TASK FORCE

The Donald C.Hellmann Task Force Program

Kirill Kudryavtsev/AFP via Getty Images

Hybrid Warfare, Disinformation, and the NATO Response

2023

Hybrid Warfare and the NATO Response

Promoting Economic Independence, Defending Cyberspace, and Combatting Disinformation

EVALUATOR

Dr. Jeffrey Rathke

President of the American-German Institute, Johns Hopkins University

FACULTY ADVISOR

Sarah Lohmann

Acting Assistant Professor

Jackson School of International Studies

EDITORS

Jack Kaltreider, Taylor Bell

CHIEF LIAISON

Paulette Bussard

COORDINATOR

Michika Fukumori

RESEARCHER

Shern Sze Lim

GRAPHIC ARTISTS

Alijah Neal, Alan Zheng

Table of Contents

Executive Summary

As Russia's war in Ukraine enters its second year, Russia is increasingly targeting NATO member states with cyberattacks, coordinated disinformation campaigns, attempts at economic coercion, and espionage operations. These tools of hybrid warfare aim to degrade allied capabilities, undermine social unity, and erode support for Ukraine. Critical energy, transportation, and information infrastructure are especially vulnerable.

This task force examined fifteen countries as case studies to better understand the threats NATO is facing to detail how member states are responding, and to propose a series of policy recommendations designed to harden allied capabilities. Outside of NATO, this task force also examined Moldova, which is increasingly threatened both by Russian hybrid warfare and Russia's existing presence in Transnistria.

Key Findings:

1) Russia and China are the main actors targeting NATO countries, both seeking to ensure economic dependence across the alliance. Russian espionage activities have targeted wind farms and oil refineries in the North Sea, adversely impacting energy security. Meanwhile, China is increasing its ownership of European logistics and banking infrastructure, providing China opportunities to transfer technology and impede NATO interoperability via their control of European ports. China is also highly motivated to maintain European reliance on China for access to raw materials, and as such has taken action to oppose the further development of new extractive industries in Finland and Norway.

2) Cyberattacks emanating from Russia are targeting countries allied with Ukraine, disrupting energy critical infrastructure, impeding transportation and logistics, and compromising vital communications networks. The expansion of smart electric grids leveraging IoT exacerbates these threats by introducing numerous potential entry points that can be exploited by malicious actors to gain access to critical industrial control and communications systems. Furthermore, private companies with access to sensitive information are increasingly being targeted due to their lack of uniform cyber protections and reduced oversight.

3) Highly specific disinformation campaigns that emphasize divisive social issues, historical trauma, and NATO's military presence in Europe are being disseminated on social media and by Russian-aligned media outlets. These campaigns cause confusion, amplify social divisions, and muddy the waters of public debate.

Most of the countries examined are responding vigorously to these hybrid threats. Many have developed national cybersecurity strategies, adopted new technologies, formed defensive cyber corps, and coordinated anti-disinformation campaigns. However, some countries, whether due to resource constraints or disinterest, are less motivated to adjust to this new threat environment and as such present serious challenges to other members of the alliance.

No country is responding to hybrid warfare threats perfectly. The benefit of conducting in-depth case studies of many different countries is that patterns emerge. Russian, and to a much lesser extent, Chinese, tactics take similar forms across borders, and can therefore be addressed on an alliance-level. Combatting

hybrid threats effectively centers around three pillars: 1) Promoting Economic Independence; 2) Defending Cyberspace; and 3) Combatting Disinformation. The following policy recommendations distill our findings across fifteen countries into seven actionable policy proposals:

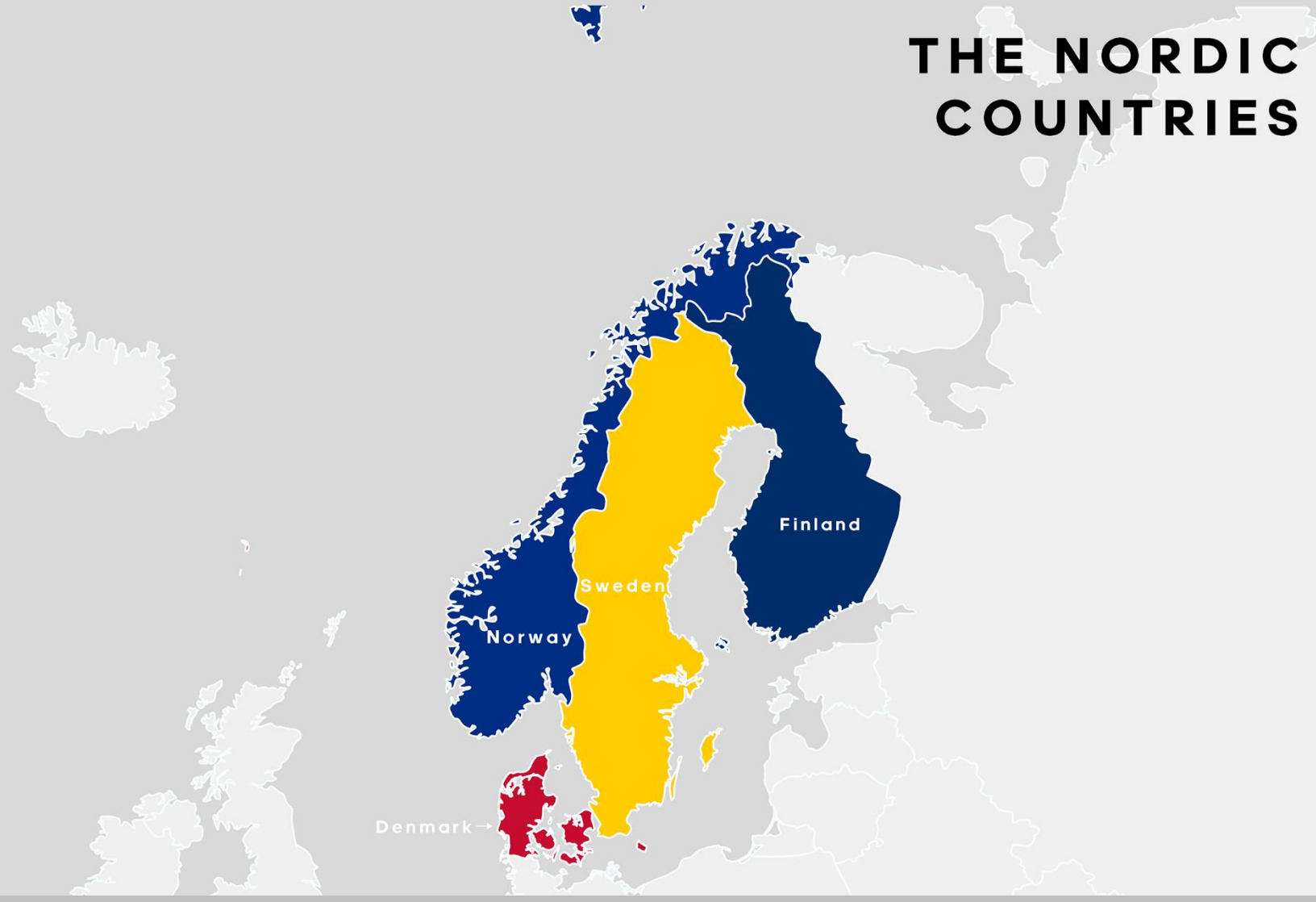
Policy Recommendations

1) Introduce EU-wide foreign direct investment (FDI) screening mechanisms to maintain EU sovereignty over its critical infrastructure.
2) Increase physical security of offshore wind farms and oil refineries in the North Sea and beyond through collaboration between NATO undersea rapid response force and Nordic countries.
3) Implement next-generation cyber early warning systems with AI and virtualization technology across NATO's critical infrastructure.
4) Provide funding through the NATO Security Investment Program for private sector cybersecurity capacity building in critical industries.
5) Establish cybersecurity standards for private IT providers that have contracts with public CI operators to be overseen by national level CERTs or CSIRTs.
6) Require all IT service providers contracting with critical infrastructure operators to undertake a mandatory security audit.
7) Implement comprehensive youth education programs on disinformation by national governments.

Structure of the Paper

The following regional case studies are organized by country, threat type, and policy response. Threats are described according to the vectors of attack, most of which emanate from Russia, including cyberattacks, disinformation campaigns,

economic coercion, and espionage, and emphasize how these methods have evolved following Russia's invasion of Ukraine. Finally, policy recommendations designed to enhance resilience to hybrid threats are provided at the end of each regional grouping.


THE NORDIC COUNTRIES
Finland
Sweden
Norway
Denmark

Case Studies

The Nordic Countries: Finland, Sweden, Norway, And Denmark

Russia's war in Ukraine is forcing a reimagining of the relationship between the Nordic countries, NATO, and Russia. Finland and Sweden, bearing witness to unprovoked Russian aggression, quickly moved to join Norway and Denmark as full members of NATO at the onset of the war. Finland's quick accession added over 800 miles to NATO's border with Russia and significantly upgraded NATO capabilities with the addition of a well-equipped and interoperable partner. Sweden's future accession will similarly enhance NATO capabilities, especially in the Baltic Sea.

Now bordering six NATO member-states, Russia is increasingly hostile towards the Nordic countries. Russian antagonism is manifesting itself below the threshold of war, taking the form of cyberattacks and disinformation campaigns, which together seek to undermine Nordic capabilities and internal security. These attacks are often difficult to attribute, however, Killnet, a Russian-backed hacker group, has made a name for itself launching distributed denial-of-service (DDoS) attacks to take down or "deface" government websites with pro-Russian messages (Roussi, 2022). Russian-aligned media outlets such as Sputnik masquerade as conventional international media to spread the Kremlin's favored narratives, especially anti-Ukraine sentiment (US Department of State, 2022).

Killnet and Sputnik highlight the centrality of state-backed actors to Russia's hybrid warfare strategy, underscoring the challenge facing the Nordic countries in this threat environment. However, not all hybrid threats are as difficult to attribute. In April 2023, a collaborative report produced by the Nordic countries documented

an at least decade-long Russian espionage operation off Nordic shores, centered on Norwegian energy critical infrastructure.

The following case studies describe the hybrid threats, the actors involved, and policy responses taken or under consideration by national governments to counter hybrid warfare tactics emanating mostly from Russia, but to a lesser extent from China as well. Policy recommendations on a national level are proposed at the end of the case study, while alliance-wide policies can be found in this section's conclusion.

Case Study
Finland
Paulette Bussard

Introduction

Finland's 830-mile-long border and the legacy of the Winter War motivated decades of Finnish non-alignment for fear of aggravating its often-aggressive neighbor. These neutral sentiments were swiftly dashed by Russia's invasion of Ukraine in February 2022. Support for joining NATO immediately skyrocketed, prompting a formal request for NATO membership delivered only months later in May (Kauranen, 2022). Finland's rapid accession to NATO has made it a notable target for Russian cyber and disinformation campaigns designed to punish, display Russian capabilities, and to discourage further involvement within the alliance. However, Finland has proven resilient. The following case study will describe the Russian hybrid warfare toolkit being deployed, Finland's response, and propose policy solutions.

Hybrid Threat Landscape

Cyberattacks

Following Finland's decision to join NATO, experts warned that both Finland and Sweden should expect an increase in small-scale cyberattacks (Kagubare, 2022). This aspect of Russia's playbook is well understood, with cyberattacks often deployed as retaliation for actions that draw the Kremlin's ire. On August 9th, 2022, the Finnish Parliament was the victim of a denial-of-service attack on its external websites (@SuomenEduskunta, 2022). The timing was no coincidence. Earlier the same day, President Biden had "signed a measure backing Finland and Sweden's admittance into NATO" (Kagubare, 2022).

