment, Estonians must be able to put their trust in institutions that transcend Estonian society. Therefore, much effort has been placed on protecting the psychological aspect of the populace, part of a greater effort of total defense implemented throughout Estonia, which consists of government institutions, the private sector, and civic organizations.[54] Unlike the current situation in many Western countries, as well as in the other two Baltics, state institutions and the national media are generally regarded as trustworthy.

---

[51] "Cybersecurity Strategy." (Publication). Republic of Estonia Ministry of Economic Affairs and Communications. 2019. Retrieved November 10, 2020. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[52] "Enterprise Estonia." (n.d.). Retrieved 4 December 2020. https://www.eas.ee/eas/?lang=en

[53] Barnett, Genna. (2019, February 25). "Digital Frontrunners Spotlight: Estonia." Nesta. Retrieved 4 December 2020. https://www.nesta.org.uk/blog/digital-frontrunners-spotlight-estonia/

[54] Kepe, Marta, & Osburg, Jan. "Total Defense: How the Baltic States are Integrating Citizenry into their National Security Strategies." Small Wars Journal. 24 September 2017. Retrieved November 11, 2020. https://smallwarsjournal.com/jrnl/art/total-defense-how-the-baltic-states-are-integrating-citizenry-into-their-national-security-

Estonian media policy has centered on the state's interaction with professional media organizations, granting broadcast licenses for radio and televisions broadcasters. As is the case with many democratic governments worldwide, the Estonian government largely relegates the rights and responsibilities of instituting sound journalistic practices to professional media organizations and NGOs, who implement guidelines and set parameters on acceptable standards for news content. However, the Estonian government has been actively involved in monitoring content from Russian-based media sources, namely, terrestrial radio and television broadcasters, to ensure that the Estonian information space is protected from outside actors and influencers that aim to spread propaganda and disinformation. By definition, democratic governments should not censor information, which is counter to constitutional guarantees on the right to receive and disseminate content. Although Estonia strives to uphold this ideal, anti-democratic measures must sometimes be undertaken to ensure the integrity of the information space.

In defending the Estonian information environment, media organizations understand the need to be as objective and factual with their audience as possible. Having shared a long and storied history with Russia, transparency and objectivity are two major areas that media organizations understand are necessary to countering information warfare operations. As in Latvia, protecting the information space and integrating ethnic Russians into Estonian society have been necessary ways in which to counter Russian information warfare efforts. In attempts to preserve the Estonian language and promote the country's cultural identity, minority language media was not necessarily discouraged, but it was not treated as a necessity. Private enterprise was largely expected to create opportunities that would cater to this demographic. Estonian media policy has not changed significantly since the country gained independence, but the need for situational awareness and technological changes have given new perspective to Estonian officials as well as private enterprise, NGO's, and the broader society. Estonian security policy did not often mention information security specifically in early National Security Strategies, but when it was, it was often linked to the cyber domain and the existence of online content. Even after the 2007 Bronze Night events, media policy was dealt with by professional media organizations, who understood the need in meeting the demand for objective sources of information.

Public broadcasting is highly regarded as providing objective content, and Estonian-based Russian-language radio has been a long-term source of information to the Russian-speaking community. Despite these efforts, Estonian-based Russian-language television has a significantly smaller audience because it was only established in the last few years.

The Estonian Ministry of Culture is the state agency that is responsible for the country's broadcasting policy. The development of Estonian media under the Western model has been perceived as an economic issue; until recently it discounted minority language media and did not feel an obligation to serve different demographics in society.[55] The events in Ukraine in 2014 were a stark reminder that there still exists two information spheres and two different conceptions of reality in Estonia, which is almost exclusively centered on the ethnic and linguistic divide. The Saar Poll OÜ survey, conducted in 2014, in both the Estonian and Russian languages, showed that Estonia has had trouble "providing pluralistic and reliable content for society as a whole, especially for the Russian-speakers and that the frequency of following the news among Estonians and Russian speakers is relatively similar."[56] Even though recent initiatives to change this have been well documented, they have either been insufficient for the demand or have occurred far too late to ensure a loyal and sizeable audience. All these factors, coupled with the market-dominated approach to media, indicate that media efforts to appeal to Russophiles have had only limited success.

The Estonian Cyber Space in the 21st Century

Estonia has long been developing a secure cyber security environment. Prior to gaining independence, Estonia was not technologically advanced, with over half of Estonians lacking basic household technologies, such as a telephone line.[57] Under Prime Minister Mart Laar in the 1990s, the decision was made to commit Estonia to becoming a technologically advanced

[55] Jõesaar, Andres. (2015). "One Country, Two Polarised Audiences: Estonia and the Deficiency of the Audiovisual Media Services Directive." Media and Communication, 3(4), pp. 1-6. Retrieved 3 December 2020. https://pdfs.semanticscholar.org/38f6/d671542ae68441fe955389cb8fbaa612bfbb.pdf?_ga=2.141431218.1454955638.1606971130-1000744679.1606971130

[56] Ibid, p. 3.

[57] "e-Estonia." (n.d.). Wikipedia. Retrieved 4 December 2020. https://en.wikipedia.org/wiki/E-Estonia

country and to bring it in line with other digital societies.[58] Estonia rejected an offer from Finland to accept its old analogue telephone system at no cost in favor of establishing its own digital phone network.[59] After regaining independence, Estonia increased efforts to modernize and has continued to do so over the last 25 years with the aspiration to join NATO and the EU being a major step in ensuring a safe security environment.[60] As the internet became more readily available to everyday users, Estonia embraced it and has become a leading example of a technologically advanced country, often nicknamed "e-Estonia."[61] In 2000, the Estonian government declared that access to the internet was a fundamental right and freedom.[62] Many services for Estonians are fully available online, including the option to vote; this has proved popular among Estonians. In the May 2019 parliamentary elections, a quarter of all votes were cast online.[63] Near universal internet access has been highly beneficial for Estonian society. The 2007 Bronze Night events were some of the most significant challenges that Estonia has faced since regaining independence. Russian-based cyber-attacks temporarily crippled much of Estonian cyberspace, but lessons learned from that event strengthened and increased national security,[64] so much so, that NATO established its Strategic Communications Centre of Excellence in Tallinn in 2008. Despite the short-term damage that may have been inflicted by Russian and/or Russian-affiliated actors, Estonian officials were quick to portray these events not in the classic Russia-versus-Estonia narrative, but in a larger, more comprehensive security dialogue that focused on the global security environment and the challenges posed to the broader global community.[65] Transparency was a crucial factor for Estonia, which declassified much of the information about the Bronze Night cyber-attacks and shared it with analysts worldwide, showing that security in both the physical and digital realm were highly interrelated.[66] This information illuminated the threats countries can face in a highly digitized environment.[67]

---

[58] Ibid
[59] Ibid
[60] Gold, Josh. "How Estonia uses Cybersecurity to Strengthen its Position in NATO." 26 May 2019. Retrieved 26 November 2020. https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/
[61] Ibid
[62] "e-Estonia." (n.d.). Wikipedia. Retrieved 4 December 2020. https://en.wikipedia.org/wiki/E-Estonia
[63] Ibid
[64] Ibid
[65] Ibid
[66] Ibid
[67] Ibid

NATO recognized Estonia's approach to cybersecurity, and along with the governments of six other member states, established the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn.[68] Fears about outside intrusion into domestic affairs regarding the Bronze Night attacks were used not only to improve Estonian cybersecurity policy, but were also used to improve cybersecurity strategy for all NATO members**.** Before these events, NATO was not adequately prepared to respond to cyber-attacks, but steps were implemented to improve its policies, which are still in place today.[69] The Estonian experience played an integral role in NATO's cybersecurity strategies in the 2010's. The 2014-2018 National Cyber Security Strategy states that:

> "At the international level, the preservation of a free and secure cyberspace as well as Estonia's central role in guiding and developing international cyber security policy in international organizations as well as like-minded communities must be ensured."[70]

Estonia implemented its first official cybersecurity strategy in 2008, which was in effect until 2013. The second cybersecurity strategy was implemented in 2014 and was in effect until 2018 while the current strategy of 2019 made further revisions to the previous two versions and is slated to be in effect until 2022. When compared to each other, the needs and aspirations for cybersecurity do not differ significantly, and progress in areas of concern can be traced. The following facts and figures have been taken from these strategies and are intended to highlight the areas of need, where progress has been made, and where attention still needs to be focused.

There are many major challenges that Estonia faces in the 21st century digital environment. The following list includes challenges faced by the public, private, and research sectors. The current *Cybersecurity Strategy* (2019-2022) lists several problem areas, the first of which is a limited capacity for specialization. As the Estonian population continues to decline, the current group of cybersecurity professionals, although highly competent, cannot continue to provide adequate protection as the number and complexity of cyber threats continues to

[68] Gold, Josh. "How Estonia uses Cybersecurity to Strengthen its Position in NATO." 26 May 2019. Retrieved 26 November 2020. https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/
[69] Ibid
[70] Ibid

increase.[71] The first *Strategy* states the importance of the security and economic growth of the country and claims that the development of the information space and other transitional reforms led to a high living standard.[72] The widespread availability of internet throughout society has left users with a high confidence in information systems.[73] To demonstrate this point, in 2007, 98% of all bank transactions were made using online technologies and 82% of all tax declarations were submitted online, while almost all schools throughout Estonia used the internet or other e-learning technologies.[74] The document declares that:

> "Since 2008, Estonian state agencies have been obliged to follow information security standards which lay down security measures for the information systems and related information assets used in processing data in state and local government databases."[75]

Recommendations to enhance and further cybersecurity measures are outlined in the document, which include increasing security requirements for companies whose "systems are included in the Estonian critical infrastructure, without neglecting owners of other information systems."[76]Additionally, the load limit on what IT and cyber infrastructure can handle should be increased, both in the public and private sectors.[77] Adequate testing measures should also be implemented to ensure increased online traffic will not crash servers while analysts should monitor network traffic for further study.[78] A fragmented cyber sector hinders the possibility of retaining a level of top-tier professionals that may not only leave the public sector, but the country entirely.[79] The second major point of concern relates to an insufficient understanding of cyber threats and cross-dependencies. Private organizations, despite good intentions, can cause cyber risks without coming to the full realization of the broader impact of their decisions as they

---

[71] "Cybersecurity Strategy." Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia
[72] Estonia, Ministry of Defense, Cyber Security Strategy Committee. (2008). Retrieved 28 November 2020. www.enisa.europa.eu › cyber-security-strategy › file_en
[73] Ibid
[74] Ibid
[75] Estonia, Ministry of Defense, Cyber Security Strategy Committee. (2008). Retrieved 28 November 2020. www.enisa.europa.eu › cyber-security-strategy › file_en
[76] Ibid
[77] Ibid
[78] Ibid
[79] "Cybersecurity Strategy." Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

are connected to public cyber networks.[80] These actions can damage the functioning of the digital environment. The state "still lacks a systematic view of the mutual cross- and cross-border dependencies and potential impacts of systems and a clear view of ensuring the minimum level of services that should also be operational in a crisis."[81] As mentioned previously, current cyber professionals are well-versed in the technical aspect of cybersecurity, but this workforce has not translated into Estonian companies producing their own cybersecurity products.[82] A significant contributing factor to this deficiency is the a shortage of specialists, which prevents necessary growth and presence in the cyber field. A lack of resources and lack of research into areas such as cryptography contribute to a gap between what exists and what is needed in cybersecurity.[83]

Lastly, the threat to Estonian cyberspace does not necessarily come from the digital realm itself, but from the stiff competition posed by other countries who are developing and exporting their ideas and technology abroad.[84] The ability to compete on a global stage, and the requirement that cyber capabilities and competencies be increased, is imperative if Estonia wants to remain competitive and influential in the 21st digital environment.

Training a workforce that is skilled in the competencies of cybersecurity also has provided a challenge for Estonia. Even though there already exists a considerable understanding of the task at hand and competency in the existing workforce, the demand for skilled cybersecurity professionals is growing in both the public and private sectors.[85] In each of Estonia's *Cybersecurity Strategies*, the shortage of cybersecurity professionals is still considered a significant issue for Estonia. After the Bronze Night events rocked Estonia in 2007, major emphasis was placed on enhancing cybersecurity and offering training opportunities that would provide for this essential aspect of national security. At the end of that same year, there were no institutions of higher education in Estonia, public or private, that offered degree programs or detailed instruction at the Bachelor's, Master's or Doctoral levels in cyber or information

[80] Ibid
[81] Ibid
[82] Ibid
[83] Ibid
[84] Ibid
[85] Ibid

security.[86] By the time the current *Strategy* was published in 2018, "national defense studies" were being offered at 127 upper secondary schools and 22 vocational institutions.[87] The in-depth offerings and trainings in this field are still insufficient for what is necessary, but there is much optimism to be had for future years. The University of Tartu and Tallinn University of Technology have created degree programs specifically to address the lack of cybersecurity professionals, and secondary schools have begun integrating cybersecurity with courses on information science[88] in the hopes that this will spark the interest of students to pursue training or professions related to cybersecurity. In 2016, the University of Tartu created an IT law and research program that was aimed at lawyers working in the cybersecurity sector and Tallinn University of Technology launched a program for lawyers specifically centered on technology law.[89]

Another major aspect for safeguarding the cyber environment is to encourage the different sectors of society to cooperate and share resources, experts, funding, communication, and other essential components that are necessary in providing for cybersecurity. The level of awareness among medium and small enterprises is growing[90] but is still deficient for the needs of the 21st century. The relative lack of awareness among Estonians in the online realm is a point of real concern to Estonian officials, as spyware, malware, and other malicious programs could find unwitting or unknowledgeable internet users and create a security breach(s) that permeates the different sectors of Estonian society. Awareness efforts aimed at target demographics, which include private businesses, are taking place in order to increase knowledge about threats and cybersecurity issues, and to create and maintain partnerships with state institutions.[91] The

---

[86] Ibid

[87] "Cybersecurity Strategy 2019-2022." Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

[88] Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

[89] Estonia, Ministry of Defense, Cyber Security Strategy Committee. (2008). Retrieved 28 November 2020. www.enisa.europa.eu › cyber-security-strategy›file_en

[90] Ibid

[91] "Cybersecurity Strategy 2019-2022." Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

Estonian Police and Border Guard have also instituted awareness campaigns with the hope of achieving similar results.

Many of these education efforts have been focused on schools, and in increasing the awareness and competencies of mid and upper-level government professionals. Increasing the skillset of these professionals is seen as directly related to prioritizing cybersecurity throughout the Estonian government.[92] Continuing education courses and instruction in new content is being monitored, trainings are being held, and exercises conducted on cyber defense.[93] Additionally, these efforts are being implemented into training programs aimed at mid and top-level leadership in the hope that competency will prepare these officials to respond to potential crisis situations.[94]

Estonian cybersecurity law remains in a state of transition as it aims to enact statutes that are adequate for the needs of cybersecurity. Efforts to address these needs consist of expanding existing law to "avoid situations where some modes of cyber-attacks would not have been covered by law at all or where sanctions would prove insufficient to prevent or prosecute the crime."[95] An amendment was also added to existing codified law that was specifically intended to address acts of terrorism where a cyber-crime was committed for terrorist purposes.[96] The state documents *Internal Security Development Plan 2015-2020*, *Cybersecurity Strategy 2014-2017*, and the *Internal Security Development Plan 2021-2030*, which is currently being developed, are the major documents that address cybercrime.[97] The stated objectives of these documents are in:

> "…promoting capability for detection and investigation of cybercrimes that takes into account developments in ICT, ensuring readiness for future threats and challenges related to cybercrime and security; promoting domestic and international practical cooperation and information exchange between partner institutions; dissemination of information; gathering and analysis of relevant information to achieve as complete an overview of the

[92] Ibid
[93] Ibid
[94] Ibid
[95] Estonia, Ministry of Defense, Cyber Security Strategy Committee. (2008). Retrieved 28 November 2020. www.enisa.europa.eu › cyber-security-strategy › file_en
[96] Ibid
[97] "Cybersecurity Strategy 2019-2022." Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

> cybercrime situation; the combating of the sale of illegal goods and services online; analysis and mitigating of risks related to e-Residency and digital identity."[98]

For the most part, the scope of Estonian cybersecurity law is vast and outside of the purview of this thesis. The above brief explanation is intended to highlight legal statutes that exist in their relation to cyber-crime, and to provide a basic explanation of actions the state may pursue if it is determined outside actors have committed cyber terrorism or violated Estonian cybersecurity laws.

The composition of Estonia's cyber infrastructure consists of internet service providers, servers owned and operated by state institutions, Estonia's root domain, network nodes, service servers, and the firewalls of both public and private entities.[99] Successfully operating state institutions requires a vast amount of data and data storage capability.[100] Ensuring access to data, and preventing access by unauthorized parties, is a major challenge that comes with an online presence and in conducting online operations. To counter outside attempts at gaining access to information databases, Estonia created a public data-sharing service known as X-Road, which was originally established in 2001. Unlike other data service platforms, data is stored in the institutions where it is created, not in a centralized location or server.[101] A decentralized data network complicates any outside efforts to obtain data, which would require that each individual database be compromised to gain access. Data is also not duplicated within the X-Road system, allowing for the secure transfer, access, and confidentiality of data to different points in the X-Road network, which is only accessible to authorized users.[102] Another major aspect of the X-Road system is to ensure that efficiency is maintained both by the data-sharing process and by human operators.[103] This consists of automating certain processes that normally would take time and energy from human operators, freeing them to attend to tasks that require human interaction.[104] The overriding objective of the X-Road platform is to provide more efficient

---

[98] Ibid
[99] Estonia, Ministry of Defense, Cyber Security Strategy Committee. (2008). Retrieved 28 November 2020. www.enisa.europa.eu › cyber-security-strategy › file_en
[100] "X-Road Introduction (short version)" [Video file]. 2016, 10 June. Retrieved November 29, 2020. https://e-estonia.com/solutions/interoperability-services/x-road/
[101] Ibid
[102] Ibid
[103] Ibid
[104] Ibid

government services to Estonians.[105] Over 99% of government services in Estonia are available online, which include access to healthcare services, security and law enforcement, education, transportation systems and parking, and general government services. This also includes the opportunity to vote online and to access the state's Cloud server for publicly available content.[106] Every Estonian citizen receives a national digital ID, in addition to a physical ID card. This allows ID holders to access the X-Road system and acts as a verification measure for online activities, thus protecting users while they are conducting official business or using state services online.[107]

The Estonian Defense League (EDL), a state paramilitary force, has also been involved in protecting the integrity of Estonian cyberspace. The EDL Cyber Unit (CU) is tasked with aiding and maintaining security measures in both the public and private sphere. Some of the efforts that the EDL undertakes, often with the assistance of other state agencies, is in providing information security specialists with training, continuing education, and a practice environment. They also aid civilian government agencies during peacetime and offer support to these agencies during crisis periods.[108] The protection of critical cyber infrastructure is integral to the work of the EDL. EDL members are often highly proficient in computers or other traditional cyber fields and have experience in other specialties that aid in the EDL's cybersecurity mission.[109]

In efforts to rectify cyber deficiencies, the *Cybersecurity Act* will address "…evaluating and managing risks and determining responsibility at the company level."[110] Better prevention of cyber attacks and providing for the security of information systems and service providers requires that:

---

[105] Ibid

[106] "Interoperability Services." (n.d.). Retrieved 29 November 2020. https://e-estonia.com/solutions/interoperability-services/x-road/

[107] Wallace, Savannah. (2020, 25 July). "Estonia: The First Digitally Literate Country." Medium. Retrieved 4 December 2020. https://medium.com/swlh/the-first-digitally-literate-country-e9dbc1d0695

[108] "The main tasks of the EDL CU." Estonian Defense League. (2020). Retrieved 2 December 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

[109] Ibid

[110] "Cybersecurity Strategy." Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

> "…a systematic and continuous overview of the architectural security and traffic in service providers' networks and cross-dependencies and cross-border dependences. To do this, a network monitoring system will be developed, of which a working prototype exists as of the start of the strategy period, the implementation of which will be expanded to private networks and analytical capability will be increased through automating monitoring and further development of solutions."[111]

To further protect private businesses, cyber insurance services will be issued and analyzed. Traditionally, these insurance services have not been widely visible, and have seldom been available in the marketplace.[112] Unfortunately, this trend continues into the present day. When services have been available, "the complexity of insurance protection is often considered a hindrance to the development of the cyber insurance market."[113] The importance of insurance and the knowledge of what it protects against, are incentives for private enterprises to decrease vulnerabilities in the case of a potential cyber-attack.

The level of cybersecurity, and efforts to address shortfalls, have increased in Estonia since the Bronze Night attacks. The quality of countermeasures and proactive protocols have grown in scope and number,[114] with a greater understanding of the capabilities of adversaries, and the consequences that can result from being unprepared for attacks. Additionally, public awareness and understanding has increased about the role of cyber-attacks and the integral role cybersecurity plays in a country's security environment. The country is, and will continue to be, a trend-setter in the field of cybersecurity in the years to come. The knowledge gained and lessons learned from the Bronze Night events have made Estonian cybersecurity policy notable on the worldwide stage. Governments from other Western nations have taken notice of these initiatives and have sought to adapt them for their own countries. Because technology continues to advance at breakneck speed, changes to existing policies and laws will occur, and the strategies of adversaries will continue to advance as well. The problems that Estonia faces regarding cybersecurity are made less severe due to the forward-looking nature of the country,

---

[111] Ibid
[112] Ibid
[113] Ibid
[114] Pernik, Piret, & Tuohy, Emmet. (2013, August). "Cyber Space in Estonia: Greater Security, Greater Challenges." Report. Retrieved 2 December 2020, from International Centre for Defense Studies website: https://icds.ee/en/cyber-space-in-estonia-greater-security-greater-challenges/

the educational and professional opportunities that are available, and the potential talent pool of future cybersecurity professionals.[115]

The Estonian Psychological Space in the 21st Century

The psychological resilience of a society to fend off information warfare operations has become imperative for governments throughout the world in the 21st century. The opportunities that the internet and social media platforms present are nearly impossible to quantify. Nations that were once considered the standard-bearers of democracy and its associated principles have seen a dramatic decline in the trust and appreciation of these ideals. This phenomenon has been reflected in the rise of populist political movements, contempt for journalists and a free press, and in the erosion of democratic governments in favor of authoritarian leaders and policies. Estonia is fortunate to have relatively high levels of trust in government institutions and national media. This, however, does not mean that Estonians are not susceptible to psychological attempts to dissuade or disinform them, either by internal or external sources. The most visible fault line in Estonia is the ethnic and linguistic divide between Estonians and ethnic Russians. Russian information operations have often focused on exploiting this divide over the past three decades. The similarities between Estonian media policy and psychological security are many, although there are notable differences.

Security experts largely agree that an active and informed citizenry is integral to strengthening any country that is the target of information warfare operations from external actor(s). According to an official with the EDL:

> "Being very creative and flexible, motivated volunteers can achieve some tangible results in supporting the state activities in the field of defence and security. Our contribution plays a vital role in diversifying activities that minimise the harmful effects of pro-Kremlin propaganda."[116]

---

[115] "Cyber security." Estonia Ministry of Economic Affairs and Communication. 2020, 15 April. Retrieved 2 December 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

[116] Teperik, Dmitri (section author). "Estonia" (2018). Disinformation Resilience Index (Publication). p. 130. Retrieved 3 December 2020. http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf

These counterpropaganda efforts are largely undertaken by NGO's and private initiatives rather than through state actions. The state is involved with certain initiatives, namely through the Ministry of Education, which implements changes in the country's education policy. Ranking organizations such as the Open Society Institute and the Media Literacy Index have placed Estonia very highly, with the country coming in fifth out of 35 European countries in the 2018 index. This designation places Estonia above the other two Baltic states and ahead of other technologically advanced countries, such as the UK and Germany. It is in the same cluster as the Netherlands, Sweden, Finland, Denmark, and Ireland.[117] The index, "…was created in 2017 as a response to the 'post-truth' phenomenon. It aims to measure resilience to 'post-truth', 'fake-news' and their consequences in a number of European countries and offer a[n] useful instrument to finding solutions."[118] According to the European Policies Programme at the Open Society Institute Sofia, education and specified media training are the most integral elements in forming a media literate society. This organization listed Estonia as having the highest level of media literacy in its rankings.[119] Numerous initiatives have been implemented in Estonia in the last decade, all with the objective of enhancing societal resiliency and providing for a media literate population, thus ensuring the psychological aspect of national security.

