Cyber Lessons that the World Can Learn from Lithuania

M.Warren[1], D.Štitilis[2] and M.Laurinaitis[2]
[1]RMIT University, Melbourne, Australia and Univeristy of Johannesburg, Johannesburg, South Africa
[2]Mykolas Romeris University, Vilnius, Lithuania.

Matthew.warren2@rmit.edu.au
stitilis@mruni.eu
laurinaitis@mruni.eu

Abstract: In an era of rapid technological advancements and increasing online connectivity, the proliferation of cyber threats, including the spread of fake news and disinformation, presents a significant challenge to nations worldwide. Lithuania has emerged as a leading example in addressing these challenges, particularly concerning cyber groups such as Killnet and disinformation / fake news. This paper aims to explore the key cyber lessons that can be learned from Lithuania's proactive approach in dealing with Killnet and combating disinformation / fake news. By analysing Lithuania's cybersecurity strategies and initiatives, this paper identifies crucial lessons that can be applied globally. Firstly, Lithuania recognises the importance of co-ordinated cyber security technologies and national frameworks to counter cyber groups such as Killnet attacks. Secondly, Lithuania has effectively tackled the spread of fake news / disinformation through a comprehensive approach involving legislation, media literacy programs, and strong cooperation between government agencies, civil society organisations, and the private sector. The country's experience underscores the significance of collaborative efforts in combating misinformation, promoting media literacy, and fostering critical thinking skills among the population.

Keywords: Cyber Security, Lithuania, Russia, Fake News and KillNet.

1. Introduction and Background

Lithuania is a unique country when it comes to cyber security due to its whole-of-government and whole-of-society approach to the issue. The country has adopted a national cyber security strategy that focuses on developing cyber defence capabilities, building a secure state data-transfer network, and promoting innovative cyber security tools. Lithuania is also recognised as one of the best-prepared countries in the world for cyber security and leads the EU's (European Union) cyber security cooperation efforts. Moreover, the country emphasises public awareness and education to deal with evolving threats. Lithuania's unique approach to cyber security emphasises cooperation and education to deal with the evolving threats of cyber security attacks and fake news (disinformation) campaigns.

Lithuania is a country located in the Baltic, with a population of 2.8 million, a member of the European Union, and NATO and Lithuania is considered a front-line cyber state. According to the International Telecommunication Union - Global Cyber Security Index, Lithuania is ranked 6th globally (ITU, 2021) for their national cyber security capability and resilience.

Historically Lithuania has developed a unique national approach to cyber security. The Lithuanian Cyber Security Law, implemented in 2015, was one of the first laws of its kind in Europe, defined critical infrastructure in Lithuania and established security requirements for Lithuanian critical infrastructure providers (Baltic News, 2018).

The first Lithuanian National Cyber Security Strategy was developed by the Lithuanian Ministry of National Defence in collaboration with other government agencies and industry stakeholders in 2017 (Ministry of National Defence, 2017). Key principles of the Lithuanian National Cyber Security strategies include (Ministry of National Defence, 2017, Ministry of National Defence, 2019):

- strengthening legal and regulatory frameworks: Lithuania has enacted legislation and established regulatory frameworks to address cyber threats effectively. This includes the Law on Cybersecurity, which provides a legal basis for preventing, detecting, and responding to cyber incidents;
- building cybersecurity capabilities: The strategy emphasizes the development of cybersecurity expertise and skills among professionals, law enforcement agencies, and the public. Lithuania has invested in cybersecurity education, training programs, and international cooperation to enhance its capabilities;
- promoting public-private partnerships: Recognising the importance of collaboration, Lithuania actively fosters partnerships between government institutions, private sector entities, and academia. This approach encourages information sharing, joint initiatives, and coordinated responses to cyber threats;

- enhancing international cooperation: Lithuania actively engages in international efforts to combat cybercrime and improve global cybersecurity.