On April 4th of the following year, when Finland officially joined NATO, Kremlin spokesperson Dmitry Peskov described "Helsinki's new military alignment

as an escalation and 'encroachment on Russia's security and national interests'" (Moscow Times, 2023). Such statements often presage further attempts to punish, disrupt, and discredit the Finnish state.

Disinformation

The Kremlin's disinformation campaigns long predate Russia's invasion of Ukraine. These campaigns historically targeted Finland's Russian minority, promoting narratives of the "alleged maltreatment of Russians in Finland" (Jong, 2017). Finland's accession to NATO has reignited the dissemination of these narratives and generated new ones. Another documented disinformation campaign promotes the idea that Finland and other European countries would be unable to "secure energy for their populations and businesses" without Russian oil and gas imports (Intelbrief, 2023). This narrative seeks to reinforce Russia's dominance in European energy markets by cultivating a fearful public.

Response to Hybrid Threats

1. Actors

Most cyberattacks and disinformation campaigns in Finland emanate from Russia or Russian-backed actors. The state-backed hacker group "NoName057(16)" claimed responsibility for the attack on the Finnish Parliament's website, citing Finland's desire to join NATO as their primary motivation (Petkauskas, 2022).

2. Policy Response

In response to the growing threat of cyberattacks on vital pillars of society, the Finnish government proposed providing vouchers that would "fund cybersecurity training, tools, assessments, and tests at companies in sectors considered critical to Finnish society" to build capacity and cultivate talent in the

private sector. The proposal would provide large companies vouchers for as much as 100,000 euros (Stupp, 2022). This sort of funding is meant to protect vital institutions within Finland from falling victim to cyberattacks, such as the one that was carried out against Parliament. As of December 1, 2022, Finnish companies and industries that have been designated as critical to society can apply for vouchers aimed at increasing cyber defense and information security (Traficom, 2023).

3. Benefits and Obstacles

The implementation of vouchers for cyber defense can help secure companies that have been deemed critical to Finnish society. Critical sectors include energy, food production, and defense, to name a few (Traficom, 2023). After meeting certain prerequisites and getting approval from the Finnish Transport and Communications Industry, a company can use up to 100,000 euros for the implementation of information security programs. Of course, this process is not immediate. It takes time for a company to identify its internal weaknesses and produce an action plan, but also to implement the new cyber defense protocols. Furthermore, companies are only eligible for vouchers if they are registered in Finland and designated as critical to Finnish security and society. This tends to exclude 'mom and pop' shops that are equally as vulnerable to cyberattacks and intrusions. However, the Finnish government has reported that "the total amount covered by the applications already exceeds the amount of funding available", and the program was estimated to accept applications for vouchers through 2024 (Traficom, 2022). In short, although some select companies have been able to secure vouchers, without enough funding, this project cannot comprehensively cover all vulnerabilities in critical sectors of Finnish society.

Conclusion

Finland is acting proactively to finance cybersecurity capacity building and to combat disinformation. However, funding gaps and onerous requirements continue to prevent more widespread adoption of new technologies and best practices in cyberspace. Finland, poised to remain a primary target of Russian hybrid warfare tactics as Finland's NATO integration progresses, must expand its existing programs to sustain high levels of resilience.

Case Study
Sweden
Paulette Bussard

Introduction

Unlike Finland, Sweden's accession into NATO has not been swift. Türkiye continues to stonewall Sweden, alleging that Sweden provides support for the Kurdish YPK, which Türkiye considers a terrorist organization. Adding Swedish naval capabilities, especially securing control over Gotland Island, will greatly enhance NATO's posture in the Baltic Sea. Russia wants to avoid a shift in the balance of power in the region and is leveraging the growing tensions between Türkiye and Sweden to delay NATO enlargement. Russian hybrid warfare tactics are spreading disinformation about the country's large Muslim community, exploiting fissures in Swedish society to drive a wedge in its relations with Türkiye. The following case study examines the current threat landscape in Sweden as Russia seeks to prevent it from joining NATO, the ways in which Sweden is fighting back, and proposes several policy recommendations.

Hybrid Threat Landscape

Cyberattacks

Sweden grades poorly in terms of its cyber defense capabilities, ranking just 43rd after Paraguay and the Philippines (BBC, 2021). These vulnerabilities have been exploited to great effect. In February 2023, the website of Scandinavian Airlines (SAS) was compromised, leaking the customer information and account login details (Mannes, 2023). This attack followed attacks on Sweden's national public television broadcaster, SVT, and on several of the nation's universities, all on the same day.

These attacks were anticipated by some of the victims. SVT had been expecting an attack after receiving threats from the hacker group `Anonymous Sudan' after several demonstrations of Quran burning in Sweden (Szumski, 2023). These cyberattacks and public demonstrations have elevated tensions between Sweden and Türkiye, making swift NATO accession difficult and opening the door for Russian meddling. In January, The Swedish Security Services (Sapö) remarked that threats "from violent Islamist extremism persist" and that "conspiracy theories and anti-state messages are widely spread online" by Russian intelligence operatives (Szumski, 2023). The rise of anti-Islamic rhetoric in Sweden is indicative of not only a growing right-wing sentiment, but also of targeted Russian disinformation operations aimed at delaying NATO enlargement.

Disinformation

Sweden has been a focus of Russian disinformation campaigns for at least the past decade. In a 2017 report, Swedish researchers found that the Russian media group, Sputnik, lessened the coverage of Russia's annexation of Crimea in 2014. They also noted an uptick in reporting by Russian-aligned media outlets that disparaged NATO and the EU (Kragh, 2017). Now, however, Russia's focus is on delaying or even preventing Sweden's accession into NATO by stoking tensions between Sweden and Türkiye. The root of the extended diplomatic row between Türkiye and Sweden is based on the latter's supposed support for Kurdish elements considered by Türkiye to be terrorists. The growing animosity between Sweden and Türkiye has manifested in several ways. Recently, the burning of the Quran took place outside of the Turkish embassy in Sweden. This provocative display was paid for by Chang Frick, a right-wing Swedish democrat and TV host who is known to work for the Russian propaganda outlet Russia Today (Ukrinform, 2023). Russia is

reinforcing the enmity between Sweden and Türkiye by coopting fringe elements — in this case right-wing politicians — to advance its national interests.

Response to Hybrid Threats

1. Actors

Russia is the primary actor targeting Sweden with cyberattacks and disinformation campaigns.

2. Policy Response

Sweden has recently taken action to mitigate the effects of disinformation by creating a new government agency: The Swedish Psychological Defense Agency (SPDA). The SPDA focuses on state and state-backed actors, seeking to identify disinformation and contribute to overall information literacy and resilience to coordinated campaigns to influence the psychology of the Swedish public (Woollacott, 2022).

3. Benefits and Obstacles

The SPDA was created in the months preceding the Swedish election in early 2022 to combat foreign disinformation campaigns. However, the goals of the agency are not bound to protect the sanctity of elections. The SPDA can make a profound impact on how the Swedish population processes media (SPDA, 2022). Since the invasion of Ukraine, it is not entirely clear what the agency has done to combat the spread of fake news. Due to mounting disinformation attacks, Prime Minister Kristersson noted that more funds need to be allocated to the agency, but specific figures were not shared (Fox News, 2023). Although Sweden has taken the first steps to protect itself from such campaigns, the agency has yet to make a significant impact due to restrictions on funding and personnel. Until these changes

are made, it is yet to be seen what the presence of the agency will do in terms of mitigating disinformation campaigns.

Conclusion

Sweden has serious shortcomings in its approach toward combatting cyberattacks and coordinated disinformation campaigns. Public interest in protecting the information space has risen, driving the creation of the SPDA. While a crucial first step, Russia's commitment to creating obstacles to Sweden's NATO accession demands a more cohesive approach toward combatting hybrid warfare tactics.

Case Study
Norway
Paulette Bussard

Introduction

As a long-time NATO member, Norway has been a critical supporter of Ukraine in its fight with Russia. Norwegian resources, most notably oil and gas, position Norway to supplant Russia as the alliance's most critical energy provider in Europe. Norway possesses significant deposits of rare earth minerals which form the bedrock of many advanced technologies and will reduce the alliance's reliance on China. Norway's pivotal role as one of the only energy-producing NATO member states makes its critical infrastructure a prime target for cyberattacks and espionage operations in the North Sea. While Norway has been diligent in protecting critical infrastructure, the scale of recent Russia's espionage activities calls for the implementation of innovative security methods. This case study focuses on the threats to Norway's critical infrastructure, especially those that might come because of Russia's recent espionage operations, examines Norway's responses, and proposes policy solutions.

Hybrid Threat Landscape

Espionage

Norway is an increasingly important energy provider within NATO as EU sanctions and poor relations reconfigure the European energy landscape. Extremely reliant on oil revenues, Russia is highly motivated to undermine Europe's energy security wherever it can. In late 2022, unidentified drones were spotted above Norwegian oil and gas extraction sites in the North Sea. Military experts assert that "espionage, sabotage, and intimidation" could be possible motives for the drone flights (AP News, 2022). More recently, intercepted communications and

confidential intelligence sources describe how Russian vessels collected information on Nordic critical infrastructure, including oil and gas fields, wind turbines, airports, and deep-water quays (Hou, Goodwin, Chernova, and Cotovio, 2023). Security experts worry that Russia's intelligence collection could be used to sabotage the undersea water cables that are critical for the operation of Norway's wind farms (Hou, 2023). Norway also recently arrested a Russian who was attempting to cross their shared border with drones, images, and video taken of Norwegian oil and drilling platforms (CBS News, 2022). Russian intelligence is clearly deploying a wide variety of assets to form a cohesive picture of Norway's energy critical infrastructure. As a result, oil and gas pipelines, ports, and critical transportation infrastructure are facing heightened security concerns because of Russia's espionage activities. As Norwegian energy infrastructure becomes even more critical to Europe and to NATO, the risks of espionage translating into sabotage will grow.

Cyberattacks

In June 2022, Norway's national data network was targeted by a cyberattack, taking down online services for both public and private sector entities for several hours. (Kagubare, 2022). Norway's National Security Authority (NSM) commented that "the attacks were aimed at a large number of Norwegian businesses that offer important services to the population" but specific victims were not disclosed (NSM, 2022). The attack was thought to be in retaliation for Norway preventing supplies bound for a Russian coal-mine settlement in the Arctic to transit Norwegian territory (AP News, 2022).

Disinformation

In August 2022, reports indicated that Beijing-linked campaigns were attempting to influence public opinion concerning Norway's extraction of its rare earth minerals. Norway recently discovered a large amount of "magnesium, niobium, cobalt, and rare earth materials [on] the European Commission's list of critical materials." (Paddison, 2023). Norway also has a wealth of graphite deposits (Go, 2022). These rare earth minerals are foundational to electric vehicle batteries, semiconductors, wind turbines, and other cornerstones of the modern, increasingly green, economy. Consequently, Norway's potential as a European hub for rare earth mineral extraction threatens China's continued dominance of the market; globally, nearly 63% of rare earths are sourced from China (Seligman, 2022). In response to Norway's movement to further develop these industries, China has spread disinformation that rare earth companies, including Lynas, are responsible for poor environmental and public health effects in the communities in which they operate. China's objective is clear: to undermine NATO-based processing and extraction firms and swing the balance of trade and development back in their favor (U.S. Department of Defense, 2022).

Response to Hybrid Threats

1. Actors

Both Russia and China are active hybrid threat actors in Norway. Russia is leveraging its cyber capabilities to punish Norwegian support for Ukraine, while engaging in considerable espionage operations to gather intelligence on Norway's energy critical infrastructure. On the other hand, China is focused on misleading the Norwegian public regarding the environmental and public health consequences of rare earth mineral extraction.