The Estonian government has instituted several notable initiatives to increase media literacy and provide for psychological security against information warfare operations, which include *Estonia 2020, Sustainable Estonia 21*, and the *National Security Concept of the Republic of Estonia*.[120] *The Lifelong Learning Strategy 2020*, another of the state's forward-looking documents, relates to education policy and includes plans that incorporate a "digital focus in lifelong learning."[121] Despite the document's name, it was first implemented in 2014, and dealt with state educational funding during that period.[122] This document stated, "improvement in the digital skills of the total population has been achieved and access to the new generation of digital

---

[117] Ibid
[118] Turp-Balazs, Craig. (2018, April 3). "Estonia is Emerging Europe's Most Media Literate Country." Retrieved 4 December 2020. https://emerging-europe.com/news/estonia-emerging-europes-media-literate-country/#:~:text=A%20major%20new%20study%20by,both%20the%20UK%20and%20Germany.
[119] Ibid
[120] "Estonia: Lifelong Learning Strategy 2020, issued in 2014." (n.d.). UNESCO Institute for Lifelong Learning. Retrieved 4 December 2020. https://uil.unesco.org/document/estonia-lifelong-learning-strategy-2020-issued-2014
[121] Ibid
[122] Ibid

infrastructure is ensured."[123] While educational initiatives are incorporated into all levels of education in Estonia, including vocational and higher education, these initiatives also extend to adult and continuing education programs. This is a key feature of the *Lifelong Learning Strategy 2020*. Efforts in schools and universities include, "strategic measures for a digital focus in lifelong learning which covers incorporating a digital culture into the learning process at all levels of education and in all curricula."[124] Students will have access to "a modern digital infrastructure for learning,"[125] and will be graded on a system that tests for progress and proficiency in learning stated digital objectives.

The desire to create opportunities for lifelong learning in Estonia have been discussed since the country regained independence. Media education efforts began to take shape in the mid-1990's when some teachers "had an[d] extensive in-service training, which included in addition to the genre education also critical reading, media economy, media ethics, etc."[126] In 1996, media education was officially added to the national educational curriculum.[127] Efforts to provide computers in all Estonian schools became a reality in 1998[128] and media literacy has been a part of the curriculum since 2002.[129] Currently, media literacy courses are offered at the level of each teacher's competence.[130] There is also "no official designation or legal definition for media education in Estonia."[131] Despite this, there are several themes and guidelines that assist teachers in organizing a curriculum:

- "elements of media literacy are present in the curricula of Estonian and social sciences at all school levels (writing the news, role of media in society, safety on internet, etc.)"[132]

---

[123] Ibid
[124] Ibid
[125] Ibid
[126] Siibak, Andra, Ugur, Kadri, & Vinter, Kristi. (2014, May). "Media and Information Literacy Policies in Estonia" (Publication). p. 2. Retrieved 4 December 2020, from University of Tartu, Institute of Journalism and Communication. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/ESTONIA_2014.pdf
[127] Ibid
[128] "e-Estonia." (n.d.). Wikipedia. Retrieved 4 December 2020. https://en.wikipedia.org/wiki/E-Estonia
[129] Siibak, Andra, Ugur, Kadri, & Vinter, Kristi. (2014, May). "Media and Information Literacy Policies in Estonia" (Publication). p. 2. Retrieved 4 December 2020, from University of Tartu, Institute of Journalism and Communication. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/ESTONIA_2014.pdf
[130] Ibid
[131] Ibid, p. 3.
[132] Ibid

- "cross-curricular theme 'Information environment' combines elements of mediated and non-mediated communication, including mass media."[133]
- "In gymnasium level (school year XI) there is a mandatory course of Estonian language called "Media and its influences" – was implemented for the first time in 2012/2013"[134]

Along with this framework are further specified guidelines detailing the different types of media, such as television and film, and providing ideas on initiating discussions on mass communication and media's role in society. Courses in media literacy are not required by the Preschool Education Act but are a mandatory part of the curriculum for elementary school students and above.[135] There are efforts, however, to implement media education classes for this age group and changes that would allow for this would be made to the *National Curriculum for Pre-School Child Care Institutions.* To enhance language skills and focus on media in the Estonian language, two courses are often taught together, known colloquially as "mother tongue."[136] The language requirement consists of these two compulsory courses, one that relates to media and its influence and the second being in linguistics, "Practical Estonian II."[137] The time that is dedicated to school media education is limited, and unfortunately, there are few adequate statistics regarding this.[138]

Student competency in media education is the major objective in both the *National Curriculum for Basic Schools* and the *National Curriculum of Upper Secondary Schools*, which state that the competence is, "to read and understand information and literature; to write different types of texts, using appropriate linguistic devices and a suitable style."[139]

In addition to state-sponsored and traditional school-based initiatives, there are partnerships with private sector organizations that allow for practical applications to enhance and increase media literacy skills. One of these notable initiatives is called Media Bubble, a competition that

---

[133] Ibid
[134] Ibid
[135] Ibid, pp. 5-6.
[136] Siibak, Andra, Ugur, Kadri, & Vinter, Kristi. (2014, May). "Media and Information Literacy Policies in Estonia" (Publication). p. 6. Retrieved 4 December 2020, from University of Tartu, Institute of Journalism and Communication. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/ESTONIA_2014.pdf
[137] Ibid
[138] Ibid, p. 7.
[139] Ibid

was originally founded in 2003 by Paide Gymnasium.[140] Media Bubble is a regional organization aimed at 16 to 19-year-old students, located in central Estonia. Since 2005, the organization has brought together local schools, from both gymnasiums and vocational institutions, and the program consists of a series of tasks. These begin with three local events in three counties eventually culminating in a grand finale, in which all participating counties are represented with one team.[141] Some of the tasks that students must complete include "creating" news content, conducting interviews for a mock radio or television program, and having a knowledge of media history.[142] Media Bubble, which reinforces previously taught media education objectives, does not include a comprehensive approach to media education, as it omits topics like media economics, etc.[143]

Non-governmental organizations (NGOs) also play a significant role in securing Estonia's psychological space. Professional organizations for journalists are part of these efforts, and programs targeted towards young and aspiring journalists should also be noted. The NGO, Young People's Media Club (Estonian: Noorte Meediaklubi or NMK), focuses on young professionals who have had basic experiences with school or university publications, such as radio, television, or newspaper.[144] Originally launched in 2000, but formally incorporated as an NGO in 2003, the NMK strives to reinforce and enhance the communication and journalistic capabilities of participants. They also provide more theoretical and economics-based knowledge of media, such as media economics and even critical reading skills.[145] A series of workshops and professional events are organized by NMK throughout the year, some of which include school competitions, multimedia events, and locally targeted events throughout the year.[146] To facilitate guidance and provide feedback and instruction, University of Tartu faculty is sometimes involved. Targeting potential journalists has reaped benefits, especially when current journalism students or beginning professionals increased their competencies due to the efforts of NMK.

[140] Ibid p. 10.
[141] Ibid
[142] Ibid, pp. 10-11.
[143] Ibid, p. 11.
[144] Ibid
[145] Ibid
[146] Ibid

Many previous NMK participants have enrolled in the University of Tartu's Institute of Journalism, Communication and Information Sciences.[147]

International media education programs have been adopted by many Western countries, with varying levels of success and implementation. The EU has also been quite active with similar initiatives that are intended to promote educational, professional and cultural organizations, and activities within its member states. The media literacy program "Media Literacy-21 Century Approach to Education" was implemented for a two-year cycle (2010-2012) and was intended to increase school literacy rates and interest in local events within both Estonia and Latvia. Much like the MNK program for aspiring and young communications professionals, media experts assisted in enhancing media education programs in regions of the two countries. Practical exercises were part of the program as were efforts to increase young people's awareness and interest in media.[148]

Efforts aimed at the broader society include private and/or NGO organizations that aim to discredit Russian information warfare efforts by providing fact-checking analysis. One of the most notable efforts in this regard is Propastop, a volunteer-run, independent blog that aims to "clean[ing] Estonia from propaganda, false information and media lie."[149] According to Propastop, the site does not create propaganda, but only aims to counter false narratives.[150] This occurs whenever Propastop bloggers, many of whom are members of the Estonian Defense League,[151] detect content that may be false, biased, or malicious against Estonia. Content that is brought to the attention of Propastop officials is addressed through the blog and brought to public attention.[152] The majority of the time and effort of Propastop officials is focused primarily on Russian-based and/or Kremlin-friendly narratives. The organization also pledges to shed light on, and counter, any other misleading content concerning Estonia. Propastop uses fact-checking and content analysis when it acts as an information mediator. They also provide detailed

---

[147] Ibid, pp. 11-12.
[148] Siibak, Andra, Ugur, Kadri, & Vinter, Kristi. (2014, May). "Media and Information Literacy Policies in Estonia" (Publication). p. 12. Retrieved 4 December 2020, from University of Tartu, Institute of Journalism and Communication. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/ESTONIA_2014.pdf
[149] "What is Propastop?" Propastop.org. (2017). Retrieved 7 December 2020. https://www.propastop.org/eng/2017/03/06/what-is-propastop/
[150] Ibid
[151] Ibid
[152] Ibid

explanations, give background information on specified events, and bring attention to the actions of what neighboring countries are doing to counter false or misleading narratives. Information related to discussions and blog posts from state agencies, media organizations, and literature are additional ways that Propastop engages readers to combat hostile information operations.

The efforts made by the Estonian government, the private sector, academic institutions, NGOs, and private individuals have increased the security environment in Estonia and have provided the requisite skills for state and society to diminish the impact of Russian information warfare operations. The challenges that face Estonia in the 21st century are many and will only continue in future years. Providing for cybersecurity and educating professionals that are competently trained for the workforce will remain a weakness for both the public and private sector. New training programs for career state employees, a greater understanding of the threat and the capabilities posed by Russia, and the possibilities granted to Estonians by the X-Road system are integral steps to ensure a protected cybersecurity environment. The ethnic and linguistic divide that exists between Estonians and ethnic Russians is still a major fracture point that Russia takes advantage of to harm the Estonian state. A linguistically segregated media environment demonstrates that efforts are needed to ensure that the information space and media policy is in line with serving all aspects and demographics of Estonian society, a fact that has worked against homogenizing the populous. Recent media initiatives, such as the launch of ETV+ in 2015 are showing promise, particularly during the coronavirus pandemic, when local news and information is essential to saving lives. The knowledge and experience of the Bronze Night events, coupled with Russia's annexation of Crimea and actions in Eastern Ukraine, spurred Estonia into enacting new initiatives and strengthening older ones. This attempted to make up for deficiencies in the country's information and media policies, while continuing to further safeguard cyberspace. The combination of these factors will allow Estonia a greater chance to thrive in the ever-changing and uncertain era that has marked the 21st century.

Estonia summary

As the most technologically advanced of the Baltic states, Estonia's actions to secure its cyberspace have been recognized internationally and its media literacy efforts aimed at school-aged students have encouraged those interested in a career in media to enroll in journalism

schools. Estonia-based Russian language media has proven increasingly effective in informing Russophiles about critical events during the coronavirus pandemic that Russia-based media does not. Though there is much room for improvement in its security environment, Estonia has managed to maintain a greater level of political stability and public trust in media and institutions than what is currently experienced in many European and Western countries. Additionally, the desire to contribute to both the European and international communities have allowed for a greater emphasis on research and development, and to make Estonia a desirable country for foreign business and investment, which has most notably manifested itself in its e-residency program. The promotion of democratic norms and practices as well as transparency in government has led to a stronger state and a more trusting and engaged society.

CHAPTER 2

Latvia

Background

After regaining independence on 21 August 1991, Latvia established itself as a Western-style, unitary parliamentary form of government,[153] one that ensures that all Latvians are free to live and exercise their beliefs openly without fear of repercussion or repression. The country's information, cyber, and psychological spaces have seen a dramatic improvement in the past three decades but continues to face significant challenges that prevent it from fully continuing the trajectory into a more free, open, and socially integrated society. Many of Latvia's difficulties relate to its demographic composition and interference by its sizeable eastern neighbor. This experience with a hostile and adversarial Russia shares many similarities with its northern Baltic neighbor, although there have also been marked differences between the two as well. Also, in

[153] "Latvia." (n.d.). Wikipedia. Retrieved 9 December 2020. https://en.wikipedia.org/wiki/Latvia

similarity to Estonia, linguistic, education, and media policy have contributed to the hinderance of societal integration, even though there have been notable improvements and liberalizing reforms to the most controversial of these policies.

The Latvian information space is regarded by observers as free and open, a guarantee that is enshrined in the Latvian constitution. This fundamental right is stated under the constitution, Chapter VIII, articles 99 and 100, which declare that:

"99. Everyone has the right to freedom of thought, conscience and religion. The church shall be separate from the State.

100. Everyone has the right to freedom of expression, which includes the right to freely receive, keep and distribute information and to express his or her views. Censorship is prohibited."[154]

The Latvian Information Space in the 21st Century

The NGO Reporters without Borders ranks Latvia at 22nd in their 2020 list of 180 countries.[155] This listing places the country below Estonia (ranked at 14th) and above Lithuania (ranked at 28th)[156]. This most recent listing is a slight improvement in the rankings with Latvia moving up two places from the 2019 survey. Even with this improvement, it should be noted that the diversity of the Latvian media landscape, while still diverse, has been on the decline in recent years. The dramatic increase in online news portals has captured the audience of many of these publications. Some publications have ceased to exist, others have had to lay off or eliminate staff. In 2019, new owners of LNT, the oldest and largest commercial television channel with the largest news operation, made the decision to shut down the newsroom and laid off 30 employees.[157] Criticism soon followed. The closing of the newsroom raised fears about what this decision means for Latvia, and what the outlook may be for other news outlets in coming years. The Latvian Association of Journalists was especially critical of this decision, calling it the "worst media-related decision of the decade."[158] Other notable events in the Latvian media

[154] "The Constitution of the Republic of Latvia" (n.d.) Republic of Latvia. Retrieved 9 December 2020. https://www.president.lv/en/republic-of-Latvia/the-constitution-of-the-republic-of-latvia#gsc.tab=0
[155] "Latvia." (n.d.) Reporters without Borders. Retrieved 9 December 2020. https://rsf.org/en/latvia
[156] Ibid
[157] Ibid
[158] Ibid

environment include the removal of nine Russian TV channels due to their owner being, "subject to EU sanctions for undermining the territorial integrity of Ukraine."[159] In addition to the many challenges facing news operations in the West in the 21st century, trust in a free and independent press is also declining in Latvia. Journalists have routinely been the recipients of insults and verbal abuse while politicians have been keen to attack and take legal action against them, especially during periods that are close to elections.[160] Structural reforms and the requisite political will to enact or enhance laws that would improve the media sector have too often met with a less than enthusiastic reception and have often become stuck in parliament, sometimes for years.[161] Other major issues facing the Latvian media sector are primarily political in nature. State authorities, who hold the power to appoint nominees to the National Electronic Mass Media Council (NEPLP), the state media regulation body, seem to hold little interest in appointing competent people to the governing body, and the country's public broadcaster suffers woefully from a lack of funding.[162] Even though press freedom is constitutionally protected, there sometimes is interference from both the public and private sectors.

Although the media has suffered a noticeable decline in political support, courts often rule in favor of journalists when lawsuits are filed against them. There are well documented instances of the politically connected interfering in the affairs of reporters and media organizations. One of these instances occurred in 2018 when the NEPLP suddenly fired the chairperson of Latvian Television, a public television broadcaster, along with an LT board member.[163] The dismissal was controversial and the Latvian Association of Journalists asked that an official investigation be conducted, which ultimately ended with the chairman of the NEPLP resigning in 2019.[164]

Latvia's media environment can be characterized as a hybrid system because it "lacks a dominant paradigm."[165] Though the media environment is in line with those in Western

---

[159] Ibid
[160] Ibid
[161] Ibid
[162] Ibid
[163] "Latvia." (n.d.). Reporters without Borders. Retrieved 9 December 2020. https://rsf.org/en/latvia
[164] Ibid
[165] Rožukalne, Anda., Stakle, Alnis., & Skulte, Ilva. (2020). "Media education in the common interest: Public perceptions of media literacy policy in Latvia." *Central European Journal of Communication, 13*(2). p. 210. Retrieved 20 December 2020. https://cejc.ptks.pl/Volume-13-No-2-26-Special-Issue-2020/Media-education-in-thecommon-interest-Public-perceptions-of-media-literacy-policy-in-Lat

democracies, there are three distinctive journalism cultures that are discernable, all of which compete with one another. The first consists of Russian language media, which falls in line with Russian journalism culture.[166] The second is representative of a post-Soviet environment but one that is not truly independent of the political and economic demands made upon it.[167] The third is the environment that most observers would associate with a democratic government, one that is set towards high standards, editorial independence. and a professional media environment.[168] Of the three cultures, the last two are the most discernable. Russian language media transmitted from Russia and its online content has a noticeable influence inside Latvia. Providing adequate securitization measures can prove difficult with competing media cultures, especially when they contrast significantly from each other. The differences in standards and professional ethics allows for a less secure environment as dubious information sources are bound to find their way to an audience.

Major Latvian media policy documents, such as the *National Strategy of Electronic Media Development 2012-2017* do not address media content that is targeted to ethnic minority audiences.[169] Nationalistic politicians have traditionally desired that integration be a foremost priority of the state, and media outlets have taken a similar approach. The closest that the strategy comes to mentioning minority language are for calls to strengthen the Latgalian dialect, in addition to public broadcasting services.[170] Furthermore, the desire to create a "Latvian" information space throughout the country is clearly indicated, but no mention is made of the Russian language or its role in Latvian society. An emphasis is placed on increasing the prevalence of public broadcasters in border regions, granting broadcasting licenses based on a media organization's reputation as well as that of its owner(s), state authorization of media outlets that produce content primarily in the Latvian language, and measures that provide for continued national security.[171] Several notable efforts have been undertaken to further protect Latvia from Russia since 2014. The state has taken the lead in these efforts, which have included

---

[166] Ibid
[167] Ibid
[168] Ibid, p. 211.
[169] Rožukalne, Anda. (2016). "All the Necessary Information is Provided by Russia's Channels. Russian-language Radio and TV in Latvia: Audiences and Content." Baltic Screen Media Review, 4, p. 111. Retrieved 14 December 2020. https://content.sciendo.com/configurable/contentpage/journals$002fbsmr$002f4$002f1$002farticlep106.xml
[170] Ibid, p. 112.
[171] Ibid

revising media policy and adding amendments to the Latvian constitution. These efforts, which were submitted to parliament by then-president Raimonds Vējonis, aimed "to expedite both government and military decision-making in case of conflict."[172] Non-traditional concepts of security were also added to the definition of "wartime" in the National Security Law which are, "…described as being a consequence of any attack, be it conventional (military) or not, or any other actions aimed against the country's independence, constitutional order or territorial integrity."[173]

Integration efforts have been a regular aspect of security discussions in the post-Soviet era. The desires of politicians in the 1990s were often based in security rhetoric. The objectives were to protect and advance security measures in all aspects of Latvian society, therefore protecting the ethnic majority while clinging to the belief that the ethnic Russian community would integrate into Latvian society and adequately learn the language. After nearly thirty years of independence, these desires have been minimally realized. For the most part, Russophiles continue to live largely in the Russian sphere, speaking Russian either regularly or exclusively, and consuming media in that language. According to the *Latvian National Security Concept*, it is necessary to "…develop and offer a high quality and understandable alternative to the information sources representing the information space of the Russian Federation, thus providing various options to choose from."[174]

Radio and television broadcasts are the most common and popular forms of media in Latvia. The continuing popularity of these mediums has carried over from the Soviet era, when radio and television outlets were perceived by the public as providing the most realistic and accurate content that best reflected the political and social trends. Though state censorship is generally not problematic, political interference and the composition of the media sector raise concerns about the security of the country's information space. Russian language broadcast media is disproportionately large in comparison to the market size, a trend that applies to both

---

[172] Fernandes, Sandra. (2018). "(Re)securitisation in Europe: The Baltic States and Russia." *Debater a Europa.* p. 117. Retrieved 17 December 2020. https://www.researchgate.net/publication/322690589_Resecuritisation_in_Europe_the_Baltic_States_and_Russia

[173] Ibid, p. 118

[174] "Cyber Security Strategy of Latvia 2014-2018." (2014). Government of the Republic of Latvia. p. 5. Retrieved 17 December 2020. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

radio and television outlets. The term "asymmetry" is used regarding the "entrenchment" of Russian channels, which also include public broadcasting channels in Russian as well.[175]

For the most part, commercial media has had limited interest in providing Russian language programming, which became the responsibility of public channels such as Latvian Radio 4, United Latvian Public Media, LTV7.[176] Competing with Russian-based outlets for the Russophile audience has proved to be an uphill battle, as the production quality, resources, and funding of the Russian-based media are significantly greater than those of Latvian-based media. Ratings numbers have repeatedly indicated that viewership for Latvian Russian language media is small in comparison to the audiences that their Russian counterparts draw. Trust in Russian-based channels remains high among Russophiles, a concerning trend for Latvian political and media officials.

The dual nature of the information space has major security implications, which will likely continue in the coming years. Countermeasures and efforts to lessen the Russian influence have largely been unimplemented for a variety of reasons. Protecting Latvia's information space is highly dependent on the desires of the political realm, which has continually proved to be a major hinderance to increase funding for Russian language public broadcasting services and providing support for further development of Latvian Television and Latvian Radio.[177] Because of these primarily political debates, the existing Latvian information environment is still susceptible to Russian messaging and influence. The continuing political controversies also hinder the economic conditions that allow for the development of Latvian-based minority language media. In line with the initial Estonian approach, relying largely on the market to provide opportunities is not sufficient for maintaining the security of this space. Economics has played a major factor in the shuttering or consolidation of media organizations, a trend that has only accelerated in the 21st century. Currently, Latvia's media sector in highly concentrated, a trend that is only likely to continue in future years. This trend inhibits competition, thus

---

[175] Kudors, Andis. (chapter author). (2018). "Latvia." In *Disinformation Reilience Index* (p. 174). Retrieved 13 December 2020. http://prismua.org/en/dri/

[176] Rožukalne, Anda. (2016). "All the Necessary Information is Provided by Russia's Channels. Russian-language Radio and TV in Latvia: Audiences and Content." Baltic Screen Media Review, vol. 4, p. 109. Retrieved 14 December 2020. https://content.sciendo.com/configurable/contentpage/journals$002fbsmr$002f4$002f1$002farticlep106.xml

[177] Ločmele, Klinta. (n.d.). "Overview." medialandscapes.org. Retrieved 10 December 2020. https://medialandscapes.org/country/latvia

weakening the security of the information space. Competition is an integral part of the Western, Anglo-Saxon media model, but conditions must be favorable for media opportunities to present themselves. The economic health of market economies does not guarantee that there will be increased growth in the media sector, or that opportunities will manifest themselves for minority language media. When these factors are coupled together, the growth and vibrancy of media will be limited. Regional media outlets may have even less opportunity for growth due to limited advertising revenues.

The events of 2014 spurred discussions throughout Latvia regarding what efforts should be considered or implemented to further safeguard Latvian television, as well as the national media environment. Proposals to launch a dedicated, full-time Russian language channel were floated, but ultimately rejected by a political coalition, especially by members of nationalistic parties.[178] Arguments against the creation of a dedicated channel centered primarily on integration, with nationalistic politicians claiming that increased broadcast content in Russian would disincentivize Russophiles from learning Latvian and would "legitimise Latvia as a bicommunal state."[179] In-depth studies have been conducted to gauge public opinion regarding this issue. A mix of different opinions was documented, which ranged from strongly supporting the creation of a dedicated Russian language channel, to supporting the improvement of existing Russian language channels, to opposition to a new channel. Concerns centered on the possibility of biased information entering the information sphere if a new channel were to be launched, citing the close relationships between high-ranking politicians and media owners.[180] Yet others claim that existing channels provide a diversity of coverage that is adequate for Latvia's needs.[181] After much debate, the decision was ultimately made to invest in existing channels, LR4 and LTV's Russian language division. Despite increased funding and Russian language content, viewership figures continue to lag behind their Russian-based counterparts.

Latvia's television broadcasters are highly concentrated in their ownership. The asymmetric information space has, or does, consist of Russian language channels like Pervy Kanal, RTR Planeta, RT, PBK, First Channel, and REN TV Baltija, which have enjoyed

[178] "Changes in Latvian Media Policy following Russia's Actions in Ukraine." [E-mail interview with Baltic Centre of Media Excellence Director Janis Siksnis]. (2020, 13 December).
[179] Ibid
[180] "Changes in Latvian Media Policy following Russia's Actions in Ukraine." [E-mail interview with Baltic Centre of Media Excellence Director Janis Siksnis]. (2020, 13 December).
[181] Ibid

consistently high viewership. They are the most popular channels with Russophiles, even with the emergence of social media and other electronic media platforms that propagate Kremlin-friendly narratives and anti-Latvian themes. These channels are either partly or wholly owned by Russians.[182] Investigations conducted by Latvian security services and communications researchers indicate that the information environment is being utilized by Russia to spread spurious information. These channels represent some of the most common ways Russia has engaged in information warfare in Latvia. The transmission model that is used to transmit Russian-based channels in Latvia has often proved a major opportunity for information operations. These channels are provided by representatives of Russian television broadcasters, comprised of Russian and Latvian businesspeople working with Russian media outlets. Authorizations are granted by media organizations for retransmission and local Latvian advertising is sold that airs on these channels that are broadcast within the country. Because of this, official monitoring efforts can only be partly undertaken to ensure that programming complies with Latvian broadcast standards. The large amount of programming that is broadcast daily, let alone over a prolonged period, allows for significant quantities of dubious information to enter the Latvian information space. Even with the current ban of several major Russian channels, there are still several channels that continue to disseminate disinformation and propaganda on a regular basis. Because of political ramifications, restricting further Russian television programming is not likely, nor would it be popular. One of the inherent weaknesses with democratic systems is the difficulty of restricting information. Besides the constitutional protections, public sentiment very often oppose state content restriction efforts, however well-intentioned they may be. Latvia will probably always have this vulnerability in its information space, and Russia will continue to exploit opportunities to broadcast their narratives to Latvian Russophiles.