The updated 2019 Lithuanian National Cyber Security Strategy outlines a range of objectives for Lithuania, including enhancing the country's cyber security capabilities, developing a strong legal and regulatory framework for cyber security and promoting international cooperation in the cyber domain (Ministry of National Defence, 2019). Lithuanian has also set up the Regional Cyber Defence Centre (RCDC) which is a subsidiary of the National Cyber Security Centre under the Ministry of National Defence of the Republic of Lithuania. The key operational objectives of the RCDC (RCDC, ND are):

- to strengthen cooperation with the United States of America, Ukraine, Georgia, Poland and other strategic partners of Lithuania in the field of cyber security;
- to carry out cyber threat analysis jointly with the partners;
- to organise training courses for cyber security specialists;
- to conduct international scientific research in the area of cyber security.

As cited in Warren 2023 (Warren et al, 2023) Russia has a long history of using information and cyber security as a weapon in offensive and defensive manners, from Estonia 2007, Georgia 2008, Ukraine 2014, 2022 as well as numerous examples of election interference in Western countries. Ukraine has been dealing with Russia as an adversary since the first Russian-Ukraine war in 2014, the illegal annexation of Crimea in 2014, and the Russian invasion in 2022 (Czosseck, 2011, Bowen, 2021).

On 24 February 2022, Russia invaded Ukraine, following the invasion the Ukrainian Government had been supported with political, economic and military support from numerous governments around the world (including Lithuania) (BBC, 2023). Russia has also been supported, but this support has come from hacking groups, at the forefront of this support have been such groups such as KillNet. KillNet is a pro-Russian hacktivist group active since at least January 2022 and known for its DDoS (Distributed Denial of Service) attacks against countries supporting Ukraine, especially NATO countries since the Russia-Ukraine war broke out in 2022. DDoS is the primary type of cyber-attack approach employed by the group which can cause thousands of connection requests and packets to be sent to the target server or website per minute, slowing down or even stopping vulnerable systems. While KillNet's DDoS attacks usually do not cause major damage, they can cause service outages lasting several hours or even days (US Government, 2023).

According to KillNet, their funding has come from a variety of different sources including (Thales, 2023):

- private charities;
- funding directly from the group's activities;
- large crowdfunding campaigns, the donations are made in cryptocurrencies or by direct donation through applications such as the Telegram message application;
- partially self-funded through crypto mining activities;
- indirect funding from Russian intelligence services.

Figure 1 shows the KillNet group providing information via the Telegram application for crypto donations via Bitcoin, Ethereum, Tether payment systems

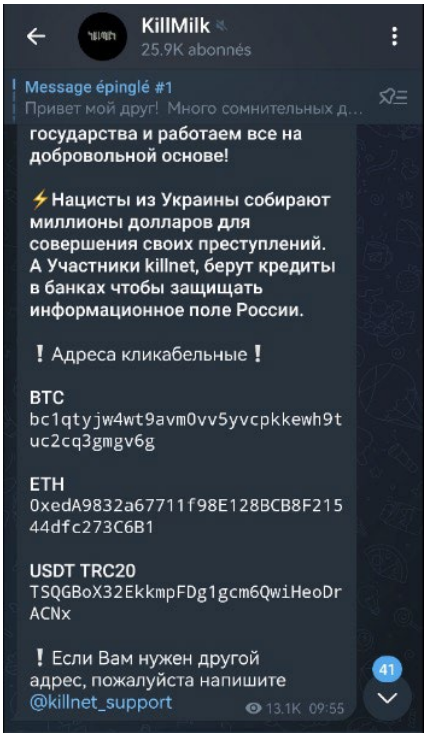

Figure 1: KillNet request for donations via Telegram application (information in Russian).

During the current Russian situation, Western organisations such as Microsoft are undertaking extensive analysis of Russian tactics and approaches. Microsoft has identified that some of the most common methods used against Western government, critical infrastructure and corporate systems include (Microsoft 2022a, Microsoft 2022b and Microsoft 2022c):

- Advanced Persistent Threats (APT): This refers to long-term, targeted attacks that are carried out by state-sponsored hacking groups. APT attacks typically involve the use of sophisticated malware and social engineering tactics to gain access to a target's network and steal sensitive information;
- phishing: This method involves tricking victims into providing login credentials or other personal information through fake emails, social media messages, or other forms of communication;
- Distributed Denial of Service (DDoS) attacks: This method involves overwhelming a website or network with a flood of traffic, making it difficult or impossible for legitimate users to access it;
- watering hole attacks: This method involves compromising a specific website that is likely to be visited by targeted victims, and using that website to deliver malware or steal information;
- supply chain attacks: This method involves compromising a third-party vendor or service provider that has access to a target's network, in order to gain access to the target's network.