2. Policy Response

Norway has taken a hard line toward Russian espionage, expelling 15 Russian diplomats in April 2023, who Norway accused using their diplomatic cover to conduct intelligence activities. This episode, as well as Russia's maritime espionage, have driven Norway's Foreign Minister, Anniken Huitfeldt, to declare Russia "the greatest intelligence threat to Norway." Mrs. Huitfeldt also described how Norway is implementing measures to "counter Russian intelligence activities in our country," but failed to elaborate on specifics (Rasmussen, 2023).

Norway is also focused on countering efforts by Russia and China to control Europe's access to oil, gas, and rare earth minerals. Although an act of parliament is required to approve undersea mining projects, Norway is moving forward with legislation that will get these projects off the ground, thereby reducing reliance on foreign powers for natural resources. Finally, Norway's sovereign wealth fund, the largest in the world, has divested itself of Russia assets in the wake of Russia's war in Ukraine, signaling a long-term commitment to participating in a separate energy ecosystem.

3. Benefits and Obstacles

Increasing the mining of rare earth minerals off Norway's continental shelf Norway is not without cost. Chinese disinformation campaigns make it clear that China is motivated to thwart Norwegian ambitions to further develop its rare earths industry. Historically, China has withheld access to rare earths when diplomatic relations sour. For example, in 2010, after a fishing dispute between China and Japan, China "blocked exports to Japan of a crucial category of minerals used in products like hybrid cars, wind turbines, and guided missiles" including the export of raw earth oxides, salts and metals (Bradsher, 2010).

Norway, and the NATO alliance more broadly, are not yet prepared to alienate China entirely for fear of losing access to vital resources (Seligman, 2022). To lose China as a source of rare earth resources before mining in countries like Norway begins would undermine key industries across the alliance. The President of LKAB (an international mining group based in Sweden), states that "it will be at least 10-15 years before [Norway] can actually begin mining and deliver raw materials to the market" based on previous permit processes in the industry (LKAB, 2023). LKAB is currently working to implement the Critical Raw Materials Act within the EU. This act would allow for shorter permitting periods for mining operations, as well as assist in developing "national programmes for exploring geological resources" (European Commission, 2023). However, this act must be reviewed and approved by the European Parliament, as well as the Council of the European Union before it becomes official policy.

Conclusion

Norway occupies a key position within the Nordic region. Norway's longstanding NATO membership and its vast energy resources are critical to reducing the alliance's reliance on Russia and China. Expediting the approval of undersea mining projects is critical for resource security, but domestic and EU-level hurdles continue to delay the process. Furthermore, Norway must take care to protect its critical infrastructure in light of Russia's extensive intelligence gathering operations.

Case Study
Denmark
Alan Zheng

Introduction

Like the other Nordic countries, Denmark has been targeted by Russian cyberattacks, disinformation campaigns, and most recently, espionage of energy critical infrastructure. Examples of this type of hybrid warfare have been more common in the wake of Russia's war in Ukraine. Russian cyber and disinformation campaigns seek to undermine Denmark's stability and erode social unity, while espionage seeks to undermine Danish energy security. This case study focuses on the types of threats to Denmark across the spectrum of hybrid warfare, details Denmark's responses, and proposes several policy recommendations.

Hybrid Threat Landscape

Cyberattacks

Denmark ranks as one of the world's most cyber-secured nations, according to the Global Cybersecurity Index (NCSI, 2023). While Denmark has a high degree of cybersecurity across the public and private sectors, no nations is immune to coordinated efforts to penetrate digital infrastructure. In January 2023, the websites of eight banks, including Denmark's Central Bank, were targeted by Russian hackers with DDoS attacks (Reuters, 2023). Additionally, the websites of nine Danish hospitals, including regionh.dk, amagerhospital.dk, bispebjerhospital.dk, bornholmshospital.dk, were hit by similar attacks. The hacker group "Anonymous Sudan" later claimed responsibility (Martin, 2023). The group also attacked Danish airports the previous week, as well as an airport in Sweden. A Swedish cybersecurity firm TrueSec has claimed that the hacker group operated from

Russia, noting that their IP address was in Russia and that they used Russian to communicate on social media (The Local, 2023).

Disinformation

Denmark's experience with Russian disinformation began before Russia's war in Ukraine. Russian disinformation campaigns typically leverage social media to exploit social and political issues. Such campaigns tend to amplify existing controversies or manufacture new ones, fostering division and mistrust within Danish society. Sensitive topics such as immigration, minority rights, and populism are used by Russia weaken Denmark's social cohesion and undermine the credibility of its political system. There have been cases of Islamophobic "fake news" on Denmark's social media, such as Telegram and TikTok, that generate hostility toward migrants and Muslims. These disinformation campaigns are reminiscent of the Russian Internet Research Agency's proven tactics (SZAKÁCS And BOGNÁR, 2021). Furthermore, Russian state-controlled media outlets, such as RT (RT, 2017) and Sputnik have been found to publish articles exaggerating or fabricating incidents involving immigrants or refugees in Denmark (Kuznetsov, 2021).

Malign Influence and Economic Coercion

After Russia's war in Ukraine began, Denmark was cut off from Russian oil and natural gas when Denmark refused to pay for imports in rubles (Olsen, 2022). Denmark's dependency on Russian energy imports has driven Denmark to pursue renewable energy alternatives, particularly wind power. However, like Norway, public broadcasters in Denmark have reported instances of Russian espionage of Denmark's wind farms, with the potential intent to engage in sabotage (Afp, 2023).

Response to Hybrid Threats

1. Actors

Across the cyber, information, and intelligence domains, Russia is the primary threat actor targeting Denmark.

2. Policy Response

In response to the ongoing threat of cyberattacks against Denmark, the Danish government raised its cybersecurity alert level from “medium” to “high” and launched a new Danish national strategy for cyber and information strategy which aims to better protect digital infrastructure and IT-systems. The strategy also prioritizes strengthening Denmark’s participation in the international fight against cyber threats (DMoD, 2022). To implement the strategy, the government has allocated a total of DKK 270 million (EUR 36 million) to 34 separate initiatives running from 2022 until 2024 (Agency for Digital Government, 2021). These initiatives cover four strategic objectives:

1. Ensuring robust protection of vital societal functions.
2. Improving and prioritizing levels of skills and management in cyber and information security.
3. Strengthening the cooperation between the public and private sectors.
4. Actively participating in the international fight against cyber threats.

Conclusion

Denmark’s national strategy emphasizes that cybersecurity is a shared responsibility; neither government agencies nor private enterprises can handle it alone. Each sector contributes distinct strengths and resources. Denmark's cybersecurity strategy seeks to create a more robust and effective defense against cyber threats by fostering closer cooperation and knowledge sharing between these two sectors. It also provides a framework for the nation to construct a more

secure digital society, encouraging investments in new technologies and capabilities which can assist Denmark in maintaining its leadership position during the digital transition of society. In addition, it presents an opportunity to strengthen ties with international bodies, such as the EU, the United Nations, NATO, and like-minded nations, in the fight against cyber threats. These alliances can facilitate the sharing of information and take concerted action against shared threats.

Nordic Countries Conclusion and Policy Recommendations

The Nordic countries face similar threats, from Russian cyberattacks to coordinated disinformation campaigns to espionage targeting energy critical infrastructure. Thwarting NATO expansion, or at the very least, imposing costs on new NATO members, is clearly a Russian priority. While Russian-backed groups have had some limited success preventing NATO expansion, the overt nature of Russia operations is generating broad resentment toward Russia, driving formerly neutral countries further away. Due to the continued nature of Russian aggression, this paper recommends the following policy recommendations:

Policy Recommendations

1. **Increased oversight** of key energy installations in the North Sea by the NATO Security Committee. Energy Security and independence are increasingly important priorities, and the Nordic countries, as mentioned throughout this chapter, are the most likely sources of this energy. With "energy ministers from European countries… set to pledge to quadruple offshore wind energy by the end of the decade", the provision of security personnel to oversee both the construction of wind farms and pipelines is mandatory (Abnett, 2023). In light of increased presence of Russian spy ships as far away as Ireland, NATO has implemented the Critical Undersea Infrastructure Cell, which is aimed at protecting against sabotage of undersea cables and related infrastructure (Leahy, 2023). In a related vein, a more general NATO undersea rapid response force, which would be a permanent fixture in NATO defense response, could oversee physical and intelligence defense of critical underwater infrastructure.

2. **Implementation** of youth education programs on disinformation, overseen by the SPDA, the NATO Resilience Committee, and the ESSA Strategic Communications division. Finland has had great success mitigating the effects of disinformation among their populace due to early education programs aimed at teaching students how to dissect and identify the validity of media. As such, a similar program in countries like Sweden and Denmark, which are having an increasingly difficult time tackling disinformation campaigns, could benefit nations in the long term.
3. Acquisition of funds through NATO's Security Investment Program (SIP) toward **vouchers for implementation of cyber defense** among state-run and private companies alike. A similar program in Finland has aimed to increase the defense of data in what has been deemed sectors that are critical to Finland. However, the main problem that is facing many groups, including Finland, is the lack of funds to pursue these projects. (NATO, 2023).

Nordic Country Citations

Finland, Sweden, and Norway Citations:

Abnett, K. (2023, April 21). North Sea countries to pledge massive ramp up of wind energy—Draft. *Reuters*. https://www.reuters.com/business/energy/north-sea-countries-pledge-massive-ramp-up-wind-energy-draft-2023-04-21/

Bradsher, K. (2010, September 23). Amid Tension, China Blocks Vital Exports to Japan. *The New York Times*. https://www.nytimes.com/2010/09/23/business/global/23rare.html

Cotovio, L.-L. A. H., Allegra Goodwin, Anna Chernova,Vasco. (2023, April 19). *Fleet of Russian spy ships has been gathering intelligence in Nordic waters, investigation finds*. CNN. https://www.cnn.com/2023/04/19/europe/russia-spy-ships-nordic-waters-intl/index.html

Cyberattack hits Norway, pro-Russian hacker group fingered | AP News. (n.d.). Retrieved April 16, 2023, from https://apnews.com/article/russia-ukraine-technology-norway-government-and-politics-b837c155fde5d9cb4215b77dff9a94f0

Edvardsen, F. A. (n.d.). *Norway, Finland, and Sweden Increase Focus on the High North as Joint Operational Area*. Retrieved April 26, 2023, from https://www.highnorthnews.com/en/norway-finland-and-sweden-increase-focus-high-north-joint-operational-area

European Critical Raw Materials Act. (n.d.). [Text]. European Commission - European Commission. Retrieved May 16, 2023, from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1661

Europe's largest deposit of rare earth metals is located in the Kiruna area. (n.d.). LKAB. Retrieved April 27, 2023, from https://lkab.com/en/press/europes-largest-deposit-of-rare-earth-metals-is-located-in-the-kiruna-area/

Fears over Russian threat to Norway's energy infrastructure. (2022, October 23). AP NEWS. https://apnews.com/article/russia-ukraine-nato-norway-north-sea-moscow-16b497174d619bbddd7b004ccd31a909

Go, J. (n.d.). *Beijing-linked influence campaign takes aim at Western investors | fDi Intelligence – Your source for foreign direct investment information—FDiIntelligence.com*. Retrieved April 16, 2023, from https://www.fdiintelligence.com/content/feature/beijinglinked-influence-campaign-takes-aim-at-western-investors-81245

Information security voucher became hugely popular | Traficom. (n.d.). Retrieved May 6, 2023, from https://www.traficom.fi/en/news/information-security-voucher-became-hugely-popular

Jong, S., Sweijs, T., Kertysova, K., Bos, R., de Rave, R., Bindt, P., Klacansky, K., & Bekkers, F. (2017). *Finland* (INSIDE THE KREMLIN HOUSE OF MIRRORS, pp. 25–34). Hague Centre for Strategic Studies. https://www.jstor.org/stable/resrep12585.8