Much of the self-made content found in the Latvian information space is not of high quality. A major criticism of citizen journalism centers on having laypersons engaging in the work of journalists, whether they intend to label themselves as journalists or not. A segment of the online space contains content that has not been properly vetted or researched but is nonetheless published for an audience. Digitally published content is more often consumed by

[182] Ločmele, Klinta. (n.d.). "Television." medialandscapes.org. Retrieved 10 December 2020. https://medialandscapes.org/country/latvia/media/television

younger audiences than traditional sources of media. Those who are more media literate seek out reputable news sites for information. A destabilizing trend in the past decade is the rise of "fake news" websites. Despite the commonalities that these sites have in disseminating content that is either partly or wholly untrue, their objectives can often vary quite drastically. In Latvia, the most common reasons include websites and social media sites whose primary motivation is to profit off dubious content. Content creators may or may not have a political stance that they aim to advance, but instead seek to create content that is popular and attracts an audience. Though each visit to one of these sites often only earns a small fraction of a Euro cent, publishing content where it will potentially be consumed by thousands or millions can make these sites highly profitable. The other major category in the "fake news" phenomenon is content creators who seek primarily to publish dubious information. They work independently or in association with other organizations and creators to advance ideological objectives, or to simply flood the information space with false or misleading information that confuses or weakens the resolve of an audience to determine if the content is factually accurate. Because of Latvia's shared history and proximity to Russia and its demographic composition, this category of fake news is highly prevalent in the country's information space, especially online. Facebook has been a major platform for false information that circulates and finds a receptive audience. The coronavirus pandemic has caused much concern among Latvian journalists because thousands of false stories are being shared by users worldwide. The Re:Baltica journalism research center has documented an extremely high number of these stories floating around online.[183] Because of the widespread practice of sharing dubious information on Facebook, confusion and skepticism have characterized the Latvian information space. In the week of 13-19 December 2020 alone, 12,000 Facebook users shared false information claiming "that COVID-19 tests were invalid because they allegedly showed positive results in lemonade."[184] Increased attention and scrutiny has been focused on media literacy and media education programs during the pandemic, specifically for these reasons. According to Evita Purina of Re:Baltica, the sharing of these false sources of information indicates a public distrust in government and the media, but also that media literacy is not appropriately valued in the Latvian education system.[185] The Ministry of Culture states that

[183] Kupčs, Edgars. (2020, 18 December). "Pandemic shows serious shortcomings in Latvian media literacy." Retrieved 19 December 2020. https://eng.lsm.lv/article/features/media-literacy/pandemic-shows-serious-shortcomings-inlatvian-media-literacy.a385822/
[184] Ibid
[185] Ibid

Latvian society has a high level of trust in social media, a trend that is only continuing to grow.[186]

Information protection measures have included temporary bans on certain Russian channels, which have included the Russian channels RTR (for three months in 2014) and RT, RT HD, RT Arabic, RT Spanish, RT Documentary HD, RT, and RT Documentary TV (for an unspecified period beginning in 2020 and continuing until owner Dmitry Kiselyov is removed from the EU sanctions list). Earlier safeguarding measures also included the shuttering of the Russian TV channel Sputnik in March 2016, with the Latvian Ministry of Foreign Affairs stating that this channel was simply a mouthpiece for disseminating the Kremlin's narratives about its actions in Ukraine, among other topics.[187] Further restrictive state efforts were soon taken up when the Latvia National Electronic Mass Media Council ordered a six-month long ban on Russian channel Rossiya RTR, citing similar reasons that were stated with Sputnik's ban.[188]

Russia has harshly criticized Latvia for these actions, claiming they are based in Russophobia and not in reality. Although Russia and some outside observers considered these actions undemocratic, Latvia considered them a necessary security measure. While protecting freedom of speech and expression, the Latvian constitution prohibits the "incitement to racial or ethnic hatred," which are treated as crimes.[189] Latvian language channels include LTV1, LTV7, Riga TV24, and Kanāls 2, and others that include local and regional channels. The composition of this market is comprised of just three companies- MTG, BMA, and Latvian Public Television- each of which own several channels.[190] Commercial stations TV3, LNT, TV6, and TV3+ also offer news and entertainment programming but are owned by a single owner.[191] The majority of viewership is primarily comprised of ethnic Latvians.

---

[186] Ibid

[187] Fernandes, Sandra. (2018). "(Re)securitisation in Europe: The Baltic States and Russia." *Debater a Europa.* p. 117. Retrieved 17 December 2020.

[188] Ibid

[189] "2018 Country Reports on Human Rights Practices: Latvia." (2018). United States Department of State. Retrieved December 2020. https://www.state.gov/reports/2018-country-reports-on-human-rights-practices/latvia/

[190] Rožukalne, Anda. (2016). "All the Necessary Information is Provided by Russia's Channels. Russian-language Radio and TV in Latvia: Audiences and Content." Baltic Screen Media Review, vol. 4, p. 112. Retrieved 14 December 2020. https://content.sciendo.com/configurable/contentpage/journals$002fbsmr$002f4$002f1$002farticlep106.xml

[191] Kudors, Andis. (chapter author). (2018). "Latvia." In *Disinformation Reilience Index* (p. 176). Retrieved 13 December 2020. http://prismua.org/en/dri/

The environment that Latvian radio broadcasters operate under is somewhat more secure and competitive than its television counterparts. Stations are conforming to the preferences of listeners and are making the older medium more technologically advanced by establishing or increasing their online presences. Many smartphones now include apps that include a built-in radio receiver that can receive traditional over-the-air radio signals. While technology is advancing and traditional radio receivers are declining in use and popularity, listenership remains relatively stable. Most people listen to privately owned outlets, but public radio also enjoys a respectable listenership. Notable efforts for the protection of the radio waves were implemented by radio broadcasters after Russia's annexation of Crimea. Legislative efforts were undertaken in response to these events in Ukraine to provide for further information security. In late 2014, amendments were added to the *Law on Electronic Media (LEM).* These mandated that radio stations broadcasting at least half of their content time in a minority language cease doing so and only broadcast in Latvian, beginning on 1 January 2016.[192] These actions did not come without controversy. Concern was focused on how the new linguistic requirements might impact Russian language media and there was a desire to avoid any significant changes or disruptions to these outlets.[193] To moderate the amendments and avoid major programming changes, parliament relegated programming decisions to the individual radio stations that broadcasted half of their content in other languages. The stations could decide what language they would broadcast, in the beginning of 2016.[194] Later protective measures were also enacted in that same year, which mandated that stations broadcast at least 90% of their content with locally or self-produced media.[195] The objective of this regulation was to bolster Latvian-based content while significantly curtailing the amount of foreign or outside media "that has the potential of disseminating propaganda."[196] Efforts have been focused on providing coverage to the Latgale region of Latvia in order to establish a more intensive presence in the region, and to provide content for all Radio Latvia stations nationwide that originates from there.[197] The eastern regions of Latvia host a high percentage of ethnic Russians, who have easy access to radio stations

[192] Ločmele, Klinta. (n.d.). "Radio." medialandscapes.org. Retrieved 10 December 2020. https://medialandscapes.org/country/latvia
[193] Ibid
[194] Ločmele, Klinta. (n.d.). "Radio." Retrieved 10 December 2020.
[195] Ločmele, Klinta. (n.d.). "Overview." Retrieved 10 December 2020.
[196] Ibid
[197] Ločmele, Klinta. (n.d.). "Radio." Retrieved 16 December 2020.

located within Russia. A new facility was opened in Rēzekne in 2016 and was financed with public funds allocated by the Saeima.[198]

Latvian print media publications have not been as popular and influential as broadcast media has been in the 21st century. In line with global trends, the number of publications in both Latvian and Russian has declined significantly and continues to do so. In the period from 2007 to 2013, newspaper circulation declined by 60%, with Latvian language publications suffering a 47% decline.[199] Daily papers have suffered the biggest losses in readership during this period. Many newspapers and magazines have ceased publication altogether in the last two decades, though certain magazines have experienced a noted increase in interest and readership. Publications that once had sizeable circulations have made up some of the difference with an enhanced online presence, though this does not replace lost advertising revenues from physical publications. Declines have been noted across both age and demographic spectrums as older readers are increasingly abandoning print media. The reasons for this are not well understood, but the cost of subscriptions, which are approximately 100 Euros annually, likely plays a role.[200] Unlike electronic and broadcast media, there have been no major efforts, state or otherwise, to safeguard the print environment. Information warfare efforts, which once found a haven in print media, have largely migrated to digital sources. Russian language print media is highly diverse and covers most of the same issues as Latvian language publications.[201] The Russian language print market is much more volatile than the Latvian language print market.[202] Major factors for this include the fact that most Russian publications are local and lack outside investment from the West,[203] a luxury many Latvian publications have. Audience sizes also tend to be smaller than their Latvian counterparts as well. Generally, Latvian authorities have not attached a major security risk to print media. The 21st century has been somewhat defined not only by technological advancements that have built upon or changed existing technologies, but also by how new digital platforms have transformed communication at all levels of society. The launch of social media platforms has shifted how relationships are developed, but also how warfare operations, disinformation, and media are consumed and disseminated. Social media networks

[198] Ibid
[199] Locmele, Klinta. (n.d.). “Print.” Retrieved 16 December 2020.
[200] Ibid
[201] Ibid
[202] Ibid
[203] Ibid

such as Facebook, Twitter, Vkontakte (the Russian version of Facebook), and countless others have come under intense criticism for policies deemed too lenient on those who disseminate hate speech, disinformation, and misinformation. The online space is unlike traditional forms of media in its vast expanse. Opportunities for hostile information and cyber warfare operations are many, and the ability to hold hostile forces accountable is limited.

Approximately 70% of Latvians use the internet daily, mostly to check social media websites. The local social media platform draugiem.lv is popular among Latvians, making Latvia the only European country where Facebook is not the most popular social media network. On Draugiem, like other social media platforms, hackers and hostile actors have used the site to spread disinformation, and they even hacked the site's main page during the 2018 Latvian parliamentary elections. Users that logged on the site saw the Russian flag, Russian president Vladimir Putin, and images of the Russian army. In addition, Russian text, stating, "Latvian comrades, this is for you. Russia's borders are boundless. Russian world can and needs to unite everyone who values Russian culture no matter where they live – in Russia or outside its borders. We recommend using the phrase 'Russian world' more often" was posted temporarily.[204] The site was returned to normal after a few hours. The capabilities of hostile actors have been consistently visible and a valid concern for many Latvians, leading to questions about how much of users' activity is being monitored by outside actors and those with malicious intentions. No significant state actions have occurred in the online space, though it is closely monitored for possible information warfare efforts and trends that regularly occur in this space.

The advent of an internet environment began in Latvia in the late 1990s and continued into the first years of the 21st century. The websites TVnet.lv and Apollo.lv were the first two sites that premiered in Latvia. From a security risk perspective, opportunities began from the earliest days of these portals for igniting controversy and fanning the flames of division and hatred. Both portals allowed users to anonymously comment and debate on news articles. Since this time, TVnet.lv and Apollo.lv have only grown in popularity and remain at the top of the rankings for the number of hits.[205] In the first years of the new millennium, print publications

[204] Rožukalne, Anda. (n.d.). "Media Audience Development in Latvia (2004-2012)." *Media Transformations*. p. 153. Retrieved 17 December 2020.
[205] Ločmele, Klinta. (n.d.). "Digital media." medialandscapes.org. Retrieved 17 December 2020. https://medialandscapes.org/country/latvia/media/digital-media

began to publish their content online.[206] Some publications made only some of their content available online while other outlets began fully publishing online. The trend towards having a multimedia environment soon caught on with traditional media organizations, which has become commonplace in the modern era. However, most Latvian newspapers only have their print materials available for online consumption.[207] By 2015, internet usage had increased across several digital technologies and was more accessible for users. Figures indicated that the number of users who accessed the internet on cell or smartphones had increased by 46% and on tablets by 39%.[208]

Media organizations have a sizeable presence online and are well-visited by internet users. The preferences of users differ greatly. The current online Latvian media environment shows that independent news organizations are more popular than the websites of more traditional media sources (radio, television, newspaper, etc.). Many of these independent sources have grown in popularity and in resources and can compete with the news operations of traditional media outlets.[209] Sites such as Delfi.lv and Tvnet.lv are examples of well-visited independent sources. The online media environment has grown in professionalism as well as in originality, benefitting media consumers. Online portals, which were once seen as areas where traditionally produced content could be copied for an online audience, have not shifted to creating original content specifically for online platforms.[210] In the online environment, which often provides a platform for dubious information to reach mass audiences, outlets such as the previously mentioned can provide a check for internet users wishing to consume content that has been subjected to the same standards and practices that traditional sources have.

The Latvian Cyber Space in the 21st Century

For the last two decades, Latvia has increasingly become a digitized, online society, with all demographic groups using e-technologies regularly, conducting private and business activities over cyber networks in addition to requesting state services electronically. At the close of the

[206] Ibid
[207] Ibid
[208] Ibid
[209] Ločmele, Klinta. (n.d.). "Digital media." medialandscapes.org. Retrieved 17 December 2020. https://medialandscapes.org/country/latvia/media/digital-media
[210] Ibid

20th century, digital technologies had begun the "digital revolution" that was transforming the developed world. Coordinated efforts to develop an information society began in Latvia in 1999 with the adoption of the national program *"*Informatics,*"* approved by the Cabinet of Ministers.[211] This program spanned the years 1999-2005, when further cyber documents were enacted. In the last fifteen years, five major policy documents or planning strategies have come into effect in Latvia. Some of these strategies, though not necessarily citing cyber security as a major aspect of their focus, do contain provisions that can be interpreted as protective measures. In October 2005, *The Concept of the Electronic Procurement System* was approved by the government, which aimed for the completion of a public procurement system expediting public purchases, along with reducing corruption and bureaucracy.[212] In 2006, the *Information Society Development Guidelines for 2006 – 2013* was implemented. Its objectives were to ensure all Latvian citizens and businesses would be able to use public services and ICT technologies. Other major goals that were outlined were to improve public sector efficiency, reduce administrative costs, and comply with the EU's Lisbon Strategy and the broader European technology initiative i2010.[213] In 2007, the *National Development Plan for 2007-2011* was approved, which focused on improving sustainable development, increasing Latvia's competitiveness, and raising living standards.[214] The *e-Government Development Plan for 2010-2013,* based upon the *National Development Plan 2007-2013* centered almost exclusively on the accessibility of e-services, sought to strengthen state policy, and enhance the state's regulatory agencies.[215] These include e-services such as e-Identification, e-Procurement, e-Invoice, e-Justice, e-Health in addition to social security and mobility services while following the EU's Digital Agenda for Europe strategy.[216] The *National Development plan for 2014-2020* stresses medium term development planning, which comprises part of the overarching *Latvia 2030* development plan. These sustainable development initiatives are intended to address public ICT programs concerning digital content, e-skills, e-services, and infrastructure. [217]

---

[211] "WSIS+10: Overall Review of the Implementation of the WSIS Outcome: WSIS 10 Year Country Report by LATVIA." (Report). (2014). p. 5. Retrieved 17 December 2020, from World Summit on the Information Society website: http://www.itu.int/net/wsis/review/inc/docs/rcreports/WSIS10_Country_Reporting-LVA.pdf
[212] Ibid
[213] Ibid
[214] Ibid
[215] Ibid
[216] Ibid
[217] Ibid pp. 5-6.

The United Nations (UN) recognized the benefits and necessity of having widespread internet access and hosted the World Summit on the Information Society (WSIS) in 2003. This was the first of a two-phase summit; the second phase began in 2005. The major objective was to close the digital gap between rich and poor countries by providing internet access opportunities and technical assistance to developing nations. Latvia has participated in WSIS processes since the program's inception in 2003 and drafted and has applied the program's principles outlined at the first meeting.[218] Many of the implemented initiatives have not been based in security rhetoric, but in developmental, professional advancement, educational, and economic language instead.

From 2006 to 2013, state agencies and private citizens increased their capabilities, experience with, and utilization of the internet. Knowledge gained during this period has been applied to future national cybersecurity documents. Important lessons include:

- providing opportunities for all users to benefit from the technologies and possibilities offered by ICT[219]
- enhancing the quality of life for Latvians while increasing the knowledge-based economy and the country's competitiveness [220]
- increasing economic growth and job creation[221]

These objectives were the driving force in the document, *Information Society Development Guidelines 2006-2013*, Latvia's first major cyber strategy document. These stated goals were included to introduce:

> "information society initiatives in Latvia and the initiatives related to achievement of the goals set in the National Development Plan 2007 - 2013 in the field of information society, and especially regarding skills, technologies, services, innovation, research and business activity."[222]

[218] Ibid
[219] Latvia, Ministry of Environmental Protection and Regional Development. (2013). "Information Society Development Guidelines 2014-2020." pp. 15-16. Retrieved 17 December 2020.
[220] Ibid, p. 15.
[221] Ibid
[222] Ibid, p. 95.

These initiatives were intended to correct the deficiencies that Latvia faced in its cyber environment, which in 2006, "considerably lagged behind the EU in terms of the number of Internet users (2 times less), use of ICT in business activity (2.3 times less), use of e-services (7-10 times less), as well as in terms of e-commerce turnover (16 times less)." [223] Innovation in cyber technology in both the research and business sectors was quite low as well. There were problems with both the technical and educational aspects of cyber implementation. The relative lack of an adequate cyber infrastructure and the limited awareness or understanding of cyber technologies hampered digitization efforts in all aspects of Latvian society. Many state services were not provided online, nor did many businesses have a presence there.[224] Also, there was limited funding for digital innovation and entrepreneurial endeavors, skill acquisition, and business opportunities outside of Latvia.[225]

Geopolitical changes and Russia's actions, especially the annexation of Crimea and support for separatists in the Donbas, have injected security measures into Latvian cyber policies and planning documents. The *Cyber Security Strategy of Latvia 2014-2018* and its latest adaptation, the *Cyber Security Strategy of Latvia for 2019-2022*, specifically stress the importance of cybersecurity and protective measures that will defend the viability of the country's digital services and infrastructure. As stated in the 2014-2018 document, "The aim of the cyber security policy is a secure and reliable cyber space, which ensures a safe, reliable, and continuous supply of services essential for the state and society."[226] This policy consists of four major objectives that aim to achieve these goals:

- Development: states that the best way to protect against constantly increasing threats in cyber space is to continually develop and improve competencies in the ICT sector and associated fields[227]
- Cooperation: states that the only effective defense against threats from domestic and foreign actors is by cooperation at the national and international levels[228]

[223] Ibid
[224] Ibid, p. 96.
[225] Ibid

[226] "Cyber Security Strategy of Latvia 2014-2018." (2014). Government of the Republic of Latvia. p. 3. Retrieved 17 December 2020. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss
[227] Ibid
[228] Ibid

- Responsibility: states that all segments and demographics within society need to be informed and to understand how their actions, or lack thereof, can impact their own security and the security of others[229]
- Openness: states that cybersecurity policy needs to be implemented in accordance with all applicable laws and constitutional structures to respect the rights and freedoms of individuals and businesses, while striving to promote professional ethics, practices, and norms in cyber space[230]

According to this strategy, Latvian cyber space has had many incidences of security issues, ranging in severity from low to high. Though not all cyber threats pose great danger to Latvia, the current geopolitical situation causes significant concern to security officials. The chaotic political nature of many countries throughout Europe, in addition to an increasingly authoritarian, opportunistic, and unpredictable Russia, indicates that the number of cyberthreats will continue to rise in the foreseeable future. Latvian cybersecurity is divided into three distinct dimensions: infrastructure, services, and processes.[231] A semi-centralized structure is currently used for implementation of these strategies. Respective state agencies enforce the responsibilities, methodologies, and coordination of the policy, which is overseen by supervisors with specialized knowledge of the policy guidelines and the technical specifications required for cybersecurity demands.

While the semi-centralized model is beneficial to the state's role in cybersecurity, cooperation is essential for the security of Latvia's entire cyber infrastructure. In line with codified law, the Council is the governing body responsible for developing cyber policy and the methodologies, planning, and implementation of these initiatives.[232] Operated by the National Cyber Security Policy Coordination Section of the Ministry of Defense, both public and private entities cooperate with the Council. They receive information and other essential guidance in carrying out policy objectives dictated by it. The approach to cybersecurity is a government-wide and society-wide effort and includes the Ministries of Defense, Foreign Affairs, and Interior. It

[229] Ibid
[230] Ibid
[231] Ibid, p. 5.
[232] Ibid

also includes the Ministry of Justice, Education, Science, and the Information Technology Security Incident Response Institution (CERT.lv).[233]

The role of CERT.lv is important in Latvia's cybersecurity efforts because it is specifically tasked with promoting information security law. Throughout the organization's twenty-year existence, the number of cyberwarfare and hostile digital efforts have increased exponentially. In 2019, the number of monthly documented threats to unique IP addresses averaged from 100,000 to 105,000. These threats include malware, fraud, and intrusion efforts, among others.[234] CERT.lv also documented 132 cases of hacked or defaced websites throughout Latvia in 2019 as well, some of which were hacked countless times throughout the year. Hackers used several types of operating systems to carry out the attacks.[235] The most commonly documented methodologies utilized by attackers were Denial of Service (DoS and DDoS), phishing and data scams, intrusion attempts, malware, and compromised devices.[236] In addition to these documented instances, CERT.lv received multiple reports of cyber-attack efforts aimed at the digital devices of government organizations and local municipalities.[237] Because of the vastness of cyberspace and the digital infrastructure even in one country, CERT.lv encourages state and private sector organizations to contact the unit to report cyber-attack efforts, whether they are successful or not. After these attempts, CERT.lv initiated technical security measures that prevented further attacks from impacting other public agencies and institutions.

CERT.lv offers penetration tests that seek to find whether online sources such as websites, databases, or other online systems are vulnerable to cyberattacks. Tests are normally conducted for sites or organizations that have a national profile. Many tests indicated that there were significant deficiencies and problem areas that needed to be addressed.[238] CERT.lv analyzes test results and drafts reports to these organizations that detail problem areas and makes recommendations to secure these online resources. Many vulnerabilities are centered on the use of outdated content management systems, which expose sites to automated cyberattacks; cross-

[233] Ibid, pp. 5-6.
[234] "2019: CERT.LV Public Performance Report." (Report). (2020). p. 10. Retrieved 18 December 2020, from Information Technologies Security Incident Response Institution website: https://cert.lv/uploads/parskati/certgada-atskaite-2019-EN.pdf
[235] Ibid, p. 16.
[236] Ibid, pp. 18-21.
[237] Ibid, p. 24.
[238] Ibid, p. 26.

site scripting issues, which expose sites to increased risk of receiving information; and lack of correct resource configuration, which allows attackers to obtain information regarding technological solutions, causing increased traffic load on the cyber infrastructure.[239]

In addition to providing technical assistance and diagnostic testing, CERT.lv also conducts educational and communication events throughout the year. These include communication with media organizations regarding research findings, bringing public attention to major cybersecurity issues and initiatives which are intended to secure the digital realm, and organizing educational events targeted to IT professionals to enhance existing skills and teach new ones. In addition to the cyber workforce, events are available for government employees, students, and even the general public.[240] These educational and professional events educate thousands of people each year during hundreds of regularly organized classes.

As is stated in state cybersecurity documents, cooperation with other state agencies and international organizations remains an integral aspect in providing for a secure cyber environment. CERT.lv regularly cooperates with officials from the European Parliament and the National Guards Cyber Defense Unit. In the event of a major cyber threat or crisis, CERT.lv and the Cyber Defense Unit would have a major role in providing support to those affected by cyber-attacks in the public and private sectors.[241] The Cyber Defense Unit solicits the expertise of private sector cybersecurity professionals, who volunteer their time to increase their competencies at the national and international levels. In efforts to broaden and intellectualize the agency, the Cyber Defense Unit encourages all IT and cyber professionals to apply to the organization.[242] In a similar vein, CERT.lv continues to cooperate with other security organizations such as the Security Expert Groups (SEG). Since 2012, SEG has allowed for the transfer of ideas between the cyber community and the public and private sectors. Those who wish to join the organization must be recommended by at two existing SEG members before they are formally allowed membership.[243]

---

[239] Ibid
[240] "2019: CERT.LV Public Performance Report." (Report). (2020). p. 32. Retrieved 18 December 2020, from Information Technologies Security Incident Response Institution website: https://cert.lv/uploads/parskati/certgada-atskaite-2019-EN.pdf
[241] Ibid, pp. 42-43.
[242] Ibid, p. 43.
[243] Ibid

The resources, depth of expertise, and influence of supra-national security organizations also play a significant role in Latvia's cybersecurity. Both NATO and the EU have cybersecurity units that provide further resources and assistance to member states. Latvia is a signatory to the Budapest Convention on Cybercrime and also joined the Protocol to the Convention on Cybercrime, which concerns the criminalization of racist and xenophobic acts perpetuated through digital means.[244] NATO has taken initiatives to increase its cyber defense capabilities and has reaffirmed that cyberwarfare shall be identified and defended against just as the alliance would respond to traditional kinetic military actions.[245] Though Latvia is not referred to specifically in NATO's cyber defense language, the fact that it is a member of the alliance is reassuring, given the vastness, technological capabilities, and financial expenditure that is required to adequately provide for cybersecurity. At a NATO summit in Warsaw, allied nations pledged to make the improvement and security of digital infrastructure and national networks a significant priority for the alliance.[246] Multi-national cooperation among allied nations and the public and private sectors of each member state is a stated practice, in order to provide for the free flow of best practices and technical assistance. Cyber defense constitutes one of the major areas of cooperation between NATO and the EU in their efforts to counter hybrid warfare. Training, exercises, and research are several of the cooperative efforts undertaken by this partnership.