Another major issue facing countries around the world is the impact of fake news also known as disinformation. What is fake news, according to Warren (2019) there are numerous aspects including:

- fabricated content: completely false content;
- manipulated content: distortion of genuine information or imagery, for example, a headline that is made more sensationalist, often popularised by ‘clickbait’;
- imposter content: impersonation of genuine sources, for example by using the branding of an established news agency;
- misleading content: misleading use of information, for example by presenting a comment as fact;
- false context of connection: factually accurate content that is shared with false contextual information, for example when a headline of an article does not reflect the content;
- satire and parody: presenting humorous but false stories as if they are true. Although not usually categorised as fake news, this may unintentionally fool readers.

2. Research Question

The paper will explore the unique challenges that Lithuania has experienced and highlight what other countries can learn from these real-life cyber experiences.

The key focus of the paper is:

How has Lithuania reacted to different cyber incidents during the Ukrainian situation?

In terms of this study, it was decided just to focus on Russia's cyber-related activities and just to focus broadly on cyber activities against Lithuania.

One of the issues with researching a live conflict is that it is unfolding, therefore a key issue is around collecting and using real-life research data that is valid in an emerging environment.

In terms of this study, it was decided to draw upon real-life public data drawn from the Lithuanian government cyber security assessments.

3. Case studies

The paper will focus on several real-life examples, in particular the hacking group KillNet and the impact of fake news. These will be discussed in the next section of the paper.

3.1 Example 1: Hacking Group KillNet

This case study is drawing upon real-life data from the Lithuanian Regional Cyber Defence Assessments (RCDC 2022a, 2022b, 2022c). The data identified the following incidents relating to KillNet and Lithuania and related to the first three quarters of 2022. The incidents identified in this period were:

Incident 1 – 16th May, 2022 "KillNet" and "Legion" Hacker groups Declare Cyber War against 10 Countries (numerous countries including Lithuania).

The pro-Russian hacker group "KillNet", together with volunteer Russian hackers "Legion", declared war on ten countries, including the UK, the US, Germany, Italy, Latvia, Romania, Lithuania, Estonia, Poland, and Ukraine. These countries were chosen "because of their support for Nazis and Russophobes," a popular narrative used by the Russian media to describe anyone supporting Ukraine's resistance to the Russian invasion. This attack was a simple call for action against Lithuania.

Incident 2 – 20th June, 2022 "KillNet" targets various network infrastructures in Lithuania.

The Russian hacktivist group "KillNet '' in their telegram channel posted a call for other hacking groups to help them cripple Lithuania's national network infrastructure. Therefore, they did by damaging the Lithuanian police website policija.lrv.lt. The hacktivist group also tried disrupting one of Lithuania's mobile providers but they were not successful. The attack was minimal in its success apart from a Lithuanian government web-site being disrupted for a short period.

Incident 3 – 27th June, 2002, a Russian hacking group takes credit for a wide-ranging cyber-attack on Lithuania.

The Lithuanian Governmental Tax Inspectorate, the Migration Department, Ministries and a number of other state agencies were among the targets of the KillNet hackers, according to a statement from the nation's defence minister and National Cyber Security Centre. On its Telegram channel, the Russian hacker organisation "KillNet" announced the attack, which was first directed at a Lithuanian and a Latvian online accounting system. The attack was minimal in its success.

Incident 4 - July 4, 2022 Lithuanian website was defaced.

One of the hacktivist groups associated with "KillNet", "NoName057(16)", posted on their Telegram channel about the defacement of the Lithuanian logistics company "ExpressTrip". On the company's defaced web page, there were claims about the "correct" attitude to the ban on the transit of Russian cargo to the Kaliningrad region. In addition, the defaced web page supported the Russian war against Ukraine and called it "the special operation of the Russian Federation armed forces". The attack was minimal in its success apart from a Lithuania corporate web-site being disrupted for a short period.