Kagubare, I. (n.d.). *Finland, Sweden's NATO moves prompt fears of Russian cyberattacks | The Hill*. Retrieved April 16, 2023, from https://thehill.com/policy/cybersecurity/3488518-finland-swedens-nato-moves-prompt-fears-of-russian-cyber-attacks/

Kagubare, I. (2022a, June 29). Norway hit with cyberattack, temporarily suspending service [Text]. *The Hill*. https://thehill.com/policy/cybersecurity/3541585-norway-hit-with-cyberattack-temporarily-suspending-service/

Kagubare, I. (2022b, August 10). Finland's parliament hit with cyberattack following US move to admit the country to NATO [Text]. *The Hill*. https://thehill.com/policy/technology/3595917-finlands-parliament-hit-with-cyberattack-following-us-move-to-admit-the-country-to-nato/

Kauranen. (n.d.). *Finns warm to NATO in alarmed reaction to Russian invasion of Ukraine | Reuters*. Retrieved April 16, 2023, from https://www.reuters.com/world/europe/finns-warm-nato-alarmed-reaction-russian-invasion-ukraine-2022-03-03/

Knuutila, A., Neudert, L.-M., & Howard, P. N. (2022). Who is afraid of fake news? Modeling risk perceptions of misinformation in 142 countries. *Harvard Kennedy School Misinformation Review*. https://doi.org/10.37016/mr-2020-97

Leahy, Pat. *Ireland likely to join Nato project to protect undersea cables*. (2023). The Irish Times. Retrieved May 16, 2023, from https://www.irishtimes.com/politics/2023/05/14/ireland-likely-to-join-nato-project-to-protect-undersea-cables/

Målrettede tjenestenektangrep mot norske nettsteder—Nasjonal sikkerhetsmyndighet. (2022, June 29). https://nsm.no/aktuelt/malrettede-tjenestenektangrep-mot-norske-nettsteder?fbclid=IwAR1DsHUYSoXSMWPP8n2cZu3tWHN2cnInwCOJ0fTfX3jcjLu_R4XHo5fXz6w

Mannes, M., & Mannes, M. (2023, February 14). Airline SAS network hit by hackers, says app was compromised. *Reuters*. https://www.reuters.com/business/aerospace-defense/airline-sas-suffers-cyber-attack-customer-info-leaked-2023-02-14/

Mission. (n.d.). The Swedish Psychological Defence Agency. Retrieved May 6, 2023, from https://www.mpf.se/en/mission/

Mohamed. (2023, February 9). IntelBrief: Disinformation Narratives Related to Sweden and Finland's NATO Applications. *The Soufan Center*. https://thesoufancenter.org/intelbrief-2023-february-9/

NATO. (n.d.-a). *Funding NATO*. NATO. Retrieved May 8, 2023, from https://www.nato.int/cps/en/natohq/topics_67655.htm

NATO. (n.d.-b). *Security Committee (SC)*. NATO. Retrieved May 8, 2023, from https://www.nato.int/cps/en/natohq/topics_69274.htm

Norway detains Russian at border with drones after reports of mystery drones near oil and gas facilities. (2022, October 14). https://www.cbsnews.com/news/norway-detains-russia-national-mysterious-drones-oil-gas-facilities/

O'Dwyer, G. (2023, January 17). *Nordic Council seeks deeper regional cybersecurity cooperation*. Defense News. https://www.defensenews.com/global/europe/2023/01/17/nordic-states-to-develop-common-cybersecurity-strategy/

Paddison, R., Laura. (2023, January 30). *Norway discovers huge trove of metals, minerals and rare earths on its seabed | CNN Business*. CNN. https://www.cnn.com/2023/01/30/business/norway-minerals-seabed-deep-sea-mining-climate-intl/index.html

Putin warns Finland NATO membership would harm relations. (2022, May 14). https://www.cbsnews.com/news/vladimir-putin-warns-finland-nato-membership-would-harm-relations/

Report: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem. (n.d.). *United States Department of State*. Retrieved May 6, 2023, from https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/

Reports of Disinformation Campaign Against Rare Earth Processing Facilities > U.S. Department of Defense > Release. (n.d.). Retrieved April 16, 2023, from https://www.defense.gov/News/Releases/Release/Article/3077280/reports-of-disinformation-campaign-against-rare-earth-processing-facilities/

Russian hackers target Finland's parliament. (2022, August 10). Cybernews. https://cybernews.com/cyber-war/russian-hackers-target-finland-parliaments-website/

Seligman, L. (2022, December 14). *China Dominates the Rare Earths Market. This U.S. Mine Is Trying to Change That.*POLITICO. https://www.politico.com/news/magazine/2022/12/14/rare-earth-mines-00071102

Suliman, A. (2022, January 24). Sweden sets up Psychological Defense Agency to fight fake news, foreign interference. *Washington Post*. https://www.washingtonpost.com/world/2022/01/06/sweden-fake-news-psychological-defence-agency/

SuomenEduskunta [@SuomenEduskunta]. (2022, August 9). *Eduskunnan ulkoisia verkkosivuja vastaan kohdistuu palvelunestohyökkäys. Hyökkäys alkoi tiistaina 9. Elokuuta noin klo 14.30. Eduskunta tekee toimia hyökkäyksen rajaamiseksi yhdessä palveluntoimittajien ja Kyberturvallisuuskeskuksen kanssa.* [Tweet]. Twitter. https://twitter.com/SuomenEduskunta/status/1557004264899510272

Sweden says claims that its agencies kidnap Muslim children is part of a systematized disinformation campaign. (2023, February 3). [Text.Article]. Associated Press; Fox News. https://www.foxnews.com/world/sweden-says-claims-agencies-kidnap-muslim-children-part-systematized-disinformation-campaign

Swedish paper says country lags behind on cyber security. (2021, August 3). *Dagens Nyheter (Stockholm, Sweden)*. Access World News – Historical and Current. https://infoweb.newsbank.com/apps/news/openurl?ctx_ver=z39.88-

2004&rft_id=info%3Asid/infoweb.newsbank.com&svc_dat=WORLDNEWS&req_dat=0D2A02882BC90595&rft_val_format=info%3Aofi/fmt%3Akev%3Amtx%3Actx&rft_dat=document_id%3Anews%252F18425A0B2175A4B0

Szumski, C. (2023a, February 15). *Sweden's main public TV broadcaster disrupted by cyberattacks*. Www.Euractiv.Com. https://www.euractiv.com/section/politics/news/swedens-main-public-tv-broadcaster-disrupted-by-cyberattacks/

Szumski, C. (2023b, February 23). *Threats from Russia, disinformation rises in Sweden*. Www.Euractiv.Com. https://www.euractiv.com/section/politics/news/threats-from-russia-disinformation-rises-in-sweden/

Think tank exposes Russia's malign operations to hinder Sweden's NATO accession. (2023, January 29). https://www.ukrinform.net/rubric-polytics/3661526-think-tank-exposes-russias-malign-operations-to-hinder-swedens-nato-accession.html

Times, T. M. (2023, April 4). *Russia Warns of 'Countermeasures' to Finland's NATO Membership*. The Moscow Times. https://www.themoscowtimes.com/2023/04/04/russia-warns-of-countermeasures-to-finlands-nato-membership-a80704

Ukraine War: Russia warns Sweden and Finland against Nato membership. (2022, April 11). *BBC News*. https://www.bbc.com/news/world-europe-61066503

What we can learn from Finland. (2023, March 1). Center for an Informed Public. https://www.cip.uw.edu/2023/03/01/finland-media-literacy/

Woollacott, E. (n.d.). *Sweden Launches Psychological Defense Agency To Counter Disinformation*. Forbes. Retrieved April 30, 2023, from https://www.forbes.com/sites/emmawoollacott/2022/01/05/sweden-launches-psychological-defense-agency-to-counter-disinformation/

Denmark Citations:

NCSI (2023). *Denmark's National Cyber Security Index.* Retrieved April 19, 2023, from https://ncsi.ega.ee/country/dk/

SZAKÁCS, J., & BOGNÁR, É. (2021, June). *The impact of disinformation campaigns about migrants and minority groups*. Retrieved April 19, 2023, from https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/653641/EXPO_IDA(2021)653641_EN.pdf

Bonnet, M. (2023, March 29). From Ukraine to the Whole of Europe: Cyber Conflict Reaches a Turning Point. *Business Wire*. Available from NewsBank: Access World News – Historical and Current: https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&docref=news/1908FA448B9BD8F8.

Olsen, J. M. (2022, June 1). *Russia cuts off natural gas supply to Denmark, Company says*. AP NEWS. Retrieved April 19, 2023, from https://apnews.com/article/russia-ukraine-putin-government-and-politics-netherlands-10923b26194d11c555f6176799465dd2

Richter, A. (2022, July). [MD] audiovisual code amended to prevent disinformation. [MD] AUDIOVISUAL CODE AMENDED TO PREVENT DISINFORMATION. https://merlin.obs.coe.int/article/9546

Reuters. (2023, January 10). Hackers hit websites of Danish Central Bank, other banks. Reuters. https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/

Martin, A. (2023, February 27). Danish hospitals hit by cyberattack from "Anonymous Sudan." The Record from Recorded Future News. https://therecord.media/danish-hospitals-hit-by-cyberattack-from-anonymous-sudan

Truesec. (2023, February 20). "Anonymous sudan": Most likely Russia disrupting Sweden's NATO application. Truesec. https://press.truesec.se/posts/news/anonymous-sudan-most-likely-russia-disrupting

DMoD. (2022, November 3). The Danish National Strategy for Cyber and Information Security - FMN.DK. Danish Ministry of Defence. https://www.fmn.dk/en/topics/cyber-security/danish-national-strategy/

Menn, J. (2023b, May 13). Cybersecurity faces a challenge from Artificial Intelligence's rise. The Washington Post. https://www.washingtonpost.com/technology/2023/05/11/hacking-ai-cybersecurity-future/

EU. (2019, April). Ethics guidelines for Trustworthy Ai. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Aachen. (2023, April 5). Denmark's S!RENEN public warning system uses Utimaco's u.warn solution. Professional cybersecurity solutions. https://utimaco.com/news/press-releases/denmarks-srenen-public-warning-system-uses-utimacos-uwarn-solution

Afp. (2023, April 19). Are Russian spy ships planning sabotage of Danish energy infrastructure?. The Local Denmark. https://www.thelocal.dk/20230419/are-russian-spy-ships-planning-to-sabotage-danish-energy-infrastructure

The Local. (2023, February 27). Danish hospital websites targeted in Cyber Attack. The Local Denmark. https://www.thelocal.dk/20230227/danish-hospital-websites-targeted-in-cyber-attack

Agency for Digital Government. (2021, December). The Danish National Strategy for Cyber and Information Security. Agency for Digital Government. https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/

O'Dwyer, G. (2023, March 21). Nordics move towards common cyber defence strategy: Computer Weekly. ComputerWeekly.com. https://www.computerweekly.com/news/365533113/Nordics-move-towards-common-cyber-defence-strategy

Kuznetsov, I. (2021, October 18). *Denmark says Non-Western immigration cost state nearly $5 billion per year*. Sputnik International. Retrieved April 19, 2023, from https://sputnikglobe.com/20211018/denmark-says-non-western-immigration-cost-state-nearly-5-billion-per-year-1089998506.html

RT. (2017, Nov 4). *Danish immigration minister flees deportation center chased by angry migrants (video)*. RT International. Retrieved April 19, 2023, from https://www.rt.com/news/408782-danish-minister-escapes-deportation-center/


POLAND AND
THE BALTICS
Estonia
Latvia
Lithuania
Poland

Case Studies

Poland and the Baltics

As the core of NATO's eastern flank, the Baltic states and Poland are often used as a laboratory for Russian hybrid warfare tactics. Decades of experience combatting Russian cyber, influence, and economic warfare operations have hardened each country's capabilities. However, Russia has escalated its efforts to undermine internal stability, create fissures in the NATO alliance, shape public opinion, impose economic hardship, and probe for weaknesses in the Baltic region as it increasingly falters on the battlefield in Ukraine. Russia is leveraging all the tools in its arsenal, especially coordinated cyberattacks and disinformation campaigns, to exert influence and propagate its favored narratives. China is also an increasingly active player, using its economic influence to advance its objectives in the Baltics, especially through its ownership of European financial institutions and transportation infrastructure. Independent of origin, hybrid warfare techniques are targeting not only the warfighter, but all of society. Therefore, a successful counter strategy must pursue a whole-of-society response to aggression below the threshold of war.