The Latvian Psychological Space in the 21st Century

Much like its northern neighbor, the similarities that Latvia shares with Estonia are many, especially regarding actions to defend the country's psychological space from Russian information operations. As previously mentioned, Latvia's dual information space is one of the most noticeable and exploitable fissures within their society. Efforts to secure this space have not been sufficient and came only after Russian media influence was well established among the Russophile community. Information and psychological security have been major initiatives since 2014, but significant gaps continue to exist in adequately securing these spaces. Political debates

[244] "Latvia: Cybercrime policies/strategies." (2020). Council of Europe. Retrieved 18 December 2020. https:www.coe.int/en/web/octopus/country-wiki-ap/-/asset publisher/CmDb7M4RGb4Z/content/latvia
[245] "Cyber defense." (2020). NATO. Retrieved 18 December 2020. https://www.nato.int/cps/en/natohq/topics_78170.htm
[246] Ibid

often hinder proposed security initiatives, and the psychological space is no exception. In the Latvian policy document *Mass Media Policy Guidelines: 2016-2020,* media literacy is defined as the capability for, "audience[s] to use mass media, search for and analyze information, and critically evaluate the messages of mass media to promote communicative integration of the society."[247] Russia's actions in Ukraine in 2014 and in the United States' presidential election in 2016 acted as major catalysts and new policy proposals were developed to provide better security measures for this environment. The term "media literacy", despite its common usage, and the alleged appropriateness of this "response" to counter Russian information operations, still lacks a solid and consistent definition. Media education efforts were first introduced in Latvia in 1997 with the project "Informatization system of schools in Latvia", but successive programs have been met with ever dwindling funding levels since that time.[248] The demands of the digital age require that new perspectives and technologies be applied to future media education programs, supplementing or replacing existing ones. This came about in 2007 when a new initiative was implemented that was intended to cover a wide variety of educational institutions.

The National Electronic Media Council is tasked with promoting media literacy under the Electronic media law and defines media literacy as:

> "a capacity to understand and use mass media critically, evaluating their aspects and the communicated content, as well as the skills of forming communication on one's own both by commenting the contents and by participating in the formation of contents thus developing an understanding that enables effectively and convincingly to use mass media. If formerly the main attention was paid how to create media contents now the attention must be also paid to how the media contents should be used."[249]

Additionally, the term "information literacy" is part of the state's media education vernacular, and is defined as:

- "the skills to search and find information, as well as to turn it into knowledge – the

[247] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 7. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-
[248] Ibid, p. 4.
[249] Ibid, p. 5.

capacity of transforming knowledge into a newly created value" [250]

- "the skills to find, evaluate, process, apply and synthesize information by orienting oneself among the immense number of information resources and information processing tools"[251]

- The desired learning objectives encompass both technical and soft skills, which include: the ability to utilize electronic resources in addition to printed texts and images[252]
- the ability to comprehend the format, location and methodologies of access[253]

- the ability to comprehend the role of information in society, how it is structured and generated, in addition to the processes of academic publication[254]
- the ability to comprehend and use research technologies to find and perform research[255]
- the ability to create textual, visual, and multimedia publications detailing the finding of research efforts[256]

Further professional and educational events are outlined in "The Basic positions of the policy of national identity, civic society and integration for the years of 2012–2018," including media education events for adults and for educators, which began in 2013.[257] Objectives are aimed at improving the resiliency and psychological integrity of the population through soft power initiatives.

Media education initiatives in Latvia are not normally independent projects centered around a theoretical or educational perspective, but instead are heavily subject to national strategies and programs that focus more on the technological aspects of development. Latvia's first implemented program, "Informatics", largely took this approach, though there was a

[250] Ibid, p. 7.
[251] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 7. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-
[252] Ibid
[253] Ibid
[254] Ibid
[255] Ibid
[256] Ibid
[257] Ibid, p. 8.

dedicated section that focused specifically on non-technological education.[258] Successive developments in media education policy eventually formed the basis of the next media strategy document. This new strategy, *Information and communication technologies to ensure education quality for 2007– 2013* was implemented a year after the European Regional Development Fund (ERDF) began efforts to complete the mission to connect Latvian schools to the internet. It had four major components: the development of teaching resources, ensuring a proficiency in media education for teachers, updating and maintaining existing ICT infrastructure, and the creation of an education information system.[259] For a nation that did not make the same efforts or place as great an emphasis on technological advancement as Estonia, Latvia has made the transition to digitizing much of its society and making internet access a universal technology. These efforts have achieved positive results and have even exceeded some European standards but have lagged in others. One of the notable deficiencies is the number of computers per capita.[260]

While there is consensus as to the importance of defensive measures in these areas, limited scholarship has been conducted into the qualitative aspect of media and its role in the development of democracy in Latvia.[261] Scholarship that has centered on media education has often consisted of analysis of the quantitative and technical aspect instead.[262] Media education efforts alone are insufficient to prepare society to critically analyze media content. The status of media in Latvia also contributes to the difficulties in protecting the information and psychological spaces. It is essential that the health, vitality, and freedom of the press be foundational principles of a democratic society. Many of these principles have been threatened in the past several decades, or have been subjected to democratic backsliding, and Latvia is no exception. In the case of many post-Soviet countries, the transition into the functioning, Western democratic mold has been a long and arduous process. Many of these nations are still not fully embracing and experiencing these results. The shift to the Western, Anglo-Saxon media model has also been accomplished more fully in some countries than in others. Latvia, although having made notable improvements in domestic media publications as well as in inviting high-quality

[258] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 8. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-
[259] Ibid, p. 5.
[260] Ibid, p. 4.
[261] Ibid
[262] Ibid

foreign media to its landscape, has faced many setbacks in previous years. These include diminishing public trust, economic constriction, media consolidation, and a two-sphere information space. All these factors greatly impact media education efforts, which have suffered because of these deficiencies. The development of media education in Latvia is complicated by the cultural, media, and information spaces.[263] Societal attitudes also dictate and limit the opportunities for critical public debate while media critique is not sufficiently developed.[264] Media education needs to analyze quality journalism, which unfortunately, is not at a sufficiently high standard for public and academic analysis, though there are exceptions. Public broadcasting, which is normally considered a high point in national media, is severely underfunded. It is often found itself at odds with the will of politicians, who have not generally been sympathetic to the needs of journalists or in the need to provide quality journalism. In July 2019, the board of Latvian Radio published an open letter that addressed a lack of funding and asked that 100,000 Euros be allocated for 2019 and nearly 1 million Euros for 2020 in a desperate attempt to maintain the standards for quality journalism[265]. The letter also states:

> "If adequate resources for producing content and broadcasts at Latvian Radio aren't provided very soon, the security of the Latvian informative space will decrease substantially along with the chance for the public to obtain independent, professional and objective information about events in the country and the world." [266]

The information and psychological spaces are faced with major problems going forward as promises for additional funding have gone unmet and journalists have left the organization to take up employment elsewhere due to low wages and overwork. The European Broadcasting Association ranks Latvia at the very bottom of their rankings of EU member states for public expenditures for public media. Compared to the country's Baltic neighbors, spending is 30-45% lower than in Estonia or Lithuania and consists of 0.1% of GDP, while the European average is approximately 0.17%.[267] As mentioned previously, economic constraints have caused many

---

[263] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 4. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-

[264] Ibid, p. 5.

[265] "Crisis announced at Latvian Radio due to funding shortage." (2019, 15 July). Public broadcasting of Latvia. Retrieved 19 December 2020. https://eng.lsm.lv/article/society/society/crisis-announced-at-latvian-radio-due-tofunding-shortage.a325668/

[266] Ibid

[267] Ibid

publications to cease operations while others have had to reduce staff, publication frequency, the quality of content, or cut back on reporting coverage in efforts to save money. In addition to these factors and the lack of quality journalism, media resources are limited and of little benefit in providing adequate analysis of media, format shifts, and industry practices.[268] Generally, media outlets are minimally involved in media education initiatives beyond offering professional support to non-media organizations. Latvia's professional journalists' organizations are notably weak and are primarily focused on the needs of their professional community, not of mass media consumers.[269]

Media education efforts are also stifled by how media literacy is defined in legal terms. Competing ideas also exist as to what media literacy entails. These ideas do not complement each other and are sometimes used interchangeably, leading to possible confusion.[270] Media policy does not include stipulations that would provide for promotional efforts. Existing legislation is often outdated, which sometimes conflicts with EU guidelines.[271] Major efforts to update laws and regulations have largely been met with an unenthusiastic response from politicians, who often hold negative views of media.

Technology education is taught in Latvia beginning in primary school and continues throughout secondary school. "Information sciences" consists of education in computer and internet usage, internet browsing, finding information for research topics, and the preparation of presentation materials.[272] Unfortunately, critical analysis skills and the evaluation of media sources are not taught as part of the curriculum. The topics that comprise Latvia's media education courses are not taught throughout a student's academic career; some of the topics in the media education curriculum, in the region and throughout Europe, are not taught in Latvia. Supranational initiatives, like ones funded by the EU, have only been partially implemented or have not been adopted in the school curriculum, despite criticism from state officials. There remains a disconnect between the political sphere and state agencies, especially

---

[268] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 5. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-Excellence.-A-Case-Study-on-Media-Literacy-as-a-Tool-Against-Russian-Disinformation-.pdf

[269] Ibid, p. 26.

[270] Ibid

[271] Ibid, pp. 9-10.

[272] Ibid, p. 10.

the Ministry of Culture, which has criticized the lack of adequate media education programs in Latvia:

> "Such a notion as "media literacy" does not appear in the school programmes at all. They contain something about the use of information technologies but that is more to do with technologies and not with the critical or analytical thinking. It is worthwhile including it into social sciences;" "[media literacy] is not to be introduced immediately within one system. It is a complex issue [..] in the context of a study subject, or in the context of world news when something specific happens [..] But in order to effectively teach it, the teachers must understand how media work. And this is not about one teacher of information technologies, the approach must be more integrated."[273]

Since 2017, concerns have been increasing throughout society regarding the skills that are necessary to distinguish factual information from false or misleading information. Surveys indicate that Latvians do not feel competent in this matter and nearly 30% of survey respondents claimed they had a "negative media experience" when they realized they had believed information that was later proved to be false.[274] Other studies and surveys have indicated that the level of confidence Latvians have in their digital skills is lower than European averages. The "Information society development basic guidelines for 2014–2020" notes that "e-skills indicators among the population of Latvia are influenced by the lack of understanding and motivation on necessity of acquiring e-skills and also by emotional barriers of individuals to use the ICT tools consistently." [275]

In 2013, a survey of Latvian schoolchildren indicated that they were highly confident about their internet skills, but answers to more detailed questions showed that their confidence about specific digital competencies was less positive. Of these responses, approximately 60% of

---

[273] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 11. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-Excellence.-A-Case-Study-on-Media-Literacy-as-a-Tool-Against-Russian-Disinformation-.pdf

[274] Ibid

[275] Ibid, p.12.

children stated they could perform basic internet browser functions, such as bookmarking a website; almost 57% claimed they could compare two websites and determine if the information presented was factual; and approximately one third claimed they could change filter preferences.[276] The same survey also showed that children's knowledge of internet safety was limited (72.1%), parental knowledge of children's internet activity was low (20.9%), and that they sometimes get help from teachers (less than 64%).[277] When secondary school students were surveyed, results showed that they primarily obtained media and technology skills on their own, from friends, or from classmates, and not from formal media education programs. [278]

In efforts to make up for the wide instructional gap in media education, and to better secure this area, Latvian colleges and universities have begun offering academic programs for teachers in a variety of fields concerning media education. The University of Latvia offers a bachelor's degree program that combines psychology, algorithms and programming, mathematics, and the basics of system theories. It also contains communication theory and media studies coursework that gives future teachers a comprehensive base of knowledge that can be implemented into media literacy programs.[279] The university also offers courses that provide for deeper study into the work of libraries and research institutions,[280] and communication courses are offered with specific focuses on media education and analysis. The Department of Communication Studies at the University of Latvia has committed to researching the media use habits of children, and published the survey cited previously in cooperation with the EU Network project.[281] Scholarship in this area is limited and requires that more studies, surveys, and

[276] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 12. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-Excellence.-A-Case-Study-on-Media-Literacy-as-a-Tool-Against-Russian-Disinformation-.pdf
[277] Ibid
[278] Ibid, p. 13.
[279] Ibid, p. 14.
[280] Ibid
[281] Ibid

qualitative and quantitative data be obtained to create better media literacy programs for younger students.

A lack of resources is a major hinderance for teachers and students. Though nearly all Latvian schools are connected to the internet, the age and quality of electronic equipment varies. In some areas of the country, internet speed is too slow.[282] Electronic equipment shortages in schools prevent students from adequately completing and participating in lessons, both in and out of the classroom. Up to 40% of students stated that there is limited access to computers during lessons and that wireless internet is only accessible in certain areas of schools.[283] Additionally, 20% of students stated that they had no access to the internet at all.[284] These two reasons were cited as the biggest factors for electronic technologies being insufficiently used in schools. The national budget for school media education is not sufficient to cover all the technological requirements and improve internet speed, let alone provide media education opportunities to university students or the general public. Media education programs rely significantly on monies allocated by the EU, NGOs, private sector organizations, and philanthropic initiatives. Organizations such as the Latvian Internet Association, the Latvian National Library, and even international philanthropic efforts such as the Bill and Melinda Gates Foundation and Microsoft Latvia, have provided funding, technical assistance, and continuing education courses to working professionals, Latvian schools, universities, and the general public[285]. Private enterprises, private sector organizations, universities, and the state cooperate to further media education. In the last two decades, a major percentage of funding and other forms of assistance has come from these organizations and their organized efforts, which will continue to be the organizational model in the coming years. The EU Structural Funds framework alone sponsors over 30 projects for teachers, some of which are wholly funded by or receive generous resources from these initiatives.[286]

---

[282] Ibid, p. 17.
[283] Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). p. 17. Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-Excellence.-A-Case-Study-on-Media-Literacy-as-a-Tool-Against-Russian-Disinformation-.pdf
[284] Ibid
[285] Ibid, pp. 21-24.
[286] Ibid, p. 15.

Library organizations offer classes and resources that promote critical reading skills and instructs teachers how to use resources efficiently and effectively, but the major focus of their efforts is primarily on printed materials rather than digital literacy.[287]

Latvia Summary

Much like its northern neighbor, Latvia has faced many of the same challenges as Estonia, especially regarding its two competing spheres of influence. The ethnic Russian population is the largest in the Baltic states, which continues to cause concern among Latvian officials as to the influence Russia continues to exert over this demographic. Trust in media and institutions is low and public broadcasters are woefully underfunded. Additionally, competing media cultures and media consolidation have impacted the quality of media content, though there is hope that increasing public broadcasting coverage to the eastern border regions and to areas beyond will increase the knowledge of events happening nationwide. Cyber response teams such as CERT.lv have proven beneficial in providing for cybersecurity for both the public and private sectors, though the cyber infrastructure is not as advanced as Estonia. Media education rarely focuses on media content analysis or criticism and is highly centered on teaching the technical skills of digital technologies instead. Despite these deficiencies, a greater knowledge of the threats facing the Latvian state and increased cooperation with its neighbors in the region are hopeful signs that additional resources, expertise, and funding will be able to bridge these gaps.

[287] Ibid, p. 24.

CHAPTER 3

Lithuania

Background

As the first Baltic state to declare independence from the Soviet Union, Lithuania has become a successful example of the transition from Soviet republic to Western democracy. Throughout the last two decades, Lithuania has gained membership in the EU and NATO, both of which were major aspirations since the early 1990s.

The demographic situation in Lithuania differs notably from Latvia and Estonia in that the percentage of ethnic minorities is considerably lower. Those of Slavic background, (Russians, Belarussians, and Ukrainians), as well as Poles, constitute approximately 10%-12% of the Lithuanian population. The Polish minority population predominates in Vilnius and Salcininkai while ethnic Russians are concentrated in Visaginas. Lithuania's post-Soviet citizenship policy also differed significantly from Latvia and Estonia, as citizenship was offered to all who resided within the country. Approximately 90% of ethnic minorities chose to accept

this offer.[288] Even with these ethnic differences, the security threats posed by Russia are many and are regularly included in security policy. Information warfare operations have been commonly documented in Lithuania for many years and have only increased in number and technological sophistication. Russian pressures throughout the post-Soviet era have made the shift from hard power threats to cyber attacks and information campaigns[289] in the 21st century, though economic pressures continue to remain a significant concern. These issues compound problems for security efforts, allowing for the possibility of future information operations to further target society and destabilize institutions. Official political and state-issued statements echo the constitutional guarantees for the protection and vitality of the media sector, which have developed and adopted Western norms and professional practices.

The Lithuanian Constitution protects the:

"(3) Freedom to express convictions, as well as to obtain and disseminate information, may not be restricted in any way other than as established by law, when it is necessary for the safeguard of the health, honor and dignity, private life, or morals of a person, or for the protection of constitutional order.
(4) Freedom to express convictions or impart information shall be incompatible with criminal actions - the instigation of national, racial, religious, or social hatred, violence, or discrimination, the dissemination of slander, or misinformation."[290]

However, recent legislative and administrative efforts were made that would limit press freedom and have led to fears of state censorship, greatly concerning journalists. In line with trends experienced in the other Baltic states, as well as in the general Western media landscape, media ownership is becoming further consolidated. Many outlets have had to reduce staff, merge with other media organizations to maximize resources, or close altogether. The print sector has suffered the most, with countless publications closing due to increased economic constraints. The relatively small media market, by European standards, contributes to the difficulties currently facing the sector. In addition to the consolidation trend, many media outlets are financially

[288] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index*. p. 190. Retrieved 24 December 2020. http://prismua.org/en/dri/
[289] In-depth interview with Nerijus Malikevicius [Online interview]. (2020, 25 July).
[290] "Lithuania Constitution." (n.d.). International Constitutional Law Project (ICL) Project. Retrieved 25 December 2020. https://www.servat.unibe.ch/icl/lh00000_.html

dependent on investors or business interests, which may compromise professional standards and influence reporting.[291]

In line with the development of the media sectors in Latvia and Estonia, Lithuania was eager to abandon the Soviet era and embrace the ideals of Western democracy, in addition to its institutions, norms, practices, economic policies, and media environment. Due largely in part to the composition of the country's Soviet-era economy, which was largely agricultural and needed less foreign workers than industries in Latvia and Estonia, Lithuania's demographic composition remained far more homogenous than its Baltic counterparts. Unlike its Baltic neighbors, Lithuania offered a liberalized citizenship policy that did not exacerbate societal tensions along ethnic and linguistic lines. This helped in integration efforts and allowed minority populations to become "Lithuanian" and have the benefits of citizenship. Media opportunities favored ethnic Lithuanians, a trend that continues into the present day. Polish and Russian language publications are the most common foreign language media and are found in many parts of the country, though their presence is more concentrated in certain regions. English has become an emergent language with some online portals offering news in English. LRT, the country's lone public broadcaster, provides English language news on their website and on social media platforms that reach audiences both within and outside of Lithuania. While LRT is obligated to provide media programming in minority languages, only a small amount is produced compared to content provided in Lithuanian. Grants from the Nordic Council of Ministers' Office in Estonia are seeking to fill this gap by providing funding that aims to "increase quality and attractiveness of local, regional and national media and media products in the Baltic countries, with a special focus on inclusive content that addresses the needs and demands of communities in ethnically diverse or distinct regions."[292] These grants are being offered in all three Baltic states. Though not necessarily considered an information security measure, a security perspective can be applied to these measures, ensuring that ethnic and linguistic minorities do not drift further into competing information spheres.

---

[291] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index*. p. 191. Retrieved 25 December 2020. http://prismua.org/en/dri/

[292] "Baltic Media Grant." (n.d.). Nordic Council of Ministers' Office in Estonia. Retrieved 26 December 2020. https://www.norden.ee/en/about-us/funding/support-for-increased-quality-of-media-content-and-strengthening-of-minority-language-media-production-in-estonia-latvia-and-lithuania

Lithuania's media environment developed without many of the partisan divides that formed the information spaces of many Western European countries. Though the levels of public trust have declined in the country's media providers, Lithuania has benefitted from the lack of animosity regarding the clear left-right divisions of the political spectrum.[293] Division is found regularly in political discussions, though it does not often go beyond the political arena. To outside observers, a less partisan media atmosphere would seem to be a positive benefit to society, though the political divisions and volatility of Lithuania's political system leads to personalization. Political parties and coalitions are often constructed along personality lines, and the focus on temporary issues, often populist in nature, are not beneficial for long-term stability.[294] The media sector being mostly commercial, has often been accused of providing an inaccurate view of Lithuanian society, which "bypasses the period of media dependence on political leanings."[295] Competition between public media and private outlets to provide popular content is less than in the past. This competition can be positive for the audience, but has the effect of public versus private in an effort to "control" the other.[296] The state may seek to control the amount of political advertising that is allowed by private media outlets, while these outlets may focus on political corruption or other state issues, giving them an advantage against the state.[297] Competition requires that conditions be right to fund programming, invest in new media opportunities, and buy or consolidate with, other media organizations. The decrease in the level of funding for public broadcasting makes being competitive more difficult, often struggling to produce quality media content.

---

[293] Balcytiene, Aukse (chapter author). (2012). "Culture as a Guide in Theoretical Explorations of Baltic Media" in "Comparing Media Systems Beyond the Western World." New York, NY: Cambridge University Press. pp. 60-61. Retrieved 29 December 2020. https://d1wqtxts1xzle7.cloudfront.net/56763719/Daniel_C._Hallin__Paolo_Mancini-Comparing_Media_Systems_Beyond_the_Western_World-Cambridge_University_Press_2011.pdf?1528576150=&response-content-disposition=inline%3B+filename%3DDaniel_C_Hallin_Paolo_Mancini_Comparing.pdf&Expires=1609300553&Signature=cfA0hNbsYXZBIaqzDNeHbgFbxYexZzcytSAvzQQRHI6SqPHZZ0Pe5EJAi6PdMrjQ6mFykgfvyo61VKyV-dh41UTfmF78iHfz~OnHLzuJ~zyUE0krQUfw1GHOexfrf1RA-gSMsvAl~JbJaSbjGY9syA6KL2oTaT9TEFAksHxZFgDGj4sgFrH6qQCMpOphr0TyC7ucNuyeCrN5NyXNP~SUaa6UC5mlERPxSAWlmMw7ugevp5WHOkbLBXW3mpIBmdzMyTdIPlJOm0r4juFewuE8zWbKqsApfeVjJ2vu7hf0KkTxcx83kaBYPuQmHXwJEK1F6VrDvEgOggwzf89nzHdsFQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=62

[294] Ibid, p. 61.

[295] Ibid

[296] Ibid, p. 64.

[297] Ibid

Though its governing institutions are in accord with European norms and its media environment characterized as free, public trust in media and institutions is in decline. Like its Baltic neighbors, there are two informational spheres of influence within Lithuania, though they are somewhat less pronounced than in Latvia or Estonia. The national minority population has declined from its peak shortly after Lithuanian independence, as has the Lithuanian population in general. A major problem in the security realm is the lack of minority language media opportunities and the anti-Baltic information that is disseminated by Russia-based media, which have long portrayed Lithuania as a failed state, often using the country's net emigration as "proof." Though the Russophile minority is less than half what it is in Latvia and Estonia, Russian television channels are watched by a sizeable non-Slavic audience in Lithuania. Though some of these viewers are not necessarily in the Russian sphere, or believe everything that is broadcast on these channels, their enduring popularity remains problematic and is a symptom of a larger media environment problem. Many of these viewers watch for the entertainment and production values that Baltic-based media lack.[298]

The NGO Reporters Without Borders ranks Lithuania 28th out of 180 countries in their latest listing (2019), which represents its highest ranking from the organization to date. In addition to this ranking, the understanding of the Russian information threat has increased in recent years. The most significant changes began after Russia's annexation of Crimea and support of separatists in eastern Ukraine, which greatly alarmed the Baltic states and captured Western attention. Even before these events, the media environment was already in decline and had been for the better part of a decade. The first decade and a half of independence (1990-2004) was characterized by the successful transition to the Western, Anglo-Saxon media model and the relatively high trust that Lithuanians had in the free press. During this era, the media acted as the Fourth Estate and enjoyed the highest level of public trust among any institutions, which surpassed that of the Catholic Church, the army, and all state agencies.[299] Journalists were highly regarded and seen as advocates for the public interest while fear of bad publicity kept public officials such as politicians and judges from accepting bribes.[300] However, the media

[298] "Media of Lithuania." (n.d.). truelithuania.com. Retrieved 27 December 2020. http://www.truelithuania.com/media-of-lithuania-1664
[299] Ibid
[300] Ibid

environment began to change in the mid-2000s when media consolidation became more prevalent among private-sector outlets. Partisanship was more common, and advertisers began to have undue influence in media coverage, resulting in dramatically reduced levels of public confidence. In the last 15 years, public sentiment has changed little as the media is still generally viewed negatively by many Lithuanians. Despite these trends, this does not necessarily indicate that Russia-based media or other minority language outlets, are gaining significant influence among society. It is beneficial for Russia that a general feeling of skepticism remains, which aids in their objective to destabilize the Baltic states.