The four identified examples in relation to KillNet, identified a number of issues, namely:

1. KillNet overstated/overemphasised the rationale and impact of their cyber attacks (incidents 1, 2, 3 and 4);
2. The KillNet attacks were not sophisticated, e.g. web site defacement (incidents 2 and 4);
3. The messaging point-to-point app – Telegram was used to communicate the incidents (incidents 2,3 and 4), the rationale being that this platform cannot be censored or removed.

The KillNet examples highlight a number of cyber incidents, but the impact of these incidents was minor and when the cyber attacks actually took place they took the form of minor website defacements. Because of the cyber security maturity of the Lithuanian government and organisations they were able to identify and resolve the issues correctly. What the incidents did highlight was the limited ability of KillNet to disrupt Lithuanian core services and Lithuanian was able to react to these attacks.

3.2 Case 2 Study - Fake News and Lithuania

Lithuania has historically been a victim of fake news and disinformation and this situation has intensified recently since 2022 with Lithuania's support of Ukraine.

From June 2022, Lithuania imposed restrictions on the transit of sanctioned goods from Russia to its Kaliningrad exclave. The Russian response was to call the situation the "Kaliningrad Blockade" with claims that the Lithuanian government had dismantled the railway line running through Lithuanian connecting to Kaliningrad (LRT, 2022). As shown by Figure 2, many of the fake news stories are focused on an internal Russian audience and focus on reinforcing the narrative of the Russian Government regarding a blockade of Kaliningrad and the false message that the Lithuanian government was physically disrupting railway traffic between Russia and Kaliningrad.

Figure 2: Russian Fake News Story about the destruction of train tracks within Lithuania (StopFake, 2022).

The fake news campaign against Lithuania ran for a series of weeks with a focus on Russian news outlets for an internal Russian audience and then faded away as other political matters came to the forefront.

One of the unique aspects of Lithuania is how civil society is involved in dealing with the impact of fake news. Lithuanian society has reacted to the fake news situation by creating citizen-based groups called Elves, the

rationale being that elves fight trolls (Time, 2022). Based on the concept of elves there are a number of citizen organisations in Lithuania that have organically developed to combat fake news and disinformation the most notable being an organisation called Debunk.

Debunk is a citizen-based movement that started in Lithuania but has expanded to other Baltic countries, Poland, Georgia and Montenegro, as well as in the United States and North Macedonia. Debunk is an independent technology think tank and non-governmental organisation that analysis fake news and runs educational media literacy programs. Debunk has the following focused capabilities and characteristics (Debunk, NDa):

- a team of skilled analysts with backgrounds ranging from political science and history to business and media;
- national institutions in our partner countries, providing valuable insights on the situation in their respective regions;
- IT professional with a broad knowledge of AI tools which helps Debunk make the fact-checking process faster and fool-proof;
- a Lithuanian community of volunteer fact-checkers also known as elves (because of their notorious skills of hunting online trolls) to assist Debunk with their activities.

The Debunk also undertake the following key activities (Debunk, NDa):

- development of detailed disinformation reports in relation to current issues and country-linked campaigns;
- ongoing influence operations and monitoring of elections for foreign interference;
- training and certification of citizens involved in monitoring fake news.

The concept of “elves” was developed in Lithuania in 2014, following the events in Maidan Square in Ukraine that included clashes between protesters and pro-government forces of the Russian-backed president Viktor Yanukovych. Shortly after, Russia attacked Ukraine and occupied part of its territory and at the same time organised sophisticated fake news campaigns against Ukraine (Debunk, NDb).

An example of the work of Debunk is shown in Figure 3, this shows an analysis of a fake news story in 2021 regarding Lithuanian “perceived jealousy” of the Belarus government and their development of a nuclear power station with Russian support and that Lithuania pressured the Ukraine government not to use any power supplied by the nuclear reactor in Belarus.