This section is organized by country, threat type, and response. It details the vectors of attack, most of which emanate from Russia, including cyberattacks, disinformation campaigns, and economic coercion. It then outlines how Poland and the Baltics are responding to these threats, which actors are involved, and what policies are being deployed to combat Russian hybrid warfare. China features only slightly, but with immense capabilities and economic clout, monitoring China's hybrid activities is important. Finally, policy recommendations for each country are offered in the conclusion. These policies are designed to harden defensive cyber capabilities, enhance societal resilience in the face of disinformation, limit Russian

and Chinese economic influence, and engage society in developing responses to these ongoing threats.

Case Study
Poland
Jack Kaltreider

Introduction

As the war in Ukraine enters a new phase, Poland is increasingly NATO's most vital logistics hub. High-tech arms, support personnel, and sustainment bound for Ukraine flow through its ports, airports, and railways. Russia has recognized Poland's centrality to NATO's continued support of Ukraine, increasingly targeting Poland with cyberattacks. Russia has also escalated its efforts to influence Polish domestic politics through disinformation campaigns and economic coercion, seeking to cultivate domestic resentment toward Ukrainian refugees in Poland.

Poland has responded vigorously to Russian hybrid threats across domains. Poland has prioritized securing its cyberspace by adopting a decentralized system of CSIRTs tasked with detecting, identifying, and preventing threat actors from harming Polish digital infrastructure. Poland has also formed new military units to counteract Russian information operations and has collaborated energetically with its EU partners to diminish Russia's economic influence in the region.

Nonetheless, Poland will remain a principal target of all the tools in Russia's hybrid warfare arsenal for as long as Russia's war in Ukraine persists. This case study details the Russia's hybrid activities in Poland, describes Poland's response, and proposes several policies at the end of the section designed to limit Russia's ability to destroy and degrade allied infrastructure, propagate disinformation, and coerce Poland by using economic leverage.

Hybrid Threat Landscape

Cyberattacks

Poland's centrality to NATO's support of Ukraine makes its critical infrastructure a ripe target for cyber operations by Russian state and state-backed actors seeking to impede the humanitarian and war efforts. In 2022, a cyberattack took place in Poland every 9 minutes, with many targeting critical infrastructure, including utilities, healthcare, transportation, and IT service providers (ITA, 2023). Disrupting critical infrastructure can have enormous consequences. In March 2022, 80% of the Polish railway network was rendered inoperable, halting the flow of refugees from Ukraine, and disrupting the movement of weapons and supplies into the country. While not considered the result of a cyberattack — a "data coding flaw" was said to be the culprit — the impact of rendering railways inoperable demonstrated how costly these actions can be for the war effort (Reuters, 2022). With battlefield gains becoming more costly in blood and treasure, Russia is increasingly exploiting cyber vulnerabilities across the spectrum of Poland's critical infrastructure to impede the war effort and to punish Poland's support of Ukraine.

In late 2022, Microsoft's Threat Intelligence Center (MSTIC) identified a ransomware campaign targeting the country's transportation and logistics industries. This attack was linked to IRIDIUM, a Russian-allied actor affiliated with the notorious, state-sponsored Sandworm hacker group. The attack used Sandworm's "Prestige" ransomware to extract "highly privileged credentials," such as domain admin privileges, and provide system access. This allowed the hackers to covertly monitor the functioning of key systems and to disrupt them at a future date to maximize damage (*New 'Prestige' Ransomware Impacts Organizations in Ukraine and Poland,* Microsoft, 2022). A similar attack occurred in March 2023, with a series of cyberattacks on public and private entities in industries from transportation to finance to IT in Poland, Romania, and Türkiye. Microsoft acknowledged that these attacks were the result of a zero-day vulnerability in

Microsoft Outlook, enabling threat actors to escalate admin privileges by using a phishing attack that required no user interaction (Jones, 2023). APT28, a Russian-linked threat actor, has been linked to the attacks.

These attacks are but two recent examples of malicious actors penetrating the systems that operate critical infrastructure, with escalation of privilege (EoP) exploits a favored tactic. However, critical infrastructure is not the only target. With Russia's war in Ukraine increasingly involving NATO countries, Poland is now the target of more Russian cyberattacks than any country besides the United States (*A Year of Russian Hybrid Warfare*, Microsoft, 2023). Furthermore, the scope of these attacks has broadened: attacks now not only seek to impede the war effort, but to undermine the Polish state. For example, after the Polish parliament declared Russia a terrorist state, its website was targeted by a distributed denial of service (DDoS) attack, preventing citizens from accessing public information (Russian Cyberattacks, 2022). A similar DDoS attack occurred in March 2023, targeting Poland's tax filing system (Reuters, 2023). These attacks demonstrate that Russia's aim is not only to influence the war effort, but also to punish Poland for its support of Ukraine by challenging the state directly. This style of broad-spectrum hybrid warfare can also be seen in Russia's coordinated disinformation campaigns.

Disinformation

With the influx of over three million Ukrainian refugees into Poland, watchdogs have observed efforts to stoke ethnic tensions between Poles and Ukrainians (Kamubski and Sliwa, 2023). This has been done by amplifying the niche views of several far-right Polish MPs who fear the "Ukrainianization of Poland" is taking place, eroding their society and culture (Warsaw Institute, 2023). A separate disinformation campaign, targeting displaced Ukrainians, promoted purportedly

leaked government documents stating that Ukrainian men in Poland could be conscripted for the war effort (*A Year of Russian Hybrid Warfare*, Microsoft, 2023). Another campaign, widely disseminated on social media after a Ukrainian anti-air missile killed two Polish citizens, alleged that Poland intended to annex three Ukrainian territories near the Polish border (Salvo, 2022). Collectively, these tactics leverage mainstream media channels to polarize target constituencies by feeding them false or misleading information. By seeking to drive wedges between Poles and Ukrainians, Russia hopes to erode support both for Ukraine and for NATO within Polish society.

Russia also favors using cyber and disinformation campaigns in tandem, targeting Polish government websites and the personal accounts of politicians. In one instance, a Polish government website was impersonated, publishing a fabricated government memo claiming that the President of Poland had signed an executive order to transfer funds to Polish citizens. The website solicited personal and financial information which was compromised before the website could be taken down (*Russian Cyberattacks*, 2022). Another common disinformation tactic is the "hack-and-leak." This typically involves compromising the personal devices of prominent politicians, doctoring photos or texts, and sharing them on popular social media channels to amplify internal divisions and create wedges between Poland and external partners. The most notorious hack-and-leak operations have been conducted by a group known as Ghostwriter, thought to be backed by the GRU. Active since 2017, this group has been responsible for a series of email leaks, including thousands of leaked emails from Poland's Prime Minister, alleging judicial conspiracy (Ibid, 2022). In many ways, these leaks represent Russian hybrid warfare at its best: state-backed, yet deniable, cyberattacks target public officials with phishing and other attacks designed to compromise sensitive accounts. This

information is then leaked and picked up by the press, undermining confidence in public officials. In this specific case, some opposition party officials believe the documents to be legitimate, as opposed to doctored by Russian intelligence services. Regardless of this claim's veracity, the domestic discord created plays directly into the Kremlin's hands by muddying the waters of public debate. Such operations are likely to continue ahead of Poland's elections later this year to sow further division and potentially influence the outcome.

Economic Coercion

Since losing access to Russian gas from the Yamal-Europe pipeline shortly after Russia's war in Ukraine began, Poland has taken measures to diversify its energy relationships and make investments in nuclear and renewable energy infrastructure. Russia has responded to these actions creatively, seeking to influence the behavior of Poland and other NATO countries through other means.

Late last year, Russia agreed to the establishment of a humanitarian corridor in the Black Sea, allowing shipments of Ukrainian grain to countries around the world to ameliorate a growing food shortage. The agreement has only been partially effective, with Russia taking every opportunity to exercise its newfound leverage. While complying with the agreement, Russia has been known to deliberately delay the inspections of vessels bearing Ukrainian wheat in the Black Sea, delaying shipments, and increasing export risk (Khan, 2023). Consequently, Ukrainian farmers began exporting substantial amounts of agricultural products to neighboring countries like Poland, Hungary, and Slovakia to avoid Russian bottlenecks in the Black Sea. The grain was supposed to transit through these countries on its way to more distant markets, but further logistical issues created a glut of cheap grain in the countries bordering Ukraine, undercutting local farmers.

Under pressure from farmers, a powerful constituency in Poland's upcoming elections, Poland unilaterally banned the import and transit of numerous Ukrainian agricultural products on Saturday, April 15th, 2023. Hungary and Slovakia quickly followed suit.

The EU rejected the authority of these countries to unilaterally conduct external trade policy, while Poland argued that they can act due to a "security clause" (Gera, 2023). Poland and Ukraine later reached an agreement that only allows Ukrainian grain to transit through the country. However, it remains unclear how this will be enforced or what will happen if further logistical issues impede the movement of these goods (Strzelecki and Wkidarczak-semczuk, 2023). Russia remains primed to further leverage the humanitarian corridor and other wedge issues to create fissures between Ukraine and some of its closest allies with Polish elections and an expected Ukrainian counteroffensive on the horizon.

Response to Hybrid Threats

Response to Cyber Threats

1. **Actors**

Most threats to Poland in cyberspace emanate from the Russian Federation and have targeted critical transportation and energy infrastructure, government websites and officials, and the private sector to cause economic damage, probe for weakness, and undermine Poland's internal stability. Killnet and Sandworm are among the most active advanced persistent threat (APT) groups that operate with the backing of the Kremlin. In response, Poland has focused on institutional overhaul and capacity building by creating and consolidating institutions responsible for ensuring its cyber defense. It has also developed a specialized

Cyber Defense Force and has appropriated considerable funding for technology procurement and workforce development.

2. Policy Response: Threat Detection, Identification, and Prevention

As a frequent proving ground for Russian cyberwarfare, Poland has placed emphasis on maintaining internal stability and ensuring the uninterrupted provision of essential services, with critical infrastructure of central importance (Toumi, 2022). In the face of these threats, Poland outlined five goals in its Cybersecurity Strategy for 2019-2024[1]:

1) Development of a national cybersecurity system
2) Increasing resilience of information systems in the public and private sectors by developing the capacity to respond to and report incidents.
3) Increase capacity by developing new technologies.
4) Build public awareness and competence in cybersecurity.
5) Build a strong international position in the area of cybersecurity.