Lithuania's relationship with Russia, in the post-Soviet era, has been one of complexity, and much of the past three decades has been dedicated to implementing protective measures in efforts to mitigate Russia's hostile actions. The understanding of Russian intentions and methodologies has increased in the post-Soviet era, even more than when it was a former Soviet republic or part of the Russian Empire. Throughout the 1990s, Russia's internal and economic struggles prevented any significant foreign interference efforts from being completely effective, though Russia did not cease from using them. Hopes that Russia would Westernize and become "predictable" by Western standards existed through much of this era and into the first few years of Vladimir Putin's presidency. These hopes were soon dashed in the mid-2000s when Putin significantly altered Russia's trajectory and took a strong turn toward authoritarianism. Additionally, "gracious" overtures that Russia made to woo the Baltics back into Russia's sphere of influence were abandoned in favor of an openly hostile and antagonistic approach, after the Baltics declared their long-desired intention to join the EU and NATO. Since this time, security measures were necessary against an ever-increasing authoritarian and unpredictable eastern neighbor.

Security in general has become one of the most common topics in Lithuania after the events in Ukraine in 2014.[301] There have been three distinct phases of national security development, each focusing on different aspects of the security environment.[302] The first of these

[301] Denisenko, Viktor. (2019, 11 June). "Regional and national security discourse in the local Russian media in Lithuania." International Centre for Ethnic and Linguistic Diversity Studies. Retrieved 28 December 2020. https://www.icelds.org/2019/06/11/regional-and-national-security-discourse-in-the-local-russian-media-in-lithuania/

[302] Bankauskaitė, Dalia. (2020, 27 February). "Lithuanian Total Defense." Center for European Policy Analysis (CEPA). Retrieved 28 December 2020. https://cepa.org/lithuanian-total-defense/

phases involved increased attention to hybrid warfare, which largely took place in the immediate aftermath of the annexation of Crimea and support for separatist movements in the Donbas (approximately 2014-2015).[303] As fears of Russian information operations were at the forefront of the security consciousness, the threat of possible Russian kinetic military operations gave extra emphasis to both the information component of hybrid warfare and to the prevalence of the term itself. The second phase concerned the physical security of the Suwalki corridor, a vulnerable chokepoint for NATO defense efforts.[304] By 2018, attention had once again shifted, this time to the concept of "total defense", which was reflected in legislative action from the Seimas. The third of these discernable phases, was the resulting implementation of *Lithuanian Defense Policy Guidelines* for the years of 2020 through 2030, which is intended to ensure the strengthening of national defense capabilities in all aspects of society.[305] Psychological security has also been regularly discussed as another defensive measure for society in general. The close connections that Lithuania has with Swedish policy makers has provided for increased dialogue and analysis of this form of security. Though any efforts have yet to be implemented, the serious consideration of this proposal signals that Lithuanian policy makers believe that currently, Lithuania is not adequately prepared to handle future, more sophisticated Russian warfare efforts.

The Lithuanian Information Space in the 21st Century

The 21st century has brought a new dimension to the fight against Russian information warfare operations in Lithuania. Lessons learned from the Soviet-era are being carried over into the 21st century information environment. Though technology has advanced significantly in the past three decades, the methodologies, strategies, and intentions of Russia largely have not. If anything, Russia has proven itself very skillful at adapting Soviet-era methodologies for a modern-day digital environment and has successfully interfered in the domestic affairs of countries throughout the world. A major objective is to stoke fear and sow division in societies, in the hopes that Russia will be able to advance its geopolitical aspirations. Though Russian

[303] Ibid
[304] Ibid
[305] Ibid

incursions into the affairs of the Baltic states have been well documented and are a continual threat, it has only been in the past few years that items included in media and state security documents have been formally implemented. The concern has been less focused on Russia's capability to influence Slavophiles and more on influencing the Polish minority, which has been a cause of tension for Lithuanian authorities. Additionally, a portion of the non-Slavic audience is causing concern, due to Lithuanian viewers watching Russia-based channels for the entertainment and production values, as they fill a noticeable void in the Lithuanian media environment.

Hard-power security concerns attracted the most attention throughout the 1990s and Lithuanian policy makers and media organizations largely shared this mindset. The removal of Russian troops and the territorial integrity of the country took precedence over soft-power concerns. Though the understanding of Russia's capabilities in the information sphere existed, policy makers were far more interested in creating a media environment that was "Lithuanian", catering to the media needs of Lithuanians. At the beginning of the 1990s, major political forces in Lithuania shared a consensus as to the direction of security policy, identifying three major security topics that were deemed as possible areas for action.[306] The first of the problem areas consisted of "external threats" that could impact Lithuania due its "unfavourable geopolitical situation".[307] The second consisted of political influence from Russia, and the third focused on an increase in organized crime.[308] Information, social, psychological, or technological security were not mentioned as major points of emphasis, nor were they named in subcategories or planning strategies of this era. What can be considered the first official Lithuanian state planning document, the *Outline of the concept of national security of Lithuania*, stated that a position of neutrality was to be the basis of the country's security policy. Soon coming to the realization that a newly independent Russia had no intention of relinquishing its influence in the region, it was soon decided that a close relationship with the West was necessary. This would be beneficial for all aspects of security for a newly independent and ambitious, albeit weak, Lithuania. A major Russian objective during the 1990s, in addition to the attempts to control its internal and

[306] Piotrowski, Sławomir. (2018). "Security Policy of the Baltic States and its Determining Factors." *Security and Defense Quarterly, 22*(5), p. 8. Retrieved 29 December 2020. http://31.186.81.235:8080/api/files/view/627285.pdf
[307] Ibid
[308] Ibid

economic situation, was to maintain influence upon the former Soviet republics. Membership in multi-national security alliances and cooperative economic organizations were offered to the former republics with the promise that they would ensure that future "security" needs would be provided. While these proposals did spark the interest of several former republics, who ultimately accepted membership in these organizations, the Baltic states rejected all Russian overtures, stating they would continue to pursue membership in the EU and NATO.

Economic security was added to the state security strategies by the mid-1990s, though information and psychological security had not yet been formulated by policymakers. Soft-power forms of security were gradually added to security strategies in succeeding years and specifically include information, cyber, social, and psychological security as major focal points for state authorities. Even after Putin ascended to the Russian presidency, official state security documents did not place information security as a major priority. Attention was largely focused on gaining membership in NATO and the EU, and in increasing economic security, reflected in security strategies of the early 2000s.

Russian information campaigns aimed at the Baltic states after these events became more common and have remained a constant threat ever since. The subsequent improvement of the Russian economy, from the tumultuous period in the 1990s, has allowed for greater funding and resources to be allocated to its information warfare operations worldwide. The effectiveness of these efforts has varied by country but have been quite effective in destabilizing many Western countries. The European Commission has stated that Russian propaganda campaigns have been "extremely successful" at spreading disinformation throughout the European Union.[309]

Lithuania enacted its first National Security Strategy in 2002, which was in effect until 2012. During this decade, the security environment changed significantly in the Baltic states, which required that the existing document be updated to include newer threats and technologies. Then-National Defense Minister Juozas Olekas confirmed that the 2002 Strategy was outdated and added that, "New challenges, including hybrid warfare, cyber and informational challenges,

[309] Stone, Jon. (2018, 17 January). "Russian disinformation campaign has been 'extremely successful' in Europe, warns EU." The Guardian. Retrieved 28 December 2020. https://www.independent.co.uk/news/uk/politics/russian-fake-news-disinformation-europe-putin-trump-eu-european-parliament-commission-a8164526.html

and a changed geopolitical situation have emerged."[310] In addition to protecting these sectors and updating new and existing security measures, the 2012 update was intended to improve relations with Russia. Unfortunately, this desire has largely been left unfulfilled as Lithuania-Russia relations have only declined since this time. Russia's unpredictability and aggressiveness have only placed greater emphasis on the security environment.

Lithuania's national security documents have expressly included information security as an aspect of the broader security environment since the 2010s. The advancement of digital technologies, the popularity of social media platforms, and Russia's actions in Ukraine in 2014 were all factors in protecting the information space. Security and planning strategies such as *The Military Strategy of the Republic of Lithuania*, the *Lithuania National Security Strategy 2012*, the *Lithuania National Security Strategy 2017*, and the agreement signed by the Seimas in 2018, the *Agreement Among the Political Parties Represented in the Seimas of the Republic of Lithuania on the Lithuanian Defense Policy Guidelines* are just a few of the major state security documents that put significant emphasis on societal, information, and cyber security. Lithuania's wariness of Russia has been a constant since the country regained independence but has increased since the mid-2010s. In September 2018, additional measures were undertaken when the agreement *On the Guidelines of the Lithuanian Defense Policy* was signed. In addition to an increase in defense funding, the document gives:

> "… particular attention to the prevention of hybrid threats: in order to assess threats and risks to national security and public resilience, the agreement provides for the development of a strategy for the protection of the state against hybrid threats. Its implementation envisages strengthening the monitoring of these threats and the preparedness to prevent and manage them, involving the state institutions, the public, non-governmental organizations and the media in the process of the unit coordinating these activities in the Government."[311]

---

[310] "Lithuania to draft new National Security strategy." (2015, 27 October). The Baltic Times. Retrieved 29 December 2020 . https://www.baltictimes.com/lithuania_to_draft_new_national_security_strategy/

[311] "An agreement on Lithuanian defense policy guidelines has been signed." My government. (lrv.lt.) (2018, 10 September). Retrieved 28 December 2020. https://lrv.lt/lt/naujienos/pasirasytas-susitarimas-del-lietuvos-gynybos-politikos-gairiu

The 2012 National Security Strategy explicitly mentions "information attacks" as a threat to Lithuanian national security and defines them as "actions of state and non-state entities in the international and national information space aimed at spreading biased and misleading information, shaping a negative public opinion in respect of interests of national security of the Republic of Lithuania."[312] Though published two years before Russia's actions in Crimea and the Donbas, the understanding of Russia's information warfare capabilities had become a very visible part of their foreign policy by this time. The Bronze Night events in Estonia five years prior showcased the damage and offensive capabilities Russia could deliver in mobilizing its diaspora with information operations. Additionally, the 2012 *Military Strategy of Lithuania* also stated that the information space was a major target and that, "The development and wide availability of information technologies and systems are likely to cause even more information attacks in the future."[313]

The security discourse in the Baltic states has been ongoing since they regained independence in 1990-91. In Lithuania, public statements made on the behalf of state officials have often been more forceful in nature than in Latvia or Estonia. While several reasons exist for this, the most significant centers on the demographic situation, which has allowed Lithuania to speak more forcefully against Russia and risk less in agitating the Russophile, or general Slavic, population. In the 21st century, the Baltic security discourse has been focused more on "normative differentiation" than on hard-power initiatives to protect the territorial integrity of the region.[314] This rhetoric has continued in the 2000s, and certainly since 2004, when the Baltic states became NATO and EU members. While Russia's actions in Georgia in 2008 provoked much concern in Lithuania, with their possible actions against the Baltics, it was only in 2014 after the events in Ukraine and the annexation of Crimea that these fears became much more prevalent. The heightened tensions were particularly noticeable in Lithuania when then-president

---

[312] Lithuania, Seimas of the Republic of Lithuania. (n.d.). "Resolution Amending the Seimas of the Republic of Lithuania Resolution on the Approval of the National Security Strategy." p. 5. Retrieved 29 December 2020. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e7fcc2608f1f11e8aa33fe8f0fea665f?jfwid=uu1o96cqv

[313] Lithuania, Ministry of Defense. (2012). "The Military Strategy of the Republic of Lithuania 2012." p. 5. Retrieved 29 December 2020. https://www.files.ethz.ch/isn/167339/THE%20MILITARY%20STRATEGY%20of%20the%20Republic%20of%20Lithuania.pdf

[314] Fernandes, Sandra. & Correia, Daniel. (2018). "(Re)securitisation in Europe: The Baltic States and Russia." Debater a Europa. p. 114. Retrieved 16 December 2020. https://www.researchgate.net/publication/322690589_Resecuritisation_in_Europe_the_Baltic_States_and_Russia

Dalia Grybauskaite voiced her concerns in a speech to the United Nations, asking, "how much time do we have" in the face of a country that "seeks to rewrite history and redraw the borders of post-war Europe?"

Beginning in 2014-2015, the protection of Lithuania's security environment became a significant priority. Though pledges to increase military spending and strengthen defense capabilities were made, Lithuania made specific commitments to enhance soft-power security. Much emphasis was placed on increasing the security of the country's information, cyber, and psychological spaces, which were deemed ineffective in defending against new and increasing threats. State efforts were implemented that focused on Russian media influence in the country, particularly Russia-based TV channels. Available to Lithuanian audiences through cable providers since the 1990s, television became a significant resource that Russia regularly utilized to spread false and misleading narratives. Since the late 2000s, the number of Russian broadcasts in Lithuanian television has more than doubled from 79 hours per week in 2007 to 198 hours in 2017.[315] This has given Russia increased opportunities to spread false or misleading narratives into the Lithuanian information space. Several major narratives are utilized by Russia on a regular basis, which include questions to Lithuania's right to exist, the country's emigration issue, income inequality, and the energy sector, among others.[316] Russian politicians have even discussed a possible Russian invasion of the Baltic states on Lithuanian television as well.[317]

In April 2015, the Radio and Television Commission of Lithuania suspended the license for the Russia-based, Russian language channel RTR Planeta for a period of three months, claiming that the channel was responsible for "inciting discord, warmongering, spreading biased information."[318] Though the dissemination and consumption of information are protected under the Lithuanian constitution, state authorities deemed that RTR Planeta sought to incite hatred, sow societal divisions, and spread disinformation to generally weaken the country. Constitutional protections are not extended to this type of content, which is defined as, "Freedom to express

---

[315] Schrøder, Anne Sofie. (2017, 28 September). "Lithuania has a volunteer army fighting a war on the internet." euronews.com. Retrieved 2 January 2021. https://www.euronews.com/2017/09/28/lithuania-has-a-volunteer-army-fighting-a-war-on-the-internet

[316] Ibid

[317] Ibid

[318] Fernandes, Sandra. & Correia, Daniel. (2018). "(Re)securitisation in Europe: The Baltic States and Russia." Debater a Europa. p. 116. Retrieved 16 December 2020. https://www.researchgate.net/publication/322690589_Resecuritisation_in_Europe_the_Baltic_States_and_Russia

convictions or impart information shall be incompatible with criminal actions - the instigation of national, racial, religious, or social hatred, violence, or discrimination, the dissemination of slander, or misinformation."[319] Restricting RTR Planeta, however was not the first temporary ban on Russia-based TV channels. Earlier protective efforts began in October 2013 when a temporary ban was placed on Russia-based First Baltic Channel (PBK) and Gazprom-owned NTV Mir in March 2014.[320] RTR Planeta was once again restricted in 2015 and 2016 while TVCI, another Russian-based channel was restricted twice in 2017, for a total of seven months.[321] Russia has strongly criticized Lithuania's actions in banning Russia-based channels and has accused the country of not truly being democratic, in addition to implementing Russophobic policies. Though the temporary nature of these programming restrictions means that these channels were reintroduced to the Lithuanian media environment, several additional channels have been restricted since. In July 2020, the Radio and Television Commission again restricted Russia-based TV channels, which include RT, RT HD, RT Arabic, RT Spanish, RT Documentary HD, RT Documentary and RT TV.[322] The length of programming restrictions has varied. Russian TV channel owners who are on the EU sanctions list have had their channels restricted in many EU countries, including the Baltic states. The EU has also encouraged all its member states to restrict these channels as well, stating they are responsible for the spread of disinformation and misleading narratives throughout Europe.

Like its Baltic neighbors, Lithuania has invested in providing media opportunities for its minority populations. Of the major television networks, three of the four have added a second channel that are dedicated to serving the different segments of society, including minority language programming.[323] In February 2017, Current Time (Nastoyashchee Vremya in Russian) was launched as a cooperative effort between Radio Free Europe/Radio Liberty (RFE/RL) and

---

[319] "Lithuania Constitution." (n.d.). International Constitutional Law Project (ICL) Project. Retrieved 31 December 2020. https://www.servat.unibe.ch/icl/lh00000_.html

[320] Fernandes, Sandra. & Correia, Daniel. (2018). "(Re)securitisation in Europe: The Baltic States and Russia." Debater a Europa. p. 116. Retrieved 16 December 2020.

[321] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index* (p. 200). Retrieved 24 December 2020. http://prismua.org/en/dri/

[322] "Lithuania considers following Latvia in banning Russia's RT." (2020, 2 July). lrt.lt. Retrieved 31 December 2020. https://www.lrt.lt/en/news-in-english/19/1194032/lithuania-considers-following-latvia-in-banning-russia-s-rt

[323] "Mass media in Lithuania." (n.d.). Wikipedia.com. Retrieved 1 January 2021. https://en.wikipedia.org/wiki/Mass_media_in_Lithuania#Radio

the Voice of America (VOA).[324] Initially offered as a cable-only channel, it is now available as an over-the-air channel nationwide and to viewers living within 50 kilometers of the Lithuanian border.[325] The launch of this channel is in response to the rise of disinformation that has been noticeable in Lithuania over the past several years and is intended to provide quality information to viewers. A secondary aim is to provide good journalistic content to outside areas within the 50-kilometer zone of the Lithuanian border, so that viewers in these areas have access to this kind of content. Outside of the Baltic region, there are often limited options for viewers to consume fact-based content, which is a continuing concern for Lithuanian officials.[326]

Television programming for the Polish minority in Lithuania has also been launched. TVP Wilno, an initiative which is funded by Poland's national public broadcaster, is intended to provide alternative sources of information to Polish-speakers that might otherwise come from Russia-based media.[327] There have been concerns in previous years that the Polish minority have become too close to Russia in the information space. Russia-based, Russian language media has gained an audience among the Polish minority, because of the overlap in the two languages. Though initially proposed a decade ago, the death of Polish President Lech Kaczynski slowed efforts to create a dedicated Polish language channel.[328] Lithuanian officials revised the idea, bringing it to the attention of Polish authorities, who were receptive of the plan.[329] Funding for programming is limited and will likely not see significant increases soon, which has been a concern for minority language media initiatives throughout the Baltic states. In line with Estonia's approach with ETV+, Lithuania-produced content will focus on local issues that affect the Polish minority in Lithuania. There are also hopes that Lithuanians may also become viewers and learn not only some of the language, but also the issues that affect the Lithuanian Polish community.[330] However, it should be noted that the general minority media landscape still does

---

[324] "Russian-language TV channel Current Time to be launched in Lithuania." (2018, 14 September). lithuaniatribune.com. Retrieved 1 January 2021. https://lithuaniatribune.com/russian-language-tv-channel-current-time-to-be-launched-in-lithuania/

[325] Ibid

[326] Ibid

[327] Ketlerienė, Aleksandra. (2019, 21 September). "New Polish channel in Lithuania seeks to win back ethnic minority viewers from Russian TV." Retrieved 1 January 2021. https://www.lrt.lt/en/news-in-english/19/1098787/new-polish-channel-in-lithuania-seeks-to-win-back-ethnic-minority-viewers-from-russian-tv

[328] Ibid

[329] Ibid

[330] Ibid

not meet the needs of these communities sufficiently and often lacks funding for growth. The chances that Lithuanian officials will ban Russia-based channels in the future is likely, though there are concerns as to using content restriction too regularly. Media experts urge that each potential ban be considered carefully as to why the content restriction is being proposed. Additionally, there should be careful attention paid protecting constitutional rights on freedom of speech/expression and free flow of information.[331]

The Lithuanian radio sector remains a popular medium for both information and entertainment content, second only to television. Generally, Lithuanian radio is not as diverse or economically vibrant as its television counterpart. The market size is small and there is great competition for advertising revenues, which creates limited opportunities for growth. Programming along ethnic and linguistic lines is also limited as there are only two Polish language radio stations nationwide[332] and two in Russian. Creating programming for minority groups has been slow in development and continues to be limited in scope. Unlike television, there are no significant plans to create further minority language programming, at least in the near future, though privately funded initiatives and multinational organizations are increasingly providing grants and other funding sources for minority language media. Radio is not a major aspect of Russia's information warfare campaigns in the Baltic states, and security measures are less focused on radio broadcasters as they are with television.

Lithuanian print media outlets have followed the trends documented in much of the Western world. Newspaper circulation has declined significantly in the 21st century and those that remain have often had to reduce publication frequency, (i.e., from daily to weekly),[333] staffing levels, and reporting assignments. Currently, no national newspaper is published daily, which is due to the decline in readership and the general uneasiness in the print media industry that is a carryover from the 2008 financial crisis, along with an increase in VAT taxes from 5% to 21%.[334] Additionally, institutional norms, the lack of trust in print media, and insufficient

---

[331] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index* (pp. 190-208). Retrieved 1 January 2021. http://prismua.org/en/dri/

[332] "National Minorities." (2016, 1 September). Ministry of Culture of the Republic of Lithuania. Retrieved 2 January 2021. https://lrkm.lrv.lt/en/activities/national-minorities

[333] "Media of Lithuania." (n.d.). truelithuania.com. Retrieved 27 December 2020. http://www.truelithuania.com/media-of-lithuania-1664

[334] "Lithuania: Online media also struggling." (2020, April). eurotopics.net. Retrieved 2 January 2021. https://www.eurotopics.net/en/149414/lithuania-online-media-also-struggling#

professional practices and ethics have all played roles in the decline of Lithuania's print media sector.[335] In 2019, the country's oldest paper, Lietuvos žinios, ceased publication after more than a century and Lietuvos Rytas, a major national publication, has reduced their publication frequency from daily to three times per week.[336] Foreign ownership has been an increasing trend in last few decades, but certainly in the last twenty years. Most foreign owners are based in Estonia and Sweden.[337] Unlike the scrutiny that radio and television outlets receive and the role that they play in propagating Russian-friendly narratives, Lithuanian print media have been less of an emphasis for countermeasures and media policy in general. For the most part, much of Russia's information operations have migrated online, though it has not completely abandoned traditional print media. The readership of these papers is generally low, though they still pose a threat.

Lithuania's online environment has become a significant focus for state and media authorities in the digital age. As mentioned previously, Russian information warfare operations have increased in sophistication and number since 2014 as Russia has increased funding and resources for these initiatives. Excluding social media platforms, online news portals containing Russian disinformation are largely centered on a few sites, such as Baltnews.lt and Sputniknews.lt. Both sites have connections to the Russian state information agency Rossiya Segodnia.[338] Fortunately for Lithuanian authorities, these sites have limited audiences in the country. The State Security Department of Lithuania and the Lithuanian Ministry of Defense have included both Baltnews.lt and Sputniknews.lt in reports of sites that are aimed at spreading disinformation in Lithuania. Because of the sites' limited audience size, they are deemed "not significant" by the State Security Department as Baltnews.lt had approximately 700 daily viewers in Lithuania while Sputniknews.lt has approximately 900 (as of August 2017).[339] Though the audience sizes of these sites have remained low, that does not mean there is not cause for concern. There are fears that sites such as Baltnews.lt and Sputniknews.lt could grow in popularity and become a significant threat to the country's information space. This largely

---

[335] "Mass media in Lithuania." (n.d.). Wikipedia.com. Retrieved 2 January 2021. https://en.wikipedia.org/wiki/Mass_media_in_Lithuania#Radio
[336] Ibid
[337] Ibid
[338] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index* (p. 198). Retrieved 2 January 2021. http://prismua.org/en/dri/
[339] Ibid

depends on the desires and resources that Russia feels is appropriate for influencing the Lithuanian information space.[340] The allocation of funding and resources could change the online environment dramatically and quickly.