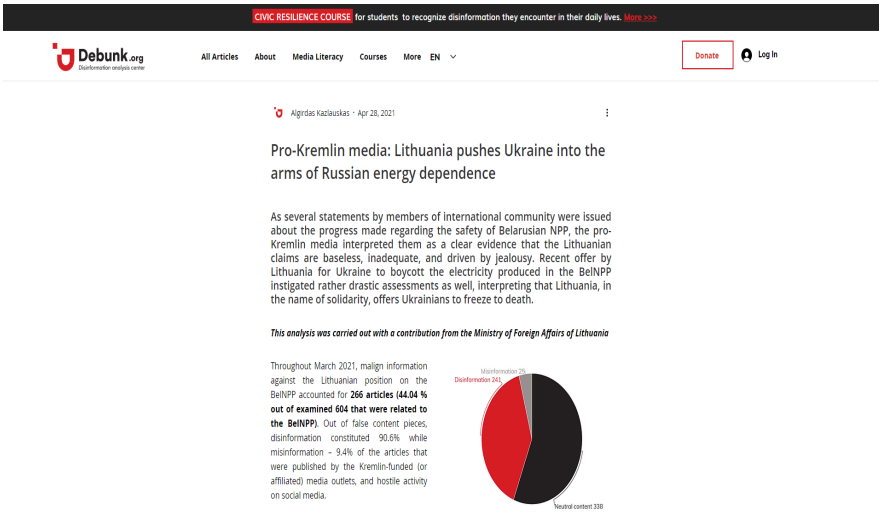

Figure 3: Debunk analysis of a Fake News story.

4. Discussion

Lithuania has been targeted by a number of Russian cyber-attacks since the Ukraine conflict started especially in terms of national DDoS attacks on Western countries. The data (see Table 1) shows that Lithuania was the 6th most attacked Western country in terms of DDoS attacks, but with Latvia in 2nd place, it shows that smaller Baltic Countries are being unproportionally targeted by these attacks.

Poland	110
Latvia	74
Sweden	60
USA	67
Germany	52
Lithuania	45

Table 1: National DDoS Attacks during the Ukraine Conflict (Thales, 2023).

In the context of this paper, many countries can learn from Lithuania's experience and expertise. In terms of the examples described in the paper and how Lithuanians responded to cyber incidents, namely:

KillNet Example

KillNet is a unique organisation, well-resourced and they have the ability to undertake cyber attacks especially DDoS attacks against a number of Western targets. Lithuania has experienced cyber security attacks against several Lithuanian government and commercial sites.

The paper reflected on four cyber incidents in 2022 related to Lithuania and KillNet and drew upon the analysis of the Lithuanian Regional Cyber Defence Centre and highlighted how Lithuania was able to mitigate these attacks and these attacks had only minimal impact.

Fake news Example

Lithuania is an ongoing target of fake news and disinformation campaigns many of which originate from Russia. Lithuania has reacted to the situation by the development of citizen initiatives that identify fake news stories and publicly disclose them as being fake news. In the age of social media and fast-spreading information, Lithuanian society is at the front line of confrontation and negative influences. Forming a strong, resilient, and critically thinking society that remains attentive to information and resistant to provocations is a key task for Lithuania, especially in the face of today's ongoing security issues (Bankauskaite and Šlekys, 2023).

There is always of risk of volunteer civic society groups such as Debunk that over time due to a lack of funding and that volunteers may leave the group due to volunteer fatigue / family commitments that these groups are not sustainable over a long period of time but now they are fulfilling a key function for Lithuanian society.

5. Conclusion

In terms of the paper, one of the challenges in reflecting upon a current conflict is the changing situation and use of appropriate data sources, this was the reason for drawing upon the data provided by the Lithuanian Regional Cyber Defence Centre and using informed data from other sources, e.g. Microsoft and Thales.

The paper has described real-life cyber challenges that are impacting the whole of Lithuania and the steps that they are undertaking to deal with the challenges. The shared Lithuania experiences is something that countries around the world can learn from. As time progress, more and more information about the current cyber and physical conflict between Russia and Ukraine will become public as more insights will be gained about groups such as KillNet and fake news campaigns against countries such as Lithuania.

By studying Lithuania's experiences in countering the Killnet group and disinformation / fake news, policymakers, cybersecurity professionals, and researchers worldwide can gain valuable insights into effective strategies, legislation, and collaborative approaches to safeguard key systems and combat the dissemination of false information in the digital age.