In service of these goals, Poland implemented the EU's NIS Directive in 2017, electing to deploy a decentralized approach to defending Polish cyberspace by granting authority to three national cybersecurity incident response teams (CSIRTs), each with their own areas of focus. CSIRT GOV, part of Poland's Internal Security Agency (ISA), identifies, prevents, and detects threats against government bodies and critical infrastructure systems in the civil sector (CSIRT GOV, 2023). It responded to more than 100,000 incidents between 2015-2019, a third of which were cyber threats (Kamubski and Sliwa, 2023). CSIRT MON is run by the Ministry of Defense and manages incident reporting for all entities "subordinate to or supervised by the Minister of National Defense" including information and communication technology (ICT) systems in critical infrastructure with national defense relevance (Government

[1] Zagórski, Marek. "CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND, Page 10" n.d.

of Poland, 2019). CSIRT MON is also the single point of contact for NATO. Finally, CSIRT NASK focuses on conducting research in the field of cybersecurity, collaborating with Poland's allies and partners abroad, and coordinating incident response for operators of essential services, excluding critical infrastructure (CSIRT NASK, 2023). It also spearheaded the implementation of ARAKIS-GOV alongside the ISA.

Collectively, these entities are at the core of Poland's cyber defense, acting proactively to mitigate cyber risks and to detect, identify, and prevent threats. Furthermore, each CSIRT is authorized to inspect software and equipment to identify vulnerabilities that could affect national security and advise on corrective recommendations (Toumi, 2022).

2B. Policy Response: Investments in the Workforce and Emerging Technologies

Poland has invested extensively to develop both the manpower and the tools to defend its cyberspace. In 2019, Poland launched its CYBER.MIL.PL program with the intent of building a dedicated cyber defense force (CDF) with defensive, reconnaissance, and offensive capabilities (Polskie Radio, 2022). Poland now deploys full-time units modeled after US Cyber Command and has dedicated 791M USD from its "Technical Modernization Plan," which runs through 2026, to procure "modern cryptographic and IT equipment" for the CDF ("Poland Details $49.8 Billion Military Modernization Plan 2026"). Moreover, Poland established a National Cybersecurity Centre (NCSC), headed by the same commander as the CDF, to integrate the National Cryptology Center and IT Inspectorate. By consolidating the various entities throughout the government under one leader, Poland hopes to streamline its cyber defense.

Response to Disinformation

1. Actors

Poland is subject to agile and persistent disinformation campaigns emanating from the Russian Federation. Disinformation in Poland has most recently sought to stoke tensions between Poles and Ukrainians, undermine faith in the Polish state, and influence the outcome of elections. In response, Poland has conducted anti-disinformation education campaigns, partnered with the EU to deliver strategic communications, and added a new branch to its military that fights disinformation as part of its mandate.

2. Policy Response

Numerous agencies within Poland are seeking to counter disinformation. Poland's Internal Security Agency, the same that runs CSIRT GOV, has responded by ramping up education efforts. Over 58,000 participants took 2,600 counterintelligence courses between 2015 and 2019, which emphasized awareness and resilience (Kamubski and Sliwa, 2023). Poland's Ministry of Foreign Affairs has also created a Strategic Communications department that partners with the European Rapid Alert System, which "exchanges information on a number of misinformation cases and related trends on a daily basis" (Prague Security Studies Institute, 2020). Finally, in 2015 Poland formed a fifth branch of its military, the Territorial Defense Forces (TDF), which augments Poland's professional soldiery. It is made up of both professional and part-time volunteers and now numbers over 30,000, with a goal of achieving 50,000 members in the coming years. Importantly, there is a Cyber Operations Team embedded within the TDF that combats disinformation as part of its mandate. It consists of mostly volunteers with day jobs

in IT and information security who want to contribute to Polish national security (Wojsko Polski, 2019).

Response to Economic Coercion

1. **Actors**

In early 2022, Poland was cut off from Russian coal and gas supplies. The Polish agricultural industry has also been adversely affected by Russia's weaponization of the Black Sea humanitarian corridor. In response, Poland has delayed its transition away from fossil fuels, partnered with the United States to diversify its domestic energy supply, and invested in renewable generation capacity and infrastructure.

2. **Policy Response**

Before Russia's war in Ukraine, several Polish coal mines were to be shuttered, with a complete phaseout planned for 2049. This was part of a broader commitment to reduce greenhouse gas emissions and develop renewable alternatives. The war put a stop to these plans, delaying the shuttering of coal mines and the winddown of coal-fired power plants. Production was even increased ahead of the winter in 2022 to meet energy demand. These plants are now due to remain active at least until the first of three nuclear reactors, built in partnership with the United States, comes online in 2033 (Krzysztoszek, 2022). Finally, Poland continues to make investments in renewable energy such as offshore wind, and modern electric grids leveraging 5G network connectivity to reduce dependence on its hostile neighbor and further integrate with the EU.

Conclusion

Poland faces more cyberattacks than any NATO state other than the US and is a frequent target of disinformation campaigns that seek use Ukrainian refugees to divide Polish society. Poland has responded to these threats by developing a comprehensive cybersecurity strategy, combatting disinformation through intentional public awareness campaigns, and seeking to distance itself from Russia economically. Poland's threat environment will remain tense for as long as Russia's war in Ukraine persists.

Case Study
Lithuania
Jack Kaltreider

Introduction

Lithuania is home to a critical land corridor used by Russia to provision its Kaliningrad exclave, where Russia's Baltic fleet is based. This makes Lithuania a common target for Russian cyberattacks when tensions rise. Russian disinformation campaigns targeting Lithuania's sizeable Russian speaking population are also prevalent. However, the greatest threats to Lithuanian security owe to the country's continued reliance on Soviet-era infrastructure for electricity transmission and rail transit. Lithuania's existing connection to the BRELL transmission network will remain a liability for at least another year, while Lithuania's continued use of the 1520mm broad rail gauge undermines economic connectivity with the EU as well as NATO interoperability.

Additionally, Lithuania's support of Taiwan has caused a notable diplomatic row with China. As a result, Lithuanian exporters have been denied access to Chinese markets, and Lithuanian authorities have been subjected to intense coercive measures intended to pressure Lithuania into adopting Beijing's worldview.

This case study examines the hybrid threats to Lithuania, emanating from both Russia and China. Lithuania's responses have been broadly successful and should serve as a template for a successful response to hybrid warfare tactics. As such, policy recommendations are provided for the NATO alliance using Lithuania as a model at the end of the Baltics section.

Hybrid Threat Landscape

Cyberattacks

In 2021, Lithuania's national-level computer emergency response team (CERT.LT) recorded 4,088 cyber incidents, with a growing share being designated as "medium or high impact." The most common targets were hosting providers (53%), internet service providers (20%), and critical information infrastructure (16%). Malware and phishing attacks defined the threat environment, representing 46% and 29% of all documented attacks, respectively. (Key Trends and Statistics of the National Cybersecurity Status of Lithuania, 2022). However, since Russia's war in Ukraine began, the threat environment has shifted. Data theft and DDoS attacks have skyrocketed, with the latter representing over 75% of global cyberattacks. There were 45 documented DDoS attacks directed at Lithuania between the start of the war and the end of Q1 2023, the sixth most in Europe (Thales 2022-2023: A Year of Cyber Conflict in Ukraine, 2023).

As seen in the Polish case, one common pattern of attack deployed by Russia is to respond to unfavorable government policies directed at Russia with cyberattacks. In the summer of 2022, Lithuania experienced a wave of DDoS attacks, striking railways, airports, media companies, and government ministries. These attacks brought down websites and compromised secure networks. This attack followed a limited restriction imposed by Lithuania on cargo transiting the country to the Kaliningrad exclave in accordance with EU sanctions due to Russia's war in Ukraine. The notorious Russian hacker group, Killnet, later claimed responsibility (Reuters, 2022). Besides the cyberattack, dueling narratives propagated by Russia sought to drive a wedge between Lithuania and the EU. At the time of the cyberattacks, Russia claimed that there was a complete blockade of

Kaliningrad. Lithuania cited that only 1% of cargo was being restricted in accordance with the few EU sanctions that came into force. At the time, some in Lithuania considered the ban to be so insignificant as to insist that it did not exist at all, while the head of Russia's Security Council vowed retaliation that would have "a serious negative impact on the population of Lithuania" (Higgins, 2022). Lithuania went on to fully enforce EU sanctions on goods while allowing unimpeded transit of Russians to the exclave. This flare-up is one example of how Lithuania's proximity to Kaliningrad continues to make it vulnerable to outsized Russian aggression as the war in Ukraine continues.

Disinformation

Lithuania faces a coordinated assault on its information space. Disinformation campaigns emanating from Russia are well-orchestrated, emphasizing similar underlying narratives across media channels. Common threads include statements that Lithuania is a state run by Nazis, that NATO "occupiers" pose risks to the Lithuanian people, and that Lithuania ought to pursue better relations with Russia (Key Trends and Statistics of the National Cybersecurity Status of Lithuania, 2022).

In 2021, Lithuania documented 5,030 discrete incidents of misleading information disseminated across media platforms. In January 2022 alone, 583 incidents were detected. (STRATCOM, 2022). These campaigns often blend the hacking of government websites with the dissemination of false information, mirroring the Polish case. Lithuania has documented at least nine attacks carried out in Lithuania's cyberspace attributed to Russia's Ghostwriter campaign, which hacked or imitated trusted government websites and altered content to propagate false narratives. Russia has also been charged with hacking the social media of

public officials and the creation of fake accounts, both done to spread disinformation. TV, radio, and blogs are other common vectors of spreading disinformation favored by the Kremlin (Bankauskaite and Deividas, 2023).

Economic Coercion

The primary levers of Russian economic coercion in Lithuania are the country's reliance on the BRELL transmission network and Lithuania's continued use of the Soviet-era rail gauge. Both grant Moscow enhanced influence in its near abroad, allowing it to control power transmission in Lithuania and to implicitly impede NATO interoperability. During periods of geopolitical tension, BRELL countries are vulnerable to power interruptions. Since the closure of its Ignalina nuclear power plant, Lithuanian power imports have generated strong revenues for Moscow while also forming a vital link to Kaliningrad. Aware of this vulnerability, Russia has taken measures to ensure Kaliningrad's power supply for when Lithuania eventually exits BRELL in 2025 (Juozaitis, 2021). This threatens Lithuania because Kaliningrad's electricity independence allows Russia to use Lithuania's existing connection as a bargaining chip without cutting off the power supply to the exclave. For this reason, the expeditious synchronization with EU power systems, as well as continued projects with Poland, Finland, and Sweden, are national security priorities for Lithuania to avoid being subject to Russian economic coercion.

The Soviet-era rail gauge is less of a bargaining chip that Russia can leverage than it is a historically contingent impediment to Lithuania's military and economic integration with the rest of the European continent. Currently, Lithuania operates a 1520mm broad rail gauge, as opposed to the 1430mm standard rail gauge used by the EU and most of NATO. The exception is a single rail line that links Poland to the Lithuanian city of Kaunas. Trains operating on different gauges are incompatible,

necessitating a transfer or shift to other ground-based transit options when moving equipment and personnel. This would hinder NATO's ability to surge troops and equipment to Lithuania in the event of a significant attack by Russia. Lithuania's use of the 1520mm rail gauge also hinders its ability to move goods across borders to other EU countries, reducing opportunities for trade (Maisel and Keturakis, 2018).

Recently, China has sought to use its economic influence to pressure Lithuania to publicly adopt Beijing's preferred worldview. In November 2021, Lithuania permitted the opening of a "Taiwanese Representative Office" in its capital, Vilnius. Both the fact that it was opened at all, as well as the fact that it used the term "Taiwanese" instead of "Taipei" sparked outrage in Beijing. China swiftly responded with a suite of measures designed to punish Lithuania, including downgrading diplomatic relations, expelling Lithuanian diplomats from the country, and enforcing unofficial sanctions on Lithuanian goods exported to China (Janeliunas and Boruta, 2022). These actions demonstrate that China retains a variety of tools to coerce countries that it sees as acting against its national interest.