Social media platforms have become major resources that Russia utilizes in disseminating propaganda and disinformation. Over the past decade, there have been countless documented instances of Russian-backed efforts to infiltrate social media sites with inflammatory, derogatory, misleading, or outright false content. The objectives are the same as they are in more traditional media sources: to inflame societal tensions, instill fear, and diminish trust in host governments. In the digital era, discussions on "regulating" the internet, or at minimum, the monitoring of content on it, has been regularly discussed. While content management strategies may be effective in countries such as China with its internet firewall, many Western countries have struggled to come up with policies that address the dramatic increase in conspiracy theories, disinformation, and extremism that has manifested itself on the web. Technically, it is possible to restrict websites and content, though there are major legal challenges that are encountered in doing so. Democratic governments often cannot restrict content, or at least not significantly, due to constitutional protections for freedom of speech/expression, a fact that Russia has eagerly exploited. In Lithuania, the task of monitoring social media, chat rooms, and the comments sections of online news portals, largely falls to individuals that act as a filter on false, defamatory, misleading, or hateful content. Reflecting online lingo used for those who seek to stoke negative reactions among other internet users (i.e., "trolls"), these guardians of the online environment have adopted the moniker of "elves" in this fight. Though many trolls are based in Russia, there are many that can be found outside of its borders, including in Lithuania and in other countries throughout the region.[341] While some elves may work with others, either loosely or in tandem, other elves are largely independent. Many are

[340] Ibid

[341] Sengupta, Kim. (2019, 17 July). "Meet the Elves, Lithuania's digital citizen army confronting Russian trolls." Retrieved 2 January 2021. https://www.independent.co.uk/news/world/europe/lithuania-elves-russia-election-tampering-online-cyber-crime-hackers-kremlin-a9008931.html

working professionals employed in a variety of jobs that volunteer their time to monitor the Lithuanian online environment to "find and expose fake accounts and pro-Russian trolls."[342]

The "elves" began as a grassroots movement in 2014 after Russia's annexation of Crimea. The number of these cyber warriors has grown over the past few years and currently numbers over 5,000 Lithuanians. Initially, elves were concerned that the Baltic states could be a future target for Russian military operations, a concern that continues to emanate throughout the community today. The desire is to avoid any potential war with Russia and to ensure that pro-Russian, pro-Kremlin narratives do not unduly influence Lithuanians, sow societal discord, and denigrate the country's institutions. Though the objective of the elves is to counteract dubious information aimed at the country, it is important to note that they are not engaged in creating and disseminating false narratives themselves. On average, approximately 20,000 online articles are analyzed by elves from more than a thousand different sources.[343] Elves are not just confined to Lithuania. Volunteers are also located in neighboring countries such as Latvia and Estonia as well as in the Nordic states and even as far south as Armenia.[344] Additionally, there has also been interest in the elves' mission in other parts of Europe, such as in Britain.[345] Other Western nations are noticing these efforts to defend cyberspace, allowing more elves to come onto the digital scene.

The Lithuanian Ministry of Defense's military strategic communications department monitors Russian communication activities, which include monitoring online content and television broadcasts. Russian activities in Lithuania have increased not only on television, but in newspapers, radio programming, and on social media, a trend that is only likely to continue in future years.[346] The Defense Ministry cannot make decisions as to the restriction of content

---

[342] Schrøder, Anne Sofie. (2017, 28 September). "Lithuania has a volunteer army fighting a war on the internet." euronews.com. Retrieved 2 January 2021. https://www.euronews.com/2017/09/28/lithuania-has-a-volunteer-army-fighting-a-war-on-the-internet

[343] Sengupta, Kim. (2019, 17 July). "Meet the Elves, Lithuania's digital citizen army confronting Russian trolls." Retrieved 2 January 2021. https://www.independent.co.uk/news/world/europe/lithuania-elves-russia-election-tampering-online-cyber-crime-hackers-kremlin-a9008931.html

[344] Ibid

[345] Ibid

[346] Schrøder, Anne Sofie. (2017, 28 September). "Lithuania has a volunteer army fighting a war on the internet." euronews.com. Retrieved 2 January 2021. https://www.euronews.com/2017/09/28/lithuania-has-a-volunteer-army-fighting-a-war-on-the-internet

themselves and must consult with the Radio and Television Commission of Lithuania, which is tasked with the final decision as to the implementation of content restriction measures.

Multinational efforts in combating the rise of fake news and disinformation, such as the EU's EUvs.Disinfo initiative, have been "professionalized" over the past few years in attempts to adequately respond to information warfare threats.[347] In 2018, over 600,000 people visited the site, though staffing levels remained low, employing only 16 people.[348] The implementation of programs such as EUvs.Disinfo indicate a shift in the thinking of the EU and show a desire to counteract dubious information as it becomes more prevalent throughout European societies. The EU has not implemented extensive strategies regarding information warfare, though its increasing activities are becoming better recognized both by member states and internationally.

Lithuanian officials, unlike their EU counterparts, have not only the knowledge and experience of being on the receiving end of Russia's information war efforts, but also generally view the information space as being filled with ever-increasing amounts of dubious information.[349] Russian content broadcast on Lithuanian television has become commonplace, largely due to cost and linguistic content regulations. Russian programs are usually less costly than EU programming and do not have to translated for rebroadcast in Lithuania.[350] Russian non-news programming often contains messaging that is critical of the West and Western institutions, pointing to examples such as Brexit and political tensions in the US.[351] Though there are no stated plans in the near future to scale back or eliminate Russian content, both news and non-news programming, there are more legal measures that Lithuanian authorities can utilize in regards to content restriction. Most significant of these measures is the option of ordering communication providers to shut down their operations (i.e., internet servers) for a period of up to 48 hours with a court order if the determination is made that they are being used by outside actors to carry out attacks (cyber, disinformation, or both).[352] Lithuanian Defense Vice-Minister Edvinas Kerza claims that a strong approach is necessary to defend against Russia's actions. This

[347] Peel, Michael. (2019, 3 February). "Fake news: How Lithuania's 'elves' take on Russian trolls." ft.com. Retrieved 2 January 2021. https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf
[348] Ibid
[349] Ibid
[350] Ibid
[351] Ibid
[352] Ibid

increasingly means taking a harder-line approach in both the information and cyber realms to quickly react to Russian attacks, which have only gotten more sophisticated.[353]

Generally, fact-checking initiatives are a fairly recent phenomena in Lithuania, and only a few have adequate resources to establish themselves as independent journalistic initiatives that differ from their host organizations. The online news portals, 15min.lt and Delfi.lt, have also begun fact-checking initiatives within the past few years, and they have enough resources to do a decent amount of claim-checking and debunking. Because of the newness of these initiatives, it is not yet known as to their effectiveness or if they will be regularly sought out by media consumers, who may or may not want to use specially designated fact-checking sites to supplement their other media consumption habits. Collaborative efforts also contribute to fighting disinformation in Lithuania's digital space. The website Demaskuok.lt is an initiative created by a group of military officials, journalists and regular citizens, funded in part by Google's Digital News Initiative.[354] Having a relationship with Delfi.lt, users have the option to directly contact journalists regarding unusual happenings they feel should be further investigated and/or brought to public attention. Similar in style to the site Propastop in Estonia and the work of Lithuanian elves, online articles are examined, approximately 20,000 per day from more than 1,000 sources, by searching databases for specific words and narratives, such as failed state, emigration, etc.[355] Though not a foolproof system, analysts, much like elves, are able to counter false and misleading information, hopefully before it becomes widely available to online audiences. Also, like Propastop, content that contains wording or themes that match databases is then examined to determine if it should be debunked or reported.

By 2017, Lithuanian officials had the benefit of observing Russian foreign policy for three years after its annexation of Crimea. However, any hope that Lithuania may have had in the effectiveness of international sanctions in response to Russia's actions was not realized. Information threats have only increased in number and intensity while sanctions have boosted Russia's domestic industries. The revised *Security Strategy* that was implemented that year once

---

[353] Ibid

[354] Peel, Michael. (2019, 3 February). "Fake news: How Lithuania's 'elves' take on Russian trolls." ft.com. Retrieved 2 January 2021. https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf

[355] Ibid

again stated that Russia's actions constituted a significant threat to Lithuania's security environment, saying:

> "military propaganda spread by certain states and non-state actors, warmongering and incitement to hatred, attempts to distort history as well as other unsubstantiated and misleading information directed against the national security interests of the Republic of Lithuania which leads to distrust of and dissatisfaction with the State of Lithuania and its institutions, democracy, national defence, seeks to widen national and cultural divides and to weaken national identity and active citizenship, attempts to discredit Lithuania's membership of NATO, NATO capabilities and the commitment to defend allies, to undermine citizens' will to defend their state; also information activities that are aimed at influencing the country's democratic or electoral processes or the party system, or that are targeted at the societies and policy makers of other Member States of the EU and NATO, seeking unfavourable decisions for the Republic of Lithuania."[356]

Understanding the threats that Lithuania faces in the information security realms requires a broad perspective on the timeline and activities that Russia has aimed at the region and how countermeasures, policies, and programming efforts have been developed. Even after the events in Ukraine in 2014, Lithuania has generally been more concerned with soft-power initiatives. The Lithuanian *Threat Assessment* documents over the past several years have largely contained security concerns that have stretched over several years, with the differences that occur year-by-year. For information security, this emphasis is on highlighting the ways in which Russia distorts Lithuanian history, culture, economic development, and its relationship with NATO and the EU. Though these documents are good references for gaining an understanding for the reasons, methodologies, and perspectives Russia has, they offer little in explaining Lithuania's countermeasures.

The Lithuanian Ministry of Culture is responsible for drafting and implementing the country's media policy. Existing policy documents have been updated to ensure that the country's media environment is able to withstand the demands that media outlets face in the 21st

[356] Lithuania, Seimas of the Republic of Lithuania. (2017, 17 January). *National Security Strategy*. pp. 5-17. Retrieved 29 December 2020. https://kam.lt/en/defence_policy_1053/important_documents/strategical_documents.html

century. Lithuania's more homogeneous demographic composition has allowed it to make more forceful statements against Russia and favor the ethnic majority in the media sector. Additionally, the need for minority language media has been lower than in Latvia and Estonia, and there are still no seriously viable Lithuania-based minority language media outlets aimed at catering to the needs of ethnic and linguistic minorities. Public broadcasters offer this kind of content, but it is insufficient in quantity. Since most media is provided in the Lithuanian language, the most recent media strategy acknowledges that "Lithuania's historical experience and today's geopolitical situation encourage the search for alternative sources of information."[357] The current media strategy document was implemented in February 2019 and is slated to run through 2022. Included in some sections more than others, security is used when describing the aims of the latest, and current, media strategy and is a significant focus of the document.

> "Accordingly, more attention should be paid not only to the dissemination and exchange of European culture, but also to European audiovisual works and their production. The theoretical aim of devoting more than half of television time to European works must be transformed into real audiovisual productions, both in television broadcasts and in the repertoire of on-demand audiovisual media service providers." [358]

The minority language media that is available in Lithuania is also problematic for state officials as "there is no in-depth monitoring of the content in the media of ethnic communities."[359] The understanding that the availability of media sources has increased exponentially is both promising and concerning for state authorities. The diversity of media sources has provided a wealth of information to societies that may, or may not, have had access to quality journalism. Media outlets in Lithuania have seen a significant increase in traffic in online content, including on social media platforms, but often face reduced advertising revenues for print-form publications that may hinder growth. Russia has aptly seized upon the lack of Russian language media outlets catering to Russophiles in the Baltic states. In efforts to counter this trend, and to increase the health and vitality of the media environment, the latest media

---

[357] Lithuania, Ministry of Culture. (2019, 19 February). "Order on Strategic Directions for Public Information Policy Approval for the Year 2019-2022." Retrieved 1 January 2021. https://www.e-tar.lt/portal/lt/legalAct/95c4cf60344211e99595d005d42b863e

[358] Ibid

[359] Ibid

strategy outlines several medium-term objectives to be undertaken over the next several years. These include the promotion of a diverse information space with sufficient availability of media sources and services, promoting regional media throughout Lithuania, and in ensuring that ethnic and linguistic minority communities have access to public information and other media sources.[360] Other objectives of the current media policy include addressing economic and businesses practices in the media sector that can have a negative impact on content, such as the current consolidation trend. They seek to promote competition and development and to use anti-trust statutes, distancing themselves from political and/or economic influences while advocating for transparency of media ownership and what interests are held by owners.[361] In a more vague suggestion, media organizations are being encouraged to practice good journalism and create content that allows media consumers to be connected to local and national events rather than seek out information from other, possibly non-Lithuanian sources that may not be of sufficient quality.

The Lithuanian Cyber Space in the 21st Century

The security of Lithuania's cyber environment has faced many new and sophisticated challenges in the 21st century. An increase in cyber-attacks has been well noted, the majority of which have come from Russia or its affiliated actors attempting to compromise the country's electronic infrastructure. State security and planning strategies have included cybersecurity among the many aspects of non-military protection that requires significant funding and resource allocation. Russian cyber-attacks have only increased in frequency and severity since 2014 and will likely continue to target all aspects of Lithuanian society in coming years. The 2016 *Military Strategy of Lithuania* states that, "It is very likely that cyber capabilities would be extensively used during any type of conventional or unconventional conflict in the region."[362] In 2015, the Ministry of National Defense became the state agency responsible for the drafting and implementation of Lithuania's cybersecurity policy. Additionally, the National Cyber Security Centre, a subunit of the Ministry of Defense, was specifically established to ensure the cyber

[360] Ibid
[361] Ibid
[362] Lithuania, Ministry of Defense. (2016). "The Military Strategy of the Republic of Lithuania." p. 5. Retrieved 3 January 2021.

security of state institutions and the general Lithuanian cyber infrastructure. The Cyber Security Council was launched to coordinate the security efforts of the public and private sectors as well as to provide professional assistance and recommendations for cybersecurity improvements.[363] Before these agencies were launched, the public and private sectors often did not cooperate significantly, which often led to confusion and a significant vulnerability in Lithuania's cyber security environment. Much like the cooperative efforts in Latvia and Estonia, public-private cooperation is integral for providing adequate cybersecurity protections in the modern era and is dependent on the actions of state and non-state actors in addition to the educational sectors, especially colleges and universities, who provide degree, certification, and other training programs. The Lithuanian Armed Forces (LAF) is also tasked with developing cyber defense capabilities, especially regarding the security of military communications and information infrastructures.[364]

Lithuania has a long tradition in information technology and telecommunications, dating back to the Soviet era. Initially, this included an IT sector and the manufacture of software and hardware, with the sector only growing over the years.[365] Agreements with universities, government, and business were eventually reached, and by the late 1980s, there were approximately 20,000 people employed in the cyber and technology fields.[366] However, the collapse of the Soviet Union ultimately brought about the end of the country's electronic development industry, which was due to the end of Soviet contracts, as well as insufficient monies needed to modernize the sector to Western standards.[367] The newly independent Lithuanian government attempted to modernize the country's electronic infrastructure beginning in the early 1990s, and has striven to provide broadband internet service to its citizens. Like its Baltic neighbors, Lithuania offers e-Government services that are available online, though most

[363] Lithuania, Ministry of National Defense of the Republic of Lithuania. (2017). "Lithuanian Defense Policy White Paper." p. 56. Retrieved 3 January 2021. https://kam.lt/download/59163/wp-2017-en-el.pdf
[364] Ibid
[365] Butrimas, Vytautas. (2015). "National Cyber Security Organization: Lithuania" (Publication). p. 5. Retrieved 4 January 2021. NATO Cooperative Cyber Defense Centre of Excellence. https://ccdcoe.org/library/publications/national-cyber-security-organisation-lithuania/
[366] Ibid
[367] Ibid

Lithuanians do not use these services. Only 41% use e-Government services and just 31% use them to submit documents to e-Government services.[368]

Lithuania has successfully established itself as a forward-looking country and has come to the realization that providing electronic services and ensuring cybersecurity will make the country more competitive and secure in the future. Cybersecurity efforts have been initiated with both top-down and bottom-up approaches. Bottom-up approaches consist of the establishment of institutions, in the absence of a comprehensive law, that define the associated responsibilities and work in relation to other cybersecurity institutions. Top-down approaches refer to comprehensive legislation that explicitly states the roles of previously established institutions or creates new cybersecurity institutions that exist in a hierarchical system.[369] Institutions of both approaches are notable in their cybersecurity efforts, which include the National Communications Regulatory Authority and the National Computer Emergency Response Team (CERT-LT).[370]

Lithuania's cyber security foundation was laid in 1996 with the passage of the *Law on the Fundamentals of National Security*. Listed within the law are security initiatives aimed at the energy, transport, telecommunications, finance, credit, information technology, and other high-technology sectors.[371] The Seimas later approved the *National Security Strategy*, which listed cybersecurity as a national security priority.[372] In declaring the digital realm as susceptible to threats, state authorities listed cyber-attacks as a threat to Lithuania when they threaten the operation of state institutions, classified information, and "other targets" which threaten the wellbeing and vitality of Lithuanians.[373] Further evidence of the state's desire to secure Lithuania's cyber space came in the form of the 29 June 2011 resolution *The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019.* The resolution included three overarching objectives to be focused upon: ensuring the security of the state's resources, the functioning of information infrastructures deemed critical to national security, and that the general cyber security environment is maintained for Lithuanians and other persons

[368] Ibid
[369] Ibid, p. 7.
[370] Ibid
[371] Ibid, p. 8.
[372] Ibid
[373] Ibid

staying in the country.[374] Another major objective was to further develop the security of electronic information throughout the country, stating that the aim was:

> "…in the year 2019, a 98 per cent level of compliance of state-owned information resources with legislative requirements on electronic information security (cyber security), reduction to 0.5 hour of the average time of response to critical information infrastructure incidents and a 60 per cent level of the Lithuanian residents who feel secure in cyberspace."[375]

The increased emphasis on cybersecurity in the 2010s was partially centered on previous security aspirations for this environment that could not be adequately carried out due to "period[s] of economic hardship, electronic information security (cyber security) received neither sufficient attention nor information resources."[376] Foreign-originating cyber threats have received significant attention. Security discussions and resources have been allocated, financially and technically, that can limit the threat of these threats succeeding in their objectives, though it is impossible to truly eliminate all cyber risks. A notable initiative on behalf of the state is the Lithuanian Traffic Exchange (ITE) node, which acts as a central site that hosts cyber protection capabilities of the country's cyber environment.[377] Later legislation enacted by the Seimas, the *Law on Cyber Security*, was approved in 2014, and contained all three of the objectives stated in the 2011-2019 document as part of its focus as well.

Russia's actions in Ukraine in 2014 spurred much activity in the Lithuania's cybersecurity sector. New state institutions were launched, and existing ones were given additional responsibilities to oversee newly created agencies. Organizational switch-ups occurred due to the shifting of responsibilities, and emphasis was placed on securing Hosting Services (HS), Industrial Control Systems (ICS), and Critical Information Infrastructure (CII), in addition

---

[374] Government of Lithuania. (2011, 29 June). "On the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019." Retrieved 3 January 2021. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf

[375] Ibid

[376] Ibid

[377] Ibid

to previous focuses on the other aspects of cybersecurity.[378] The 2014 Cyber Security law places the Ministry of Defense in charge of planning and implementing the country's cybersecurity policy. A new agency that was created in direct response to the events of 2014 is the Cyber Security Council, an advisory group that hosts experts from the private, public, and academic sectors.[379] The major responsibilities of the Council are to:

> "(1) to prepare and submit proposals to the cyber security Community of Interest… regarding priorities, areas of focus for further activity, propose goals and means to achieve them; (2) to prepare and submit proposals to the CoI" (Community of Interest) "for wider public, private and research cooperation in the area of cyber security; (3) to analyse cyber security implementation methods and provide the CoI proposals for more effective management of cyber incidents; and (4) to submit the CoI with recommendations for strengthening cyber security."[380]

Lithuania's first *National Defense System Cybersecurity Strategy and Implementation Plan* was approved in December 2009, which was later updated and reapproved in 2013.[381] This document focuses on ensuring the continued security of the transfer of electronic information, the general protection of the state's cyber, and defense infrastructure.[382] One of the most recognizable initiatives was the establishment of CERT-LT by the Ministry of Defense. As the main Lithuanian cyber institution, CERT-LT, otherwise known as the National Cyber Security Centre at the Ministry of National Defense (NCSC), is "responsible for unified management of cyber incidents, monitoring and control of the implementation of cyber security requirements, accreditation of information resources."[383] Having first begun operations on 1 January 2015, the NCSC's objectives are to: implement national cyber security policy, function as the protection service for national communications, provide research and analysis of cybersecurity issues, and perform information dissemination, among others. In 2018, the agency expanded its

---

[378] Butrimas, Vytautas. (2015). "National Cyber Security Organization: Lithuania" (Publication). Retrieved 4 January 2021. p. 9. NATO Cooperative Cyber Defense Centre of Excellence. https://ccdcoe.org/library/publications/national-cyber-security-organisation-lithuania/
[379] Ibid
[380] Ibid, pp. 9-10.
[381] Ibid, p. 11.
[382] Ibid
[383] "National Cyber Security Centre." (n.d.). National Cyber Security Centre. Retrieved 4 January 2021. https://www.nksc.lt/en/

responsibilities to provide assistance to not only other state agencies, but also private businesses and the general public at large.[384] Other notable state security initiatives include the SVDPT-CERT, a computer emergency response team affiliated with the Secure State Data Communication Network and the LTU MOD CIRT, another computer response team that is part of the Ministry of Defense.[385] Cooperation with Latvia and Estonia is also an important part of Lithuania's cybersecurity activities and has been since 2009, when the Ministry of Defense began conducting meetings and consultations with Latvian and Estonian officials. Additionally, Lithuania is one of the founding nations of the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn.[386]

Lithuania does not have a general, specialized crisis management law that recognizes a crisis(es) brought on by a cyber-attack. Select state ministries and their affiliated institutions are tasked with formulating a response to any cyber incident. Though each respective agency and sub-institution are well equipped, there still remains logistical problems that can hinder the state's response, which in terms of a cyber incident, can be devastating to the cyber infrastructure (in a short period of time), depending on the severity and scale of the attack. To better rectify these issues, the Lithuanian government approved a concept for the Law on Crisis Management, which intends to build a system that is more in line with those of NATO and the EU for responding to potential cyber crises.

As mentioned previously, cooperation between the public and private sectors is an integral aspect for creating a secure cyber environment. Though there is much yet to be accomplished, this relationship is growing and is an on-going process. Task forces and work groups have been formed in the past in attempts of addressing specific questions and aspect of cybersecurity, such as a temporary group that was created by the Ministry of the Interior that was asked to propose protocols and policy suggestions in responding to cyber incidents.[387] Also, the Academy of Science of Lithuania held a conference in November 2014 that hosted experts from

---

[384] Ibid

[385] "Cyberwellness Profile Lithuania." (n.d.). International Telecommunication Union. Retrieved 5 January 2021. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Lithuania.pdf

[386] Butrimas, Vytautas. (2015). "National Cyber Security Organization: Lithuania" (Publication). Retrieved 4 January 2021. p. 11. NATO Cooperative Cyber Defense Centre of Excellence. https://ccdcoe.org/library/publications/national-cyber-security-organisation-lithuania/

[387] Ibid, p. 13.

the public, private, and academic sectors.[388] Though there are no guarantees that policy solutions will be implemented from those suggested by these groups or that they will be adopted into policies at all, there is an increase in dialogue and understanding between the different sectors that did not exist in large part before. The Cyber Security Council is a possible organization that could influence the public-private-academic cooperation in coming years, though this is far from assured.[389]

Initiatives for the promotion, training, and education aspects of cybersecurity are developing in Lithuania and are still considered at a "formative stage of maturity."[390] Though programs and other resources, such as seminars and online content exists for various groups in society, the awareness level that Lithuanian society as a whole has regarding cybersecurity generally differs from the one that businesses and working professionals have.[391] Unsurprisingly, this is most likely due to the presence of digital technologies and education level that this demographic has in addition to a greater understanding of the effects cyber-attacks can have not only on the business environment, but also throughout society. A national program for cybersecurity awareness has not yet been implemented in Lithuania and it is not clear who would take the lead if one were (private or public sector-led). The current *Lithuanian National Cybersecurity Strategy*, implemented in 2018, lists several major points of emphasis, one of which is the promotion of cybersecurity culture and advancement of innovation.[392] A lack of cyber awareness has led to many instances of cyber insecurity, where workers have unknowingly exposed their workplaces to cyber threats. This fact is confirmed in an IBM report released in 2017, which states that the number of cyber incidents due to employee negligence have been on the rise. From 2016 to 2017, the number of these incidents increased by more than five percentage points (from 15% to more than 20%) with more than 30% occurring when employees

---

[388] Ibid
[389] Ibid
[390] Bada, Maria., & Weisser, Carolin. (2017, August). "Cybersecurity Capacity Review: Republic of Lithuania" (Report). p. 7. Retrieved 4 January 2021. Global Cyber Security Capacity Centre; Oxford Martin School, University of Oxford https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf
[391] Ibid
[392] Lithuania, Ministry of National Defense. (2018, 13 August). "National Cyber Security Strategy." p. 12. Retrieved 5 January 2021. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/programme-for-the-development-of-electronic-information-security-cyber-security-for-2011-2019-2011

opened malicious links or documents sent via email containing malicious content.[393] According to the current version of the *Cyber Security Strategy*, "the number of emails created using social engineering methods has also been rising."[394]

Efforts have been focused on increasing professional training opportunities for both the public and private sectors. Civil servants are being offered more opportunities to increase their competencies in cyber skills and cybersecurity, which has proven popular among these workers. In 2015, 146 civil servants partook in training programs, a number that increased to 249 in 2015 and 289 in 2017.[395] There is hope that increased training opportunities in the public sector will translate to a more secure public cyber environment in future years and enhance the capabilities of public response institutions, such as CERT-LT. Private sector businesses have increased their understanding of cybersecurity and what the implications are for an unsecured business environment. The European Innovation Scorecard states that the private sector in Europe has focused on increasing ICT training for employees. In Lithuania, this trend is lagging behind the European average index (21% vs. 10% in Lithuania).[396] While employees may benefit from increased training programs, there are currently no requirements in Lithuania that require CEOs to receive specified training.[397]

In the education sector, Lithuanian universities are offering degree programs in cybersecurity to better educate a workforce that can adequately provide for and respond to cyber incidents. Currently, there are four universities offering degree programs at both the bachelor's and graduate levels in cybersecurity or cyber-related fields (Vilnius University, Vilnius Gediminas Technical University, Kaunas University of Technology, and Vytautas Magnus University).[398] Though these efforts have undoubtedly aided in this objective, there is still a demand for cybersecurity professionals that is not being met under current conditions. Studies have indicated that this gap is significant and will require approximately 13,000 new

---

[393] Ibid
[394] Ibid
[395] Ibid
[396] Ibid
[397] Bada, Maria., & Weisser, Carolin. (2017, August). "Cybersecurity Capacity Review: Republic of Lithuania" (Report). p. 7. Retrieved 4 January 2021. Global Cyber Security Capacity Centre; Oxford Martin School, University of Oxford. https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf
[398] Lithuania, Ministry of National Defense. (2018, 13 August). "National Cyber Security Strategy." p. 13. Retrieved 5 January 2021.

cybersecurity professionals in the next few years to supplement the existing workforce, which numbers approximately 22,600 ICT specialists.[399] Proposals have been made that would provide cybersecurity knowledge to school-aged children, beginning in nursery school and continue throughout a student's educational career into primary and secondary school.[400] The current *Lithuanian Cyber Security Strategy* also states that efforts should be made to enhance teacher-training programs in cybersecurity. It claims that this would not only benefit students but would further advance knowledge and innovation, helping increase the general cybersecurity literacy of society.[401]

Lithuania's membership in NATO and the EU have also aided in the country's aims of providing for a secure cyber environment. NATO's commitment to ensuring the cyber integrity of its allied member states has allowed for a sense of relief for officials in the Baltic states. Additionally, NATO has promised to treat cyberwar with the same significance that the alliance would treat traditional military threats against all of its member states. While NATO's assistance has primarily been one of defense, the EU has provided many opportunities for Lithuania in the financing and promotion of scientific research and innovation through its *Horizon 2020* program (2014-2020). The program has allowed Lithuania to contribute to the digital economy on the national and supranational (EU) level, though restrictions are placed on the direction of state measures, which must be focused on support "that promote international networking in finding potential employees and partners," which advances research and development objectives in the cyber realm.[402]

The Lithuanian Psychological Space in the 21st Century

The threats posed by Russia's information warfare operations are an ever-present reality for Lithuania. The traditional concepts of literacy, which once focused primarily on proficiency in reading and writing, have been expanded upon in many countries to include competencies in digital technologies and critical analysis of information sources. For Lithuania, the desire to

[399] Ibid
[400] Ibid
[401] Ibid
[402] Ibid

develop a media literate society has increased over the last several years, with increased urgency coming after the success of Russia's information operations in Ukraine in 2014 and subsequent annexation of Crimea. Despite these aspirations, there are significant obstacles that must be overcome to best ensure this objective. Major obstacles include the lack of availability of digital technologies across age and demographic lines, and a general lack of political will to institute major initiatives at the state level, despite the necessity of media education programs.