References

Baltic Times. (2018) Lithuania's cyber security: key initiatives and future challenges. URL https://www.baltictimes.com/lithuania_s_cyber_security__key_initiatives_and_future_challenges/, accessed: 16/01/23.

Bankauskaite, D and Šlekys,D (2023) Lithuania's Total Defense Review, PRISM Vol. 10, No. 2, URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323902/lithuanias-total-defense-review, accessed: 16/01/23.

BBC (2023) Has Putin's war failed and what does Russia want? https://www.bbc.com/news/world-europe-56720589, accessed: 16/01/23.

Bowen, A (2021) Russian Cyber Units – US Congressional Research Service, URL: https://crsreports.congress.gov/product/pdf/IF/IF11718, accessed 16/10/22.

Czosseck, C., Ottis, R., & Talihärm, A. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism (IJCWT), 1*(1), 24-34. URL: http://doi.org/10.4018/ijcwt.2011010103

Debunk (NDa) About Debunk. URL: https://www.debunkeu.org/about, accessed: 16/01/23.

Debunk (NDb) Elves. URL: https://www.debunk.org/about-elves, accessed: 16/01/23.

International Telecommunication Union (2021). Global Cyber Security Index 2020, URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. accessed: 16/01/23.

LRT (Lithuanian National Radio and Television) Russian propaganda targets Lithuania – Kaliningrad 'blockade' and 'betrayal, URL: https://www.lrt.lt/en/news-in-english/19/1736701/lrt-facts-russian-propaganda-targets-lithuania-kaliningrad-blockade-and-betrayal, accessed: 12/08/21.

Microsoft (2022a) Microsoft Digital Defence Report 2022, Microsoft.

Microsoft (2022b) Defending Ukraine: Early Lessons from the Cyber War, Microsoft.

Microsoft (2022c) Special Report: Ukraine – An overview of Russia's cyber attack activity in Ukraine, Microsoft.

Ministry of National Defence of the Republic of Lithuania (2017). National Cyber Security Strategy for 2017-2020. URL: https://kam.lt/download/87423/national_cyber_security_strategy_for_2017-2020.pdf, accessed: 12/08/21.

Ministry of National Defence of the Republic of Lithuania (2019). National Cyber Security Strategy.URL: https://kam.lt/wp-content/uploads/2022/11/2019-EN-KibernetineSaugumoStrategija-el.pdf, accessed: 16/01/23.

RCDC (ND) About RCDC (Regional Cyber Defence Centre), URL: https://www.nksc.lt/rkgc/en.html, accessed 2/2/23.

RCDC (2022a) RCDC 2022 1st Quarter Report, URL: https://www.nksc.lt/doc/rkgc/CTAC_2022_1st_Quarter_Report.pdf, accessed 2/2/23.

RCDC (2022b) RCDC 2022 2nd Quarter Report, URL: https://www.nksc.lt/doc/rkgc/CTAC_2022_2nd_Quarter_Report.pdf, accessed 2/2/23.

RCDC (2022c) RCDC 2022 3rd Quarter Report, URL: https://www.nksc.lt/doc/rkgc/CTAC_2022_3rd_Quarter_Report.pdf, accessed 2/2/23.

StopFake (2022) Fake: Lithuania Dismantles Railway to Kaliningrad, URL: https://www.stopfake.org/en/fake-lithuania-dismantles-railway-to-kaliningrad/, accessed 2/2/23.

Thales (2023) 2022-2023: A year of Cyber Conflict in Ukraine, Thales.

Time (2022) Meet the Lithuanian 'Elves' Fighting Russian Disinformation, URL: https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine, accessed 2/2/23.

US Government (2023) Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector, Office of Information Security, URL: https://www.hhs.gov/sites/default/files/KillNet-analyst-note.pdf, accessed: 16/01/23.

Warren, M. (2020). Fake News Case Study during the Australian 2019 General Election. Australasian Journal of Information Systems, 24. https://doi.org/10.3127/ajis.v24i0.2803, accessed 2/2/23.

Warren, M, Štitilis, D and Laurinaitis, M (2023) The impact of Russian Cyber Attackers within the Ukraine Situation, Journal of Information Warfare, Volume 22, Issue 1.