Response to Hybrid Threats

Response to Cyber Threats

1. **Actors**

Lithuania attributes most state-sponsored cyberattacks to Russia, accounting for over 58% of global state-sponsored malicious cyber activity (Burt, 2021). Lithuania has also identified Chinese hardware companies as potential vectors for malicious cyber activity. In response, Lithuania has developed a regulatory environment that encourages cyber vulnerability disclosures, reformed its procurement process for critical infrastructure, and created a sectoral CERT tasked

with detecting, identifying, and protecting against the most critical threats to Lithuanian cyberspace.

2. Policy Response

Lithuania ranks sixth in the world (4th in Europe) in defense cyber capabilities, according to the Global Cybersecurity Index (Key Trends and Statistics of the National Cybersecurity Status of Lithuania). Lithuania owes its proficiency in this space to a clear regulatory environment that incorporates the knowledge of its citizens, robust oversight by relevant authorities, and decades of experience defending itself from Russian cyberattacks. On the regulatory level, Lithuania has incorporated the efforts of the cybersecurity community into the nation's defense by enshrining the "responsible disclosure of vulnerabilities in communication and information systems (CIS) that could otherwise be exploited for a cyber-incident" into the country's legal code (Lithuanian Ministry of Defense, 2020). This framework enables ethical hacking that contributes to a more secure Lithuanian internet and provides certainty for "white hats," providing legal protection if they find and duly report vulnerabilities. Lithuania likens this vulnerability disclosure model to the way citizens report potholes, downed powerlines, or cracked pavement tiles — just another reporting mechanism in service of the public interest.

Lithuania has also taken proactive measures to deter and defend against cyberattacks on its critical infrastructure by reforming its procurement process. Fully leveraging the benefits of 5G, smart meters and grids, and renewable energy requires accounting for the vulnerabilities these systems introduce. Lithuania's Ministry of Defense has spearheaded this process, assessing over 200 objects of procurement related to critical information infrastructure (CII) in 2021. The goal is to prevent unreliable manufacturers from providing technologies to the over 500

designated CII entities deemed critical for national security. Lithuania has specifically focused on Chinese-made technology provided by Huawei and others. The NSCS conducted a systematic review of 5G smart devices made by Chinese manufacturers, identifying critical vulnerabilities on several devices related to manufacturer-installed apps (Cybersecurity Status, 2022). Collectively, these efforts to secure Lithuania's supply chain are world-class and should be models for other allied countries.

Lithuania has also observed that the complexity and sophistication of attacks is increasing year-over-year, necessitating new ways of combatting cyber threats. Lithuania has responded to this new threat environment by creating MIL CERT, which focuses on "preventing and responding to cyber incidents in the National Defence Network (NDN) more effectively." Lithuania has found that sectorial CERTs are more effective at combatting the most sophisticated attacks on the most critical pieces of Lithuanian infrastructure. MIL CERT responded to an average of one cyber incident per day in 2021 and seeks to further reduce incidents by emphasizing user awareness across the NDN (Cybersecurity Status, 2022).

Response to Disinformation

1. **Actors**

Following the annexation of Crimea, Lithuanian experts raised alarms about Russian disinformation campaigns targeting the country and its Russian-speaking communities. Russian troll farms are notorious for flooding social media with fake accounts, comments, and videos promoting pro-Kremlin narratives. In response, Lithuania primarily has chosen to combat disinformation similarly to the way it protects its cyberspace: by engaging the Lithuanian public. Additionally, strategic

communications and comprehensive education campaigns have played major roles in Lithuania's response to disinformation.

2. **Policy Response**

Lithuania benefits from the ingenuity and awareness of its own citizens, who have taken it upon themselves to combat the industrial-scale disinformation produced by Russia's troll farms. These "elves," so-called because "elves fight trolls" are volunteers who monitor social media for obviously fake or misleading information and report it to the publishers, escalating the review process that leads to account bans and de-platforming (Abend, 2022). Lithuania's success in the face of the omnipresent attempts by the Kremlin to shape the information space is owed not only to its embrace of citizen activism, but also to Lithuania's whole-of-society approach to information literacy. The Ministry of Defense actively promotes public awareness about its military posture to avoid misunderstandings, while also engaging in "education campaigns on potential risks to Lithuanian citizens" (Bankauskaite and Deividas, 2023). The Ministry of Foreign Affairs has taken a similar approach, routinely clarifying its positions on international issues to its own citizenry and to the EU to keep a firm hand on the information space. Furthermore, Lithuanian think tanks, media fact checkers, NGOs, and the Ministry of Defense all work in concert to understand current trends in Russian disinformation campaigns and to leverage new techniques and technologies, including artificial intelligence, to better detect, flag, and take down fake content.

Response to Economic Coercion

1. **Actors**

Russia has economic leverage over Lithuania via Soviet-era infrastructure, most notably the BRELL transmission network and Lithuania's 1520mm broad rail

gauge. China has also used its economic clout to punish Lithuania for its close relations with Taiwan. In response, Lithuania has committed to exiting the BRELL network by 2025 or earlier and is a proponent of the Rail Baltica project to connect the capitals of Finland, Estonia, Latvia, Lithuania, and Poland on one, modern, EU standard rail line. Furthermore, Lithuania has acted to counter Chinese economic coercion by further developing its partnership with Taiwan.

2. Policy Response

By being connected to the BRELL network, Lithuania is reliant on Russian grid operators to balance and transmit power. In 2018, Estonia, Latvia, and Lithuania signed a deal to "decouple from the BRELL circuit and join the continental power grid by 2025" (Sytas, 2023). This would deny Russia the opportunity to use the flow of power as a bargaining chip. This concern has become more salient as Russia's failures on the battlefield are leading Russia to target NATO countries supporting Ukraine. Lithuania is pushing hard to decouple as soon as 2024 and is in the process of conducting a feasibility study to see if this is possible (Ibid, 2023).

Like with the BRELL network, the Soviet-era infrastructure also plays a role in Lithuanian transportation and logistics. The 1520mm broad rail gauge has negative impacts on economic development and NATO interoperability. To address these concerns, Lithuania, along with Finland, Estonia, Latvia, and Poland, have partnered with the EU on the *Rail Baltica* project to connect the capitals of these countries using the EU standard rail gauge. Progress is being made on this project, but the initial completion date of 2025 is no longer possible, with new completion estimates quoting a wide range from 2026 to 2030.

Finally, Lithuania's response to China has mostly been to not respond to Chinese pressure. The projected costs of China's informal ban on Lithuanian

exports, paired with foregone investment, amount to between .3 and 1.3% of GDP in 2023 (Janeliunas and Boruta, 2022). This is far from trivial, but so far Lithuania has preferred to continue to develop its relationship with Taiwan and to partner even more closely with the United States. In return, Taiwan has offered to help Lithuania expand its nascent semiconductor industry, with investments targeting assembly and packaging (Ibid, 2022).

Conclusion

Lithuania owes its success at combatting hybrid warfare tactics to its forward-thinking regulatory regime, the commitment of its citizens to controlling their information space, and to proactive infrastructure projects that seek to distance the country from its Soviet legacy.

Case Study
Latvia
Shern Sze Lim

Introduction

Russia's invasion of Ukraine has been accompanied by an increase in the number of hybrid threats across the EU. With Latvia's compromised critical infrastructure and a significant number of Russian speakers, Moscow has deployed cyberattacks and disinformation campaigns to sow social disruptions. This case study begins by introducing Latvia's hybrid threats such as cyberattacks and disinformation campaigns before and up to Russia's invasion of Ukraine. It proceeds with a hybrid threat assessment and a policy analysis. Finally, specific policy recommendations are provided to protect Latvia's cyber and national security.

Hybrid Threat Landscape

Cyberattacks

Latvia's critical infrastructure such as the electricity grid, along with other Baltic countries, is highly vulnerable to cyberattacks by Russia. Even before Latvia's transfer from the Russian electricity-dependent BRELL (Belarus, Russia, Estonia, Latvia, and Lithuania) Network to the EU-based ENTSO-E (European Network of Transmission System Operators for Electricity) Network in 2017, Russian hackers had attacked a Baltic electricity grid using distributed denial of service (DDoS) attack (Reuters, 2017). A similar attack targeted a major petrol distribution network in the Baltics, disrupting petrol operations in Latvia and elsewhere (Reuters, 2017). These attacks demonstrate hackers' interest in exploiting weaknesses in Baltic's critical infrastructure and presaged more significant attacks. Cyberattacks skyrocketed when Russia invaded Ukraine in 2022, with documented attacks increasing by 40%.

Attacks on Latvia's public sector have since quadrupled. (Constitution Protection Bureau (SAB), 2022).

In July 2022, the Russian state-backed hacking group, Killnet, targeted Latvia's public broadcasting center using a distributed denial-of-service (DDoS) attack. This was in response to Latvia's announcement of the demolition of almost 300 Soviet monuments in Latvia (Antoniuk, 2022). This caused a 12-hour disruption of the network's operations.

In February 2023, Russian cyber espionage group Gamaredon conducted a phishing attack on Latvia's Ministry of Defense. Hackers impersonated Ukrainian government officials and sent out malicious emails to Latvia's government officials to gain sensitive information (Antoniuk, 2023). According to Ukraine's CERT, "Gameradon'' is classified as an Advanced Persistent Threat (APT) and is associated with the largest number of cyberattacks on Ukraine (Security Service of Ukraine, 2021).

These attacks highlight that Latvia's pursuit of independent electric grids is not sustainable. This is because proliferation of IoT, 5G networks, and smart grids that improve connectivity comes with increased vulnerability. As described by Rafael Leal-Arcas, Filipa Santos, and Danai Papadae of the University of London: "The proliferation of IoT smart grids has opened many possible routes through which the function of a grid can be compromised: electric vehicles, smart meters, thermostats, and home appliances all could potentially be vulnerable access points of entry to the grid" (Bervell, 2022). Looking ahead, Latvia's security system must adopt structural technological changes to prevent attacks from happening in the future.

Disinformation

Beyond cyberattacks, Latvia is also impacted by Russian disinformation campaigns. With almost 25% of the Russian ethnic population in Latvia receiving news from the Russian state media, this demographic easily transmits disinformation to other Latvian communities (Cooliscan, 2021). A telling example is Russia's disinformation campaign on the 2022 Saeima elections. Russian media used fear-mongering tactics such as tying anti-Russia content to "Nazism", portraying the Latvian government as "Russophobic," and NATO as an imperial power that oppresses the will of ethnic Russians (SAB, 2022). Though Russia failed to interfere with Latvia's elections, its propaganda had a far-reaching effect. After the election, 45.7% of the Russian-speaking households in Latvia had a negative perception regarding NATO's presence in Latvia and 41% of them believed that Russia's interventions in other countries are justified and necessary (SAB, 2022). On Russia's social media presence, the Russian Embassy used platforms such as Telegram to defame the Latvian government and share pro-Kremlin foreign policy reports to justify its "defensive operations" in Ukraine (SAB, 2022). With disinformation enhanced during times of uncertainty, this makes propaganda ever more digestible, threatening Latvia's social unity.

Response to Hybrid Threats

1. Actors

Russia is the key cyber actor threatening Latvian's critical infrastructure and public institutions (SAB, 2022). A recent report by Microsoft Threat Intelligence ranked Latvia the 5th most targeted country by Russia's cyber operations, just behind the United States, Poland, the United Kingdom, and Lithuania between February 2022 and February 2023 (Microsoft, 2023). As Russia expands cyberattacks on Ukraine's allies, the Latvian government's IT Security Incident

Prevent Incident (CERT.LV), Constitution Protection Bureau (SAB), and NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) should work together to produce a cohesive cyber defense strategy.

2. **Policy Response**

With the increased sophistication and adaptability of Russian cyberattacks, Latvia's CERT.LV should adopt cyber early warning systems with AI and virtualization technology.