Though mitigating measures have been implemented and security strategies enforced, the sophistication of modern-era Russian disinformation requires more than technical and bureaucratic actions to adequately provide for Lithuania's security environment. As mentioned in the previous section, the recent cyber-attacks against the websites of several municipal government agencies and the posting of misinformation have showcased that these means alone are insufficient to safeguard Lithuanians from hostile information warfare operations. Lithuania has prioritized media education as a significant aspect of its safeguarding initiatives, with media literacy being considered a hot topic.[403] Despite these desires, media literacy education is still developing and is unevenly applied throughout different sectors of society.

It is important to note the differences between media education and media literacy, the terms sometimes used interchangeably. Though the terms may be similar, the concepts associated with them have often been quite different in their educational objectives. Media education is generally referred to as an overarching educational concept that includes the teaching of both technical skills and media content analysis. Until recently, media education almost exclusively focused on the technical aspects of digital technologies in many countries, including the Baltic states. Later, criticism came that media education was incomplete and not adequately preparing students to discern fact from fiction. This was internalized by policymakers in many countries, who added various forms of media literacy to national educational curriculums. The aim was to teach students analytical and critical thinking skills in addition to technological ones. Issues related to the offerings of media education and media literacy in colleges and universities were less apparent. In time, postsecondary institutions began to

[403] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index*. p. 205. Retrieved 6 January 2021. http://prismua.org/en/dri/

embrace media education and add it to their curriculums, emphasizing "the importance of the impact of media usage on 'lived society.'"[404]

Historically, Lithuania's media literacy initiatives have focused almost exclusively on teaching digital technical skills along with the development of new technologies, a focus that was reflected in the state's educational document *E-School Program Education for Information Society*.[405] Programs such as this were implemented from 2002-2005, primarily to provide digital technologies to schools and to increase the digital competency level for teachers.[406] For the most part, this largely remained a common practice for several years, when a more comprehensive approach was implemented. The national planning strategy *Lithuania 2030*, adopted by the Seimas in 2012, seeks to promote a national vision and sets priorities proposed by both the public and private sectors as well as civil society organizations.[407] In reference to media literacy, the strategy aims "to introduce media literacy programmes in all education institutions."[408]

One of the most recognizable forms of media education in Lithuania has centered on media literacy initiatives directed towards primary and secondary students. While this demographic continues to receive much attention, the perspective on media education has been broadened to include colleges and universities, and the wider society. Initiatives are focused on increasing media literacy rates among this demographic. A major step came in 2006 when the Ministry of Education and Science implemented a nationwide program for high school students, *Teaching about Information Processes and Human Rights*.[409] The program's description:

---

[404] Šuminas, Andrius., & Jastramskis, Deimantas. (2020). "The importance of media literacy education: How Lithuanian students evaluate online news content credibility." Central European Journal of Communication, 13(2), p. 231. Retrieved 6 January 2021. https://www.researchgate.net/publication/342203091_The_importance_of_media_literacy_education_How_Lithuanian_students_evaluate_online_news_content_credibility

[405] "WP3. Formal Media Education Lithuania." (n.d.) (issue brief). EMEDUS Europe Media Education. Retrieved 6 January 2021. http://www.gabinetecomunicacionyeducacion.com/sites/default/files/field/investigacion-adjuntos/lithuaniad.pdf

[406] Ibid

[407] Juraite, Kristina. (2014, May). "Media and Information Education Policies in Lithuania" (Report). p. 3. Retrieved 6 January 2021. Vytautas Magnus University. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/LITHUANIA_2014.pdf

[408] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index*. p. 205. Retrieved 7 January 2021. http://prismua.org/en/dri/

[409] Juraite, Kristina. (2014, May). "Media and Information Education Policies in Lithuania" (Report). p. 5. Retrieved 6 January 2021. Vytautas Magnus University. http://ppemi.ens cachan.fr/data/media/colloque140528/rapports/LITHUANIA_2014.pdf

> "…is to develop information literacy among 9-11 grade students by encouraging students' critical thinking and the ability to use media, the Internet and other information, advertising and entertainment sources, while fostering students' awareness, civic and cultural maturity, social skills. Students' ability to understand the phenomena of the mass audience will not only help to develop their thinking and awareness, but also to bring their individual needs with the opportunity to evaluate everything they read and see."[410]

Additional learning objectives included instruction in technical competencies, such as how to use the internet, and how to interpret advertising and entertainment through the perspective of civic, social, and cultural skills.[411] The program was a major initiative, especially regarding the study of media content. Involvement of non-state groups was also notable, which included the Commission of Journalists and Editors Ethics, Education Development Center, and the Modern School Center, an NGO.[412] Reports published in the early 2000s indicated that there was a need to add media education programs to the national educational curriculum. Though initially well-intentioned, a lack of trained professionals, contrasting views on media education, and the late 2000s financial crisis prevented any significant adoption by educational institutions.

To determine the media literacy level of Lithuanians, the Lithuanian Ministry of Culture initiated a survey to measure the media literacy competencies of society. Based on the state document *The Methodology of Media Literacy Research*, the study indicated that the general population lacked the critical analytical skills necessary for media consumption. The survey also noted that "fake news is rarely noticed" and the media in general is not seen as a significant instrument of influence. They ultimately concluded that the analytical skills of Lithuanians were most to blame for the findings, not the quality of media content.[413] Efforts to further measure the media literacy levels of Lithuanians will aid in planning strategies and help direct funding and other resources to areas in need of improvement. Future surveys will be regularly conducted, the latest of which took place in 2020.[414]

---

[410] Ibid
[411] Ibid
[412] Ibid, p. 6.
[413] "Survey on Media Literacy Level in Lithuania." (2020, 17 April). en.unesco.org. Retrieved 7 January 2021. https://en.unesco.org/creativity/node/19648
[414] Ibid

Most often, media education activities are offered via a mix of public, private, media, and NGO initiatives. The events in Ukraine spurred the Baltic states into implementing security measures to guard themselves against the possibility of a Russian attack, militarily or otherwise. From 2014-2015, the most significant media literacy initiative was implemented by the Education Development Centre, aided by the Ministry of Education and Science, and the Nordic Council of Ministers Office in Lithuania.[415] To make up for the shortcomings of previous media literacy efforts, the project's aim was to create a centralized system that would formulate materials to be integrated into other aspects of the primary school curriculum. Literacy efforts continued in 2016 and 2017 when the National Institute of Social Integration created programs that were aimed at sharpening critical thinking skills and media literacy programs in general.[416] Much like non-governmental efforts in Estonia (Media Bubble), 90 students from 45 schools across Lithuania met and participated in professional trainings, culminating in an event known as the Critical Thinking Festival.[417] Additionally, more professional gatherings such as this have been planned by the Education Development Centre, which are mostly aimed at primary schools, in the hopes of sparking interest and further engaging students in media education initiatives. Media literacy efforts aimed at adults have been discussed but have not been met with the same enthusiasm that they have for school and university-aged students. Though no initiatives have been formally implemented, discussions have largely centered on marketing alternative sources of information to adults, especially older ones. One idea is to label Russia-based content as untrustworthy, though there have not been significant discussions for adult-oriented literacy initiatives.

International cooperation has proven successful in providing guidance for psychological security efforts, which can be conformed to the specific needs and requirements of Lithuania. The notion of psychological defense, and more broadly, psychological security, comes from Sweden, which has offered its assistance to countries seeking to provide a broad scope of security.[418] According to Lithuanian Ministry of Defense policy director Vaidotas Urbelis,

---

[415] Denisenko, Viktor. (chapter author). (2018). "Lithuania." In *Disinformation Resilience Index*. p. 206. Retrieved 7 January 2021. http://prismua.org/en/dri/
[416] Ibid
[417] Ibid
[418] In-depth interview with Nerijus Malikevicius [Online interview]. (2020, 25 July).

"Sweden is essential for the defence of the Baltic[s]."[419] Psychological defense originated as Sweden's way of responding to psychological warfare efforts that an enemy was could possibly utilize during warfare operations. The concept has outlasted all competing concepts and consists of three major components:

1. The countering of disinformation and deceptive information, which includes propaganda and rumor-mongering[420]
2. To ensure that state officials are able to successfully convey essential information during times of war or crisis[421]
3. To enhance society's resiliency and strengthen resolve to defend the country[422]

The effectiveness of psychological defense ensures that society is not only prepared during times of war or crisis, but to defend a homeland during peacetime. Enhancing communications strategies, ensuring a resilient communications infrastructure, supporting NGOs, implementing media literacy into educational curriculums, and researching the intricacies of society are some of the recommendations that have been proposed to fit Lithuania's security needs and its broader security environment. Additionally, the relationships that exist between state agencies and media organizations are also an integral part of psychological security. Swedish government agencies and media outlets regularly confer, and information is exchanged, which builds trust and establishes lines of communication during periods when it is integral for the protection of national security.[423]

NGOs and private initiatives also play a vital role in media literacy and psychological security. While the benefits of these organizations are noticeable and the effects long-lasting, Lithuania's NGOs do not always collaborate with each other, and fact-checking organizations

---

[419] "What defence help do the Baltics want from Sweden?" (2015, 12 February). Radio Sweden. Retrieved 7 January 2021. https://sverigesradio.se/artikel/6092292

[420] Rossbach, Niklas. H. (2017, November). "Psychological Defence: Vital for Sweden's Defence Capability" (Issue brief). pp. 1-2. Retrieved 7 January 2021. The Swedish Defense Research Agency. https://www.foi.se/rest-api/report/FOI%20Memo%206207

[421] Ibid

[422] Ibid

[423] "Lithuanian-Swedish Roundtable Expert Discussions on Social Resilience and Psychological Defence" (Issue brief). (2018, September). p. 9. Retrieved 7 January 2021. European Integration Studies Centre. http://www.eisc.lt/uploads/documents/files/EISC_policy%20brief(1).pdf

are often in a similar position. Increased cooperation and the concentration of resources would likely provide a needed boost to the reach and effectiveness of these groups, practices that are undertaken in Sweden. The Lithuanian government has not implemented a national, society-wide program, though NGOs are working to fill the gap. Unlike Latvia and Estonia, Lithuania offers media literacy in Russian- and Polish-language schools, though this it is not part of the current Lithuanian secondary school curriculum. Organizations such as the Lithuanian Journalists Union, Human Rights Center, National Institute for Social Integration, Art Hive, Teacher Professional Development Center, and Transparency International Lithuania are all active in media literacy efforts, both directly and indirectly.[424] Activities include moderating public discussions, hosting professional trainings for journalists and teachers, as well as publishing materials and conducting public awareness campaigns.[425] Strengthening NGOs has proven beneficial in Sweden as it has boosted civic participation and empowers citizens to strengthen and defend their country, especially in regard to soft-power initiatives.

Lithuania summary

The security environment that exists in Lithuania differs somewhat from its Baltic neighbors, especially concerning information security. Demographically, Lithuania is more homogenous than Latvia or Estonia and has traditionally been more forceful in its official statements against Russian's actions in the region. The country's information space has reflected the demographic situation with most media being only offered in Lithuanian, though there has been an increased offering of minority language media aimed at the small Polish and Slavic populations. Showcasing that fighting Russian information operations is a whole-of-society endeavor, Lithuanian "elves" have played an increasingly important role in ensuring the vitality of the information space by reporting and highlighting false, hostile, or misleading narratives posted by Russian "trolls" to the proper authorities and the general public. The competencies of Lithuanian cyber officials and civil servants have been increased to guard against malicious cyber incursions while state and private enterprises have been involved in cooperative efforts to

[424] Juraite, Kristina. (2014, May). "Media and Information Education Policies in Lithuania" (Report). p. 10. Retrieved 6 January 2021. Vytautas Magnus University. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/LITHUANIA_2014.pdf
[425] Ibid

offer technical assistance and professional expertise in securing the country's cyber infrastructure. To ensure the psychological security of Lithuanians, state officials have turned to international cooperation to find strategies that offer a broad level of protection. The concept of "psychological defense" comes from Sweden and has become an important aspect of information, psychological, and social security. Strengthening the relationships between the public and private sector is integral in maintaining the lines of communication, understanding, and trust, which are essential during times of crisis. Media literacy efforts need to be increased and enhanced to have a more significant impact. However, the security efforts that have been implemented do show indications of having long-term impacts on the information, cyber, and psychological environments. Increased cooperation, both domestically, regionally, and internationally have brought positive results and the desire to attempt new and innovative proposals may also increase the level of security in these sectors.

Recommendations

After conducting research for this thesis and gaining a better understanding of the security environments of the Baltic states, I have formulated several recommendations that may improve upon the current security situation in the region. I have chosen to organize my recommendations to showcase the most innovative initiatives in each country. Criteria for the selection process consisted of the analysis of policies, protocols, technological achievements, or educational initiatives that could be considered innovative for the security need they fill. Additionally, the adaptability and expandability of these measures was also considered, not only for the other Baltic states, but for countries throughout the world. In line with the topic of my thesis, these security initiatives concern the information, cyber, and psychological realms. Though there are many soft power security measures that have been debated or implemented in the Baltic states, the following are measures that I have found to be particularly unique and innovative.

The vitality of Estonia's information space differs from that of its Baltic neighbors, in that public trust in media has been maintained. The launch of ETV+ in 2015 signals that Estonian officials understand the consequences of having two spheres of influence, and the opportunity this provides Russia to exert undue influence over Russophiles. Though ETV+'s launch came well after many Russophiles had firmly established viewing habits with Russia-based channels, the establishment of an Estonian-based Russian language channel programmed with local content has proven somewhat successful. Initial ratings figures were low, but they have noticeably risen during the coronavirus pandemic. This is likely due to the vital local information broadcast on the channel that is not featured in Russia-based programming.

The development and implementation of digital technologies has proven successful at establishing Estonia as a global leader in technology and cybersecurity development. The country's X-Road initiative has allowed Estonians greater access to secure state services. The decentralized nature of the system provides for a greater level of security than would a centralized one and allows businesses easy access to financial and tax services, both those based in Estonia and those abroad through the country's e-residency initiative.

The security of Estonia's psychological environment is due in part to several factors, but one of the initiatives that has proven successful are the media literacy efforts aimed at school-

aged students. Though existing media literacy programs are by no means perfect, NGO initiatives, such as Media Bubble, a program aimed at secondary school students, allows them to participate in competitions against other schools to create compelling media content and receive guidance from journalism faculty from the University of Tartu. Actively engaging students, building analytical and critical thinking skills, and encouraging students to consider careers in journalism has laid a foundation upon which students can become media literate members of society and better understand the media's role in a democratic government.

Providing for a secure information environment has been important to Latvian authorities, who seek to close the gap between the Latvian and Russian information spheres. Investments in television channels LR4 and LTV, and in public radio broadcasting, have been made to achieve this objective. Bureaus established in border areas allow for media content to be distributed nationwide, and greater physical coverage has provided for better comprehension of the issues happening elsewhere in Latvia.

Responding to cyber threats has been a challenging endeavor in the digital age. Latvia has experienced a huge number of cyber incidents in previous years and has tasked the Information Technology Security Incident Response Institution, otherwise known as CERT.lv to respond to and defend against malicious cyber incursions. In addition to providing protection to state agencies, the private sector also benefits from their activities as well. CERT.lv provides penetration tests to prevent future cyber-attacks and educates thousands of government employees, students, and even the general public every year.

Latvia's psychological space, though not as secure as Estonia's, has seen some improvements in the past few years. Though state involvement continues to be limited, efforts to obtain outside funding and support from philanthropic and educational initiatives, such as the Bill and Melinda Gates Foundation, has provided funding, professional training, and technical assistance. This benefits Latvian schools, universities, and the general public. Private sector involvement has also allowed for additional resources to be allocated to media education efforts.

Lithuania's information space faces many of the same threats as its Baltic neighbors. However, early on, thousands of ordinary citizens took the responsibility to patrol the internet looking for dubious sources of information. This volunteer force of cyber warriors, known as "elves," actively monitors the county's online and social media environments for possible

disinformation, and hateful and defamatory content posted by Russian "trolls." Tens of thousands of online articles are analyzed daily with content likely posted by trolls being reported to social media authorities, news organizations, or to fact-checking initiatives to debunk false or misleading narratives.

The Lithuanian cyber environment has been vulnerable due to the lack of awareness from civil servants on the methodologies and implications of malicious links and emails targeting state agencies. Professional and continuing education courses are being increasingly offered to civil servants to better educate them on the cyber threats that are designed to fool them and the implications this has for the whole of Lithuania's cyber space. By educating civil servants of all levels, this raises the security awareness over a wide swath of society.

Ensuring that Lithuania's psychological security is adequately provided for has become an increasingly important concern among state officials. The close relationship that Lithuania has with Sweden has allowed for outside perspectives to enter the psychological security dialogue, which includes the concept of psychological defense. A long-running practice within Sweden, this doctrine states that increased communication between media and government provides a system where critical messages can be transmitted to communicate with citizens. Media literacy and the countering of information warfare efforts are also an integral aspect of this doctrine, which allows citizens to maintain trust in the state and enhance the willingness of society to strengthen and defend the country.

Conclusion

The security environments in which the Baltic states emerged three decades ago have changed significantly and have required a broadening of the concept of security from traditional hard-power forms to soft-power, entire society efforts. The willingness of Russia to utilize information warfare, though not a new phenomenon, has been well documented. This has been responsible, either wholly or in part, for the destabilization of many countries throughout Europe and the post-Soviet region. Russia's information warfare playbook has been successfully modernized in the 21st century and remains a major aspect of the country's foreign policy. The implications of an inadequate security environment were displayed most notably in Russia's actions in Ukraine in 2014. This acted as a catalyst for the Baltic states to invest in non-military security measures that had only been met with varying levels of support prior. The success of Russia's information operations in Georgia and Ukraine led to efforts by the state, the private sector, educational institutions, NGOs, and civil society to bridge the gaps in the Baltic states' security environments.

The multitude of soft-power efforts listed in this thesis by Estonia, Latvia, and Lithuania, highlight the wisdom of Buzan in widening the traditional concepts of security out of the hard-power realm into society as a whole. In 2015, then-National Defense Minister, Juozas Olekas, noted that the 2002 *National Security Strategy* was outdated and added that, "New challenges, including hybrid warfare, cyber and international challenges, and a changed geopolitical situation have emerged."[426] The tragedy of Georgia, Ukraine, and Crimea, need not be repeated, but the solutions begin at home.

Many efforts have been focused on uniting the various ethnic groups in each country. These have been met with varying levels of funding, political support, and effectiveness. Baltic-based minority language media has been funded in Estonia, Latvia, and Lithuania, and media education, and more specifically media literacy, has been considered a necessity to enhance the analytical and critical thinking skills of citizens. While most of these efforts have focused on traditional school-aged students, there have been calls to expand these initiatives to the broader

[426] "Lithuania to draft new National Security strategy." (2015, 27 October). The Baltic Times. Retrieved 29 December 2020. https://www.baltictimes.com/lithuania_to_draft_new_national_security_strategy/

population. Unfortunately, media education is not uniform across the Baltic states and it varies in quality and implementation in each country. Philanthropic and global technology initiatives have also provided funding and technical support to close the existing gaps caused by a lack of state funding and/or political initiative. While the 21st century has brought a wide range of technologies that benefit the Baltics, it has also ushered in many threats that come from an increasingly interconnected world. Cyber-attacks have risen exponentially in the last two decades. To combat these incursions and limit the damage of future ones, state agencies have created specialized cyber units to provide assistance to the public, private, and educational sectors. The private sector has increasingly offered its cooperation to provide resources, technical support, and innovation.

While much still needs to be done to secure the deficiencies in the information, cyber, and psychological environments, the measures that have been implemented give hope to officials throughout the region that the long-term benefits will produce countries that will be vibrant members of the European and international communities, and that they will be able to resist the hostile actions and undue influence from their eastern neighbor.

Summary

The topic of my thesis is how the Baltic states are expanding the security environment to adapt to the information, cyber, and psychological environments. My primary research question aims to answer what actions each of Baltic states are undertaking to guard against Russian and Russian affiliated hybrid warfare efforts. I also aim to research not only what these efforts and initiatives consist of, but what the implications are for not providing adequate security measures; how hostile actors can exploit gaps in these respective environments; and to provide recommendations to guard against these Russian incursions.

The rapid advancement of digital technologies in the 21st century has altered the information, cyber, and psychological environments in countries throughout the world and has ushered in an era of non-traditional, asymmetrical warfare operations conducted against the Baltic states by Russia and its affiliated actors. The practices of Soviet-era information warfare have not changed significantly but have been modernized to fit an ever-expanding digital space. Russia's willingness to engage in information warfare has been well documented and has led to the destabilization of many countries, not only in the region, but throughout Europe and beyond. The options that hostile actors now have in interfering in the affairs of other countries in the digital era are seemingly unlimited and have increasingly blurred the lines between what does, and does not, constitute a threat. Because of these technological advancements, countries have been forced to implement security measures to safeguard non-traditional aspects of security, such as the information, cyber, and psychological spaces. The shared experiences that Estonia, Latvia, and Lithuania have had with their eastern neighbor provide an understanding as to the current methodologies, geopolitical aspirations, and the implications that exist, and what measures must be implemented to successfully safeguard their societies from hostile information and cyber threats.

Each of the Baltic states has its own unique characteristics that dictate what measures are considered and enacted, though there exists much overlap in these strategies. The competing spheres of influence in the Baltics, which are largely based on ethnic and linguistic lines, have provided Russia many opportunities to exert its influence in the region. Media programming efforts, which often focus on local issues, have offered an alternative source of information than those that emanate from Russia.

Cyber-attacks, such as the ones undertaken during the Bronze Night events in Estonia in 2007, showcase the negative consequences that can affect countries in the online environment, which can greatly hinder the delivery of state and business services.

The ability of Baltic citizens to discern fact from fiction has become a vitally important skill to guard against information warfare threats. The number and sophistication of these threats has increased in recent years and will continue to do so in the future. Media education initiatives have been expanded to include media content analysis and enhancing critical thinking skills in the hopes that these initiatives will provide citizens with the cognitive abilities to reason and decide what information is factually accurate. State, private, NGO, philanthropic, and civil society initiatives have all offered instruction, funding, technical support, or other forms of aid in conducting media literacy courses.