3. **Benefits and Obstacles**

The adoption of next generation CEWS is beneficial to counter two emerging cyber threats from Russia. The first trend is Russia's use of ransomware as deniable destruction weapons (Microsoft, 2023). Early warning and intrusion detection systems combined with AI methods (FIDes) mitigate this risk as it detects malware attacks on a wide area and at a fast speed (Seker, 2019). Detection accuracy is also enhanced by reducing the number of false positives often occurring in the classical approach of anomaly-based intrusion detection system (IDS). This AI technology also goes beyond intrusion detection by providing practical assistance and instructions to defend against cyberattacks (Lohmann, 2022). This protection is especially important to Latvia's energy sector and the increase of smart grids because any disruption to the supply chain compromises NATO's defense line. However, the effectiveness of AI based EWS still depends on the adaptability of cyberattacks. While such CEWS is at its nascent phase, continued R&D is necessary to adopt a combination of technologies that can produce long-term predictive capabilities of Latvia's cyber defense.

The second emerging Russian cyber threat is its ability to gain initial access through diverse means (Microsoft, 2023). This is evident where Russian hackers targeted private “IT providers to reach more sensitive targets downstream without immediately triggering alerts'' (Microsoft, 2023). CEWS with AI mitigates this risk as it enhances wide scale intrusion detection systems. Specifically, it creates a nonlinear response capable of disorienting attackers while also allowing observers to track attackers’ tactics in real time (William, 2020). This limits hackers’ ability to gain initial access that threatens the entire supply chain. However, this technology would still be vulnerable against adversarial AI that can identify recurring defenses.

In addition, CEWS should be coupled with allied cyber operation exercises to gain cybersecurity shared intelligence. This provides the framework to enhance information sharing, interoperability, and logistical support across EU and NATO cyberspace in real time (Lohmann, 2022). This helps to build a NATO wide comprehensive cyber defense knowledge exchange and cohesive cyber trust models that increase resiliency (Lohmann, 2022). While Latvia’s cyber joint operations with NATO allies are just in its nascent stages, collaboration should increase from a yearly basis to a quarterly basis. This frequency is justified by the intensity of cyberattacks on Latvian public institutions. Specifically, there were 450 attacks on 50 public authorities in 2022 and more than 220 attacks in the first four months of 2023 (ENG.LSM.lv). CEWS and monthly joint operations support the development of a robust centralized cyber communication infrastructure and intelligence sharing among NATO nations. However, the increase of CEWS also means higher exposure to cyberattacks on critical infrastructure. This reveals CEWS’s nature as a double-edged sword: cyber vulnerabilities can be both aggravated and alleviated by the advancement of next generation CEWS.

Conclusion

As Latvia works to gain energy security independent of Russian influence, it is exposed to a higher degree of hybrid threats from cyberattacks on government institutions and electrical grids. Latvia has taken practical steps to mitigate cyber risks through investing in new technologies at key institutions such as CERT.LV, SAB, BRELL network, and the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). However, Latvia must continue to invest in detection capabilities through CEWS with virtualization and AI to combat more sophisticated cyber actors. This technology allows Latvia to gain cyber resilience by preventing cyberattacks before they begin. In addition to new technological policies, Latvia can enhance cyber resilience by increasing cyber joint operations to boost shared intelligence. As highlighted, the combination of both CEWS and joint operations may raise cyber exposure to cyber threats. Yet, such a collaborative cyber strategy is necessary considering Latvia's limited resources and historical dependence on neighboring countries to safeguard national security.

Poland and the Baltics Conclusion and Recommendations

As its military falters on the battlefield, Russia is increasingly leveraging its hybrid warfare capabilities to erode support for Ukraine. Russia uses cyberattacks as punishment for policies it finds unfavorable, as well as to damage and degrade allied capabilities by targeting critical energy and information infrastructure. Coordinated disinformation campaigns accompany attacks in cyberspace, seeking to stoke ethnic and historical tensions and undermine the internal security of the targeted countries. Moreover, Russia is reluctant to relinquish its historic superiority, and consequent leverage, attained from its dominant position in the European energy market. As countries seek to diversify their energy relationships and develop renewable energy resources, Russia is poised to take all measures below the threshold of war to prevent European energy independence. China, while a comparably minor hybrid warfare actor in the Baltics and Poland, retains significant and growing capabilities to shape the cyber, information, and economic domains in the region. The Baltic states, Poland, the EU, and NATO must remain vigilant and share best practices in order to remain resilient in a rapidly changing threat environment. The following policy recommendations position Poland and the Baltics to address existing gaps and continue to lead NATO's efforts to be more secure in the face of hybrid warfare tactics.

Policy Recommendations:

Poland and the Baltic states have proven capable of defending against Russian, and to a much lesser extent, Chinese, hybrid warfare tactics. However, there are forward-looking opportunities for these countries to develop resilient infrastructure and institutions. First, national governments should seek to counter one of the favored tactics of cybercriminals, which is to compromise IT providers.

These companies are ripe targets because they often have delegated access to the sensitive systems of hundreds if not thousands of entities in both the public and private sectors. Successful escalation of privileges (EoP) attacks enable remote access not only to the systems of the IT provider, but to those of their clients. These can be used to extract, alter, or delete sensitive data, as well as to compromise other systems downstream. This vulnerability category should be addressed at a national level.

Recommendation 1:

A. Encourage national governments to empower their CERTs or CSIRTs to implement and provide funding for the development of standards for IT providers contracting with entities classified as being critical information or energy infrastructure operators.
B. Following the establishment of standards, national governments should require all IT service providers contracting with entities classified as being critical information or energy infrastructure operators to undertake a mandatory security audit to be completed by the nationally recognized CERT/CSIRT.
C. Following the audit, the national CERT/CSIRT should provide a list of requirements based on the audit that are needed for the IT service provider to meet the national standard. The exact timeframe for implementation is to be determined by respective national governments.

Recommendation 2:

Establishing standards is only valuable if the tools used to defend critical energy and information infrastructure match the threat environment. To achieve long-term cyber defense, Latvia should collaborate with both the NATO Science and

Technology Organization (STO) and NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) to implement next-generation CEWS. To expedite cyber technology implementation across the EU, a streamlined funding process between STO and NATO budget should be considered. Additionally, next-generation CEWS should be coupled with cyber joint operations. NATO-wide cyber operations would facilitate an accountability mechanism to foster common knowledge of the latest risk analysis, best practices, and also practical instructions to protect critical infrastructure.

Recommendation 3:

Finally, while Rail Baltica is a good step toward enhancing Lithuania's economic and military connectivity, it will also be a priority target for Russian cyber and kinetic attacks in the event of a conflict, as it would be the primary network used to surge NATO assets to the region. Alternative EU standard rail networks in Lithuania are mostly non-existent, presenting a significant impediment to NATO interoperability by hindering troop movements and sustainment. Replacing the entire network (and its trains) is impracticable, however, these governments should take urgent action to minimize the security risks presented by operating on a non-EU standard rail system. Lithuania's rail system will remain vulnerable until it more broadly diversifies its rail gauge to provide alternative methods of moving soldiers and equipment in the event of a conflict. Following the completion of Rail Baltica, which uses the EU standard gauge, Estonia, and Lithuania should jointly apply for EU mobility financing to replace the 20% of the existing, non-Rail Baltica network to diversify transportation networks and to enable "rapid surge capability" of allied forces in the event of a Russian incursion (Maisel and Keturakis, 2018).

Poland and the Baltics Work Cited

Poland and Lithuania:

Abend, L. (2022, March 5). *Meet the Lithuanian 'Elves' Fighting Russian Disinformation*. Time. https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine/

BankMuscat, D., & Deividas, S. (n.d.). *Lithuania's Total Defense Review*. National Defense University Press. Retrieved May 9, 2023, from https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323902/lithuanias-total-defense-review/https%3A%2F%2Fndupress.ndu.edu%2FMedia%2FNews%2FNews-Article-View%2FArticle%2F3323902%2Flithuanias-total-defense-review%2F

Burt. (n.d.). *Russian cyberattacks pose greater risk to governments and other insights from our annual report—Microsoft On the Issues*. Retrieved May 9, 2023, from https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/

Butrimas, V. (n.d.). *Defending critical infrastructure: The challenge of securing industrial control systems*.

Connect the Dots on State-Sponsored Cyber Incidents—Sandworm. (n.d.). Council on Foreign Relations. Retrieved April 17, 2023, from https://www.cfr.org/cyber-operations/sandworm

CSIRT MON. (n.d.). Retrieved May 9, 2023, from https://csirt-mon.wp.mil.pl/en/

Cyber.mil.pl—We develop Poland's abilities to fight threats in cyberspace—Ministry of National Defence—Gov.pl website. (n.d.). Ministry of National Defence. Retrieved May 9, 2023, from https://www.gov.pl/web/national-defence/cybermilpl-we-develop-polands-abilities-to-fight-threats-in-cyberspace

Defending Ukraine: Early Lessons from the Cyber War. (2022, June 22). Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Florkiewicz, P., Strzelecki, M., & Wkidarczak-semczuk, A. (2023, April 18). *Ukraine agrees with Poland on grain transit, but Black Sea deal in doubt | Reuters* [News Outlet]. Reuters. https://www.reuters.com/world/europe/poland-ukraine-resume-grain-transit-talks-2023-04-18/

Gera, V. (2023, April 17). EU investigates after 3 countries ban Ukraine grain imports. *Associated Press: Worldstream*. Access World News – Historical and Current. https://infoweb.newsbank.com/apps/news/openurl?ctx_ver=z39.88-2004&rft_id=info%3Asid/infoweb.newsbank.com&svc_dat=WORLDNEWS&req_dat=5571AD5ADB7245A884D175640FB2C7D8&rft_val_format=info%3Aofi/fmt%3Akev%3Amtx%3Actx&rft_dat=document_id%3Anews%252F190F65000387F610

Higgins, A. (2022, June 27). Lithuania blames Russia for cyberattacks, citing threats over cargo restrictions. *The New York Times*. https://www.nytimes.com/2022/06/27/world/europe/lithuania-russia-cyberattacks.html

How Ordinary Lithuanians Are Fighting Russian Disinformation | Time. (n.d.). Retrieved April 19, 2023, from https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine/

https://www.studiox.bg. (2023, May 5). *What would it cost Estonia to switch from Russian to European railway gauge? | TheMayor.EU*. https://www.themayor.eu/en/a/view/what-would-it-cost-estonia-to-switch-from-russian-to-european-railway-gauge-10970

Hybrid CoE Working Paper 18: Defending critical infrastructure: The challenge of securing industrial control systems. (n.d.). *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats*. Retrieved April 18, 2023, from https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-18-defending-critical-infrastructure-the-challenge-of-securing-industrial-control-systems/

In training with Poland's volunteer militia. (2018, October 18). *Reuters*. https://www.reuters.com/article/us-poland-nationalism-militia-idUSKCN1MS1OP

julija. (2020, September 10). Lithuania starts work to create legal framework for ethical hackers. *LR Krašto Apsaugos Ministerija*. https://kam.lt/en/lithuania-starts-work-to-create-legal-framework-for-ethical-hackers/

Juozaitis, D. J. (2021). *Baltic States' Synchronisation with Continental European Network: Navigating the Hybrid Threat Landscape*.

Kamubski, M., & Sliwa, Z. (2023, March 10). *Poland's Threat Assessment: Deepened, Not Changed*. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323942/polands-threat-assessment-deepened-not-changed/https%3A%2F%2Fndupress.ndu.edu%2FMedia%2FNews%2FNews-Article-View%2FArticle%2F3323942%2Fpolands-threat-assessment-deepened-not-changed%2F

Keturakis, A. M., Laurynas. (2018, April 2). *Baltic Trainspotting: Railways and NATO's Logistics Problem in Northeastern Europe