LIST OF LITERATURE

Introduction

Laurinavicius, Marius. "A Guide to the Russian Tool Box of Election Meddling: A Platform to Analyse the Long Term Comprehensive Kremlin Strategy of Malign Influence." International Elections Study Center. 4 December 2018. Retrieved 17 October 2020. http://iesc.lt/app/uploads/2018/10/IESC_Guide_ToolBox_2018_FINAL.pdf

Marler, Scott W. "Russian Weaponization of Information and Influence in the Baltic States." Master's thesis, U.S. Army Command and General Staff College, 2016. Leavenworth, Kansas: U.S. Published: Army Command and General Staff College. Retrieved 17 October 2020. www.apps.dtic.mil/dtic/tr/fulltext/u2/1038780.pdf.

Buzan, Barry, "New Patterns of Global Security in the Twenty-first Century" International Affairs, 673 (1991). pp. 432-433. Retrieved 26 December 2020.

"Lithuania to draft new National Security strategy." (2015, 27 October). The Baltic Times. Retrieved 29 December 2020. https://www.baltictimes.com/lithuania_to_draft_new_national_security_strategy/

Chapter 1--Estonia

Bahovski, Erkki. "First Steps towards the Estonian Media Space." 2 April 2020. Retrieved 19 November 2020. https://icds.ee/en/first-steps-towards-the-estonian-media-space/

Barnett, Genna. (2019, February 25). "Digital Frontrunners Spotlight: Estonia." Nesta. Retrieved 4 December 2020. https://www.nesta.org.uk/blog/digital-frontrunners-spotlight-estonia/

"Cyber security." Estonia Ministry of Economic Affairs and Communication. 2020, 15 April. Retrieved 2 December 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

Cybersecurity Strategy." (Publication). Republic of Estonia Ministry of Economic Affairs and Communications. 2019. Retrieved November 10, 2020. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

"Cybersecurity Strategy 2019-2022." Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

"e-Estonia." (n.d.). Wikipedia. Retrieved 4 December 2020. https://en.wikipedia.org/wiki/E-Estonia

"Enterprise Estonia." (n.d.). Retrieved 4 December 2020. https://www.eas.ee/eas/?lang=en

"Estonia: Lifelong Learning Strategy 2020, issued in 2014." (n.d.). UNESCO Institute for Lifelong Learning. Retrieved 4 December 2020. https://uil.unesco.org/document/estonia-lifelong-learning-strategy-2020-issued-2014

Estonia, Ministry of Defense, Cyber Security Strategy Committee. (2008). Retrieved 28 November 2020. www.enisa.europa.eu › cyber-security-strategy › file_en

Estonia, Ministry of Economic Affairs and Communication. (2019). Retrieved 30 November 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

"Estonia's Constitution of 1992 with Amendments through 2015." [Scholarly project]. 20 July 2020. pp. 3-4. constituteproject.org. Retrieved 18 November 2020. https://www.constituteproject.org/constitution/Estonia_2015.pdf?lang=en#:~:text=Everyone%20has%20the%20right%20to,also%20protect%20its%20citizens%20abroad.&text=The%20guarantee%20of%20rights%20and,powers%2C%20and%20of%20local%20governments.

Gold, Josh. "How Estonia uses Cybersecurity to Strengthen its Position in NATO." 26 May 2019. Retrieved 26 November 2020. https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/

"Interoperability Services." (n.d.). Retrieved 29 November 2020. https://e-estonia.com/solutions/interoperability-services/x-road/

Joesaar, Andres. "Day After: The Impact of the Launch of the Russian-Language Television Channel ETV+ on Estonian Public Broadcasting's Viewing Trends." 2017. Vol. 2. Report. Tallinn University. Retrieved 18 November 2020. https://www.researchgate.net/publication/318984136_DAY_AFTER_THE_IMPACT_OF_THE_LAUNCH_OF_THE_RUSSIAN-LANGUAGE_TELEVISION_CHANNEL_ETV_ON_ESTONIAN_PUBLIC_BROADCASTING'S_VIEWING_TRENDS

Jõesaar, Andres. (2015). "One Country, Two Polarised Audiences: Estonia and the Deficiency of the Audiovisual Media Services Directive." Media and Communication, 3(4), pp. 1-6. Retrieved 3 December 2020. https://pdfs.semanticscholar.org/38f6/d671542ae68441fe955389cb8fbaa612bfbb.pdf?_ga=2.141431218.1454955638.1606971130-1000744679.1606971130

Joesaar, Andres, Rannu, Salme, & Jufereva, Maria. (2013). "Media for the Minorities: Russian Language Media in Estonia 1990-2012." Media Transformations. Retrieved 22 November 2020. https://www.vdu.lt/cris/handle/20.500.12259/31465

Kepe, Marta, & Osburg, Jan. "Total Defense: How the Baltic States are Integrating Citizenry into their National Security Strategies." Small Wars Journal. 24 September 2017. Retrieved 11 November 2020. https://smallwarsjournal.com/jrnl/art/total-defense-how-the-baltic-states-are-integrating-citizenry-into-their-national-security-

Lavrentjev, Ivan. (2020). "The Securitization of Russian-speaking Media in Estonia: Case Study of ETV+ Channel." Master's thesis, University of Helsinki. University of Helsinki. Retrieved 23 November 2020. https://helda.helsinki.fi/bitstream/handle/10138/316401/Lavrentjev_Ivan_thesis_2020.pdf?sequence=3

Loit, Urmas, & Harro-Loit, Halliki. "Media Pluralism Monitor 2016 Monitoring Risks for Media Pluralism in the EU and Beyond." Report. pp. 4-12. December 2016. Retrieved 18 November 2020. Centre for Media Pluralism and Media Freedom. https://cadmus.eui.eu/bitstream/handle/1814/46794/Estonia_EN.pdf?sequence=1&isAllowed=y.

Meister, Stefan. (Ed.). (2018). "Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia" (ifa Edition Culture and Foreign Policy). Stuttgart: ifa (Institut für Auslandsbeziehungen). https://nbn-resolving.org/urn:nbn:de:0168-ssoar-59979-0

Pernik, Piret, & Tuohy, Emmet. (2013, August). "Cyber Space in Estonia: Greater Security, Greater Challenges." Report. Retrieved 2 December 2020, from International Centre for Defense Studies website: https://icds.ee/en/cyber-space-in-estonia-greater-security-greater-challenges/

Siibak, Andra, Ugur, Kadri, & Vinter, Kristi. (2014, May). "Media and Information Literacy Policies in Estonia" (Publication). Retrieved 4 December 2020, from University of Tartu, Institute of Journalism and Communication. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/ESTONIA_2014.pdf

Teperik, Dmitri (section author). "Estonia" (2018). Disinformation Resilience Index (Publication). Retrieved 3 December 2020. http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf

Turp-Balazs, Craig. (2018, April 3). "Estonia is Emerging Europe's Most Media Literate Country." Retrieved 4 December 2020. https://emerging-europe.com/news/estonia-emerging-europes-media-literate-country/#:~:text=A%20major%20new%20study%20by,both%20the%20UK%20and%20Germany.

"The main tasks of the EDL CU." Estonian Defense League. (2020). Retrieved 2 December 2020. https://www.mkm.ee/en/objectives-activities/cyber-security#:~:text=The%20new%20Cybersecurity%20Strategy%20lays,all%20key%20competences%20for%20Estonia

Vihalemm, Peeter. (2006) "Media Use in Estonia: Trends and Patterns." Nordicom Review. p. 18. Retrieved 18 November 2020. https://www.researchgate.net/publication/47502946_Media_Use_in_Estonia_Trends_and_Patterns

Wallace, Savannah. (2020, 25 July). "Estonia: The First Digitally Literate Country." Medium. Retrieved 4 December 2020. https://medium.com/swlh/the-first-digitally-literate-country-e9dbc1d0695

"What is Propastop?" Propastop.org. (2017). Retrieved 7 December 2020. https://www.propastop.org/eng/2017/03/06/what-is-propastop/

"X-Road Introduction (short version)" [Video file]. 2016, 10 June. Retrieved November 29, 2020. https://e-estonia.com/solutions/interoperability-services/x-road/

Chapter 2--Latvia

"2018 Country Reports on Human Rights Practices: Latvia." (2018). United States Department of State. Retrieved December 2020. https://www.state.gov/reports/2018-country-reports-on-human-rights-practices/latvia/

"2019: CERT.LV Public Performance Report." (Report). (2020). Retrieved 18 December 2020. Information Technologies Security Incident Response Institution. https://cert.lv/uploads/parskati/certgada-atskaite-2019-EN.pdf

"Changes in Latvian Media Policy following Russia's Actions in Ukraine." [E-mail interview with Baltic Centre of Media Excellence Director Janis Siksnis]. (2020, 13 December).

"Crisis announced at Latvian Radio due to funding shortage." (2019, 15 July). Public broadcasting of Latvia. Retrieved 19 December 2020. https://eng.lsm.lv/article/society/society/crisis-announced-at-latvian-radio-due-tofunding-shortage.a325668/

"Cyber defense." (2020). NATO. Retrieved 18 December 2020. https://www.nato.int/cps/en/natohq/topics_78170.htm

Cyber Security Strategy of Latvia 2014-2018." (2014). Government of the Republic of Latvia. Retrieved 17 December 2020. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Fernandes, Sandra. (2018). "(Re)securitisation in Europe: The Baltic States and Russia." Debater a Europa. Retrieved 17 December 2020. https://www.researchgate.net/publication/322690589_Resecuritisation_in_Europe_the_Baltic_States_and_Russia

Garcia, Cynthia. (2018). "The Baltic Centre for Media Excellence: A Case Study on Media Literacy as a Tool Against Russian Disinformation." (Master's thesis). Tufts University. Retrieved 19 December 2020. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-

Kudors, Andis. (chapter author). (2018). "Latvia." In Disinformation Reilience Index. Retrieved 13 December 2020. http://prismua.org/en/dri/

Kupčs, Edgars. (2020, 18 December). "Pandemic shows serious shortcomings in Latvian media literacy." Retrieved 19 December 2020. https://eng.lsm.lv/article/features/media-literacy/pandemic-shows-serious-shortcomings-inlatvian-media-literacy.a385822/

"Latvia." (n.d.) Reporters without Borders. Retrieved 9 December 2020. https://rsf.org/en/latvia

"Latvia." (n.d.). Wikipedia. Retrieved 9 December 2020. https://en.wikipedia.org/wiki/Latvia

"Latvia: Cybercrime policies/strategies." (2020). Council of Europe. Retrieved 18 December 2020. https: www.coe.int/en/web/octopus/country-wiki-ap/-/asset publisher/CmDb7M4RGb4Z/content/latvia

Latvia, Ministry of Environmental Protection and Regional Development. (2013). "Information Society Development Guidelines 2014-2020." Retrieved 17 December 2020. https://www.varam.gov.lv/sites/varam/files/content/files/information_society_development_guidelines_2014_20.docx

Ločmele, Klinta. (n.d.). "Digital media." medialandscapes.org. Retrieved 17 December 2020. https://medialandscapes.org/country/latvia/media/digital-media

Ločmele, Klinta. (n.d.). "Overview." medialandscapes.org. Retrieved 10 December 2020. https://medialandscapes.org/country/latvia

Locmele, Klinta. (n.d.). "Print." Medialandscapes.org. Retrieved 16 December 2020.https://medialandscapes.org/country/latvia/media/print

Ločmele, Klinta. (n.d.). "Radio." medialandscapes.org. Retrieved 10 December 2020. https://medialandscapes.org/country/latvia

Ločmele, Klinta. (n.d.). "Television." medialandscapes.org. Retrieved 10 December 2020. https://medialandscapes.org/country/latvia/media/television

Rožukalne, Anda. (2016). "All the Necessary Information is Provided by Russia's Channels. Russian-language Radio and TV in Latvia: Audiences and Content." Baltic Screen Media Review, 4. Retrieved 14 December 2020. https://content.sciendo.com/configurable/contentpage/journals$002fbsmr$002f4$002f1$002farticlep106.xml

Rožukalne, Anda. (n.d.). "Media Audience Development in Latvia (2004-2012)." Media Transformations. Retrieved 17 December 2020. https://www.researchgate.net/profile/Anda_Rozukalne/publication/308046946_Media_audience_development_i n_Latvia_2004-2012/links/5992d56d0f7e9b98953664b2/Media-audience-development-in-Latvia-2004-2012.pdf

Rožukalne, Anda., Stakle, Alnis., & Skulte, Ilva. (2020). "Media education in the common interest: Public perceptions of media literacy policy in Latvia." Central European Journal of Communication, 13(2). Retrieved 20 December 2020. https://cejc.ptks.pl/Volume-13-No-2-26-Special-Issue-2020/Media-education-in-thecommon-interest-Public-perceptions-of-media-literacy-policy-in-Lat

"The Constitution of the Republic of Latvia" (n.d.) Republic of Latvia. Retrieved 9 December 2020.https://www.president.lv/en/republic-of-Latvia/the-constitution-of-the-republic-of-latvia#gsc.tab=0

"WSIS+10: Overall Review of the Implementation of the WSIS Outcome: WSIS 10 Year Country Report by LATVIA." (Report). (2014). Retrieved 17 December 2020, from World Summit on the Information Society website: http://www.itu.int/net/wsis/review/inc/docs/rcreports/WSIS10_Country_Reporting-LVA.pdf

Chapter 3--Lithuania

"An agreement on Lithuanian defense policy guidelines has been signed." My government. (lrv.lt.) (2018, 10 September). Retrieved 28 December 2020. https://lrv.lt/lt/naujienos/pasirasytas-susitarimas-del-lietuvos-gynybos-politikos-gairiu

Bada, Maria., & Weisser, Carolin. (2017, August). "Cybersecurity Capacity Review: Republic of Lithuania" (Report). Retrieved 4 January 2021. Global Cyber Security Capacity Centre; Oxford Martin School, University of Oxford https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf

Balcytiene, Aukse (chapter author). (2012). "Culture as a Guide in Theoretical Explorations of Baltic Media" in "Comparing Media Systems Beyond the Western World." New York, NY: Cambridge University Press. pp. 60-61. Retrieved 29 December 2020. https://d1wqtxts1xzle7.cloudfront.net/56763719/Daniel_C._Hallin__Paolo_Mancini-Comparing_Media_Systems_Beyond_the_Western_World-Cambridge_University_Press_2011.pdf?1528576150=&response-content-disposition=inline%3B+filename%3DDaniel_C_Hallin_Paolo_Mancini_Comparing.pdf&Expires=1609300553&Signature=cfA0hNbsYXZBIaqzDNeHbgFbxYexZzcytSAvzQQRHI6SqPHZZ0Pe5EJAi6PdMrjQ6mFykgfvyo61VKyV-dh41UTfmF78iHfz~OnHLzuJ~zyUE0krQUfw1GHOexfrf1RA-gSMsvAl~JbJaSbjGY9syA6KL2oTaT9TEFAksHxZFgDGj4sgFrH6qQCMpOphr0TyC7ucNuyeCrN5NyXNP~SUaa6UC5mlERPxSAWlmMw7ugevp5WHOkbLBXW3mpIBmdzMyTdIPlJOm0r4juFewuE8zWbKqsApfeVjJ2vu7hf0KkTxcx83kaBYPuQmHXwJEK1F6VrDvEgOggwzf89nzHdsFQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=62

"Baltic Media Grant." (n.d.). Nordic Council of Ministers' Office in Estonia. Retrieved 26 December 2020. https://www.norden.ee/en/about-us/funding/support-for-increased-quality-of-media-content-and-strengthening-of-minority-language-media-production-in-estonia-latvia-and-lithuania

Bankauskaitė, Dalia. (2020, 27 February). "Lithuanian Total Defense." Center for European Policy Analysis (CEPA). Retrieved 28 December 2020. https://cepa.org/lithuanian-total-defense/

Butrimas, Vytautas. (2015). "National Cyber Security Organization: Lithuania" (Publication). p. 5. Retrieved 4 January 2021. NATO Cooperative Cyber Defense Centre of Excellence. https://ccdcoe.org/library/publications/national-cyber-security-organisation-lithuania/

"Cyberwellness Profile Lithuania." (n.d.). International Telecommunication Union. Retrieved 5 January 2021. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Lithuania.pdf

Denisenko, Viktor. (chapter author). (2018). “Lithuania.” In Disinformation Resilience Index. Retrieved 24 December 2020. http://prismua.org/en/dri/

Denisenko, Viktor. (2019, 11 June). “Regional and national security discourse in the local Russian media in Lithuania.” International Centre for Ethnic and Linguistic Diversity Studies. Retrieved 28 December 2020. https://www.icelds.org/2019/06/11/regional-and-national-security-discourse-in-the-local-russian-media-in-lithuania/

Fernandes, Sandra. & Correia, Daniel. (2018). “(Re)securitisation in Europe: The Baltic States and Russia.” Debater a Europa. Retrieved 16 December 2020. https://www.researchgate.net/publication/322690589_Resecuritisation_in_Europe_the_Baltic_States_and_Russia

Government of Lithuania. (2011, 29 June). “On the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019.” Retrieved 3 January 2021. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf

Juraite, Kristina. (2014, May). “Media and Information Education Policies in Lithuania” (Report). Retrieved 6 January 2021. Vytautas Magnus University. http://ppemi.ens-cachan.fr/data/media/colloque140528/rapports/LITHUANIA_2014.pdf

Ketlerienė, Aleksandra. (2019, 21 September). “New Polish channel in Lithuania seeks to win back ethnic minority viewers from Russian TV.” Retrieved 1 January 2021. https://www.lrt.lt/en/news-in-english/19/1098787/new-polish-channel-in-lithuania-seeks-to-win-back-ethnic-minority-viewers-from-russian-tv

“Lithuania considers following Latvia in banning Russia's RT.” (2020, 2 July). lrt.lt. Retrieved 31 December 2020. https://www.lrt.lt/en/news-in-english/19/1194032/lithuania-considers-following-latvia-in-banning-russia-s-rt

“Lithuania Constitution.” (n.d.). International Constitutional Law Project (ICL) Project. Retrieved 25 December 2020. https://www.servat.unibe.ch/icl/lh00000_.html

Lithuania, Ministry of Culture. (2019, 19 February). “Order on Strategic Directions for Public Information Policy Approval for the Year 2019-2022.” Retrieved 1 January 2021. https://www.e-tar.lt/portal/lt/legalAct/95c4cf60344211e99595d005d42b863e

Lithuania, Ministry of Defense. (2012). “The Military Strategy of the Republic of Lithuania 2012.” p. 5. Retrieved 29 December 2020. https://www.files.ethz.ch/isn/167339/THE%20MILITARY%20STRATEGY%20of%20the%20Republic%20of%20Lithuania.pdf

Lithuania, Ministry of National Defense. (2018, 13 August). “National Cyber Security Strategy.” p. 12. Retrieved 5 January 2021. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/programme-for-the-development-of-electronic-information-security-cyber-security-for-2011-2019-2011

Lithuania, Ministry of National Defense of the Republic of Lithuania. (2017). "Lithuanian Defense Policy White Paper." p. 56. Retrieved 3 January 2021. https://kam.lt/download/59163/wp-2017-en-el.pdf

"Lithuanian-Swedish Roundtable Expert Discussions on Social Resilience and Psychological Defence" (Issue brief). (2018, September). Retrieved 7 January 2021. European Integration Studies Centre. http://www.eisc.lt/uploads/documents/files/EISC_policy%20brief(1).pdf

Lithuania, Seimas of the Republic of Lithuania. (2017, 17 January). National Security Strategy. pp. 5-17. Retrieved 29 December 2020. https://kam.lt/en/defence_policy_1053/important_documents/strategical_documents.html

Lithuania, Seimas of the Republic of Lithuania. (n.d.). "Resolution Amending the Seimas of the Republic of Lithuania Resolution on the Approval of the National Security Strategy." Retrieved 29 December 2020. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e7fcc2608f1f11e8aa33fe8f0fea665f?jfwid=uu1o96cqv

"Lithuania to draft new National Security strategy." (2015, 27 October). The Baltic Times. Retrieved 29 December 2020 . https://www.baltictimes.com/lithuania_to_draft_new_national_security_strategy/

Malikevicius, Nerijus, (Online interview) 2020, 25 July.

"Mass media in Lithuania." (n.d.). Wikipedia.com. Retrieved 1 January 2021. https://en.wikipedia.org/wiki/Mass_media_in_Lithuania#Radio

"Media of Lithuania." (n.d.). truelithuania.com. Retrieved 27 December 2020. http://www.truelithuania.com/media-of-lithuania-1664

"National Cyber Security Centre." (n.d.). National Cyber Security Centre. Retrieved 4 January 2021. https://www.nksc.lt/en/

"National Minorities." (2016, 1 September). Ministry of Culture of the Republic of Lithuania. Retrieved 2 January 2021. https://lrkm.lrv.lt/en/activities/national-minorities

Peel, Michael. (2019, 3 February). "Fake news: How Lithuania's 'elves' take on Russian trolls." ft.com. Retrieved 2 January 2021. https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf

Piotrowski, Sławomir. (2018). "Security Policy of the Baltic States and its Determining Factors." *Security and Defense Quarterly*, *22*(5). Retrieved 29 December 2020. http://31.186.81.235:8080/api/files/view/627285.pdf

Rossbach, Niklas. H. (2017, November). "Psychological Defence: Vital for Sweden's Defence Capability" (Issue brief). Retrieved 7 January 2021. The Swedish Defense Research Agency. https://www.foi.se/rest-api/report/FOI%20Memo%206207

"Russian-language TV channel Current Time to be launched in Lithuania." (2018, 14 September). lithuaniatribune.com. Retrieved 1 January 2021. https://lithuaniatribune.com/russian-language-tv-channel-current-time-to-be-launched-in-lithuania/

Schrøder, Anne Sofie. (2017, 28 September). "Lithuania has a volunteer army fighting a war on the internet." euronews.com. Retrieved 2 January 2021. https://www.euronews.com/2017/09/28/lithuania-has-a-volunteer-army-fighting-a-war-on-the-internet

Sengupta, Kim. (2019, 17 July). "Meet the Elves, Lithuania's digital citizen army confronting Russian trolls." Retrieved 2 January 2021. https://www.independent.co.uk/news/world/europe/lithuania-elves-russia-election-tampering-online-cyber-crime-hackers-kremlin-a9008931.html

Stone, Jon. (2018, 17 January). "Russian disinformation campaign has been 'extremely successful' in Europe, warns EU." The Guardian. Retrieved 28 December 2020. https://www.independent.co.uk/news/uk/politics/russian-fake-news-disinformation-europe-putin-trump-eu-european-parliament-commission-a8164526.html

Šuminas, Andrius., & Jastramskis, Deimantas. (2020). "The importance of media literacy education: How Lithuanian students evaluate online news content credibility." Central European Journal of Communication, 13(2). Retrieved 6 January 2021. https://www.researchgate.net/publication/342203091_The_importance_of_media_literacy_education_How_Lithuanian_students_evaluate_online_news_content_credibility

"Survey on Media Literacy Level in Lithuania." (2020, 17 April). en.unesco.org. Retrieved 7 January 2021. https://en.unesco.org/creativity/node/19648

"What defence help do the Baltics want from Sweden?" (2015, 12 February). Radio Sweden. Retrieved 7 January 2021. https://sverigesradio.se/artikel/6092292

"WP3. Formal Media Education Lithuania." (n.d.) (issue brief). EMEDUS Europe Media Education. Retrieved 6 January 2021. http://www.gabinetecomunicacionyeducacion.com/sites/default/files/field/investigacion-adjuntos/lithuaniad.pdf

CONCLUSION

"Lithuania to draft new National Security strategy." (2015, 27 October). The Baltic Times. Retrieved 29 December 2020. https://www.baltictimes.com/lithuania_to_draft_new_national_security_strategy/

ACRONYMS

CCDCOE	Cooperative Cyber Defense Center
CEO	Chief Executive Officer
CERT-LT	National Computer Response Team (Lithuania)
CERT.lv	Security Incident Response Institution (Latvia)
CII	Critical Information Structure
CoI	Community of Interest
CU	Cyber Unit
DoS	Denial of Service
DDoS	Denial of Service
EDL	Estonian Defense League
ERDF	European Regional Development Fund
EU	European Union
GDP	Gross Domestic Product
HS	Hosting Service
IBM	International Business Machines
ICS	Industrial Control Systems
ICT	Information Communications Technology
ID	Identification
IT	Information Technology
LAF	Lithuanian Armed Forces
LEM	Law on Electronic Media
LTU MOD CIRT	Ministry of Defense computer response team
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Center
NEPLP	National Electronic Mass Media Council

NGO	Non-Governmental Organization
NMK	(Estonian: Noorte Meediaklubi) Young People's Media Club
RFE/RL	Radio Free Europe/Radio Liberty
SEG	Security Expert Groups
SVDPT-CERT	Secure State Data Communication Network
US	United States
VAT	Value Added Tax
VOA	Voice of America
WSIS	World Summit on the Information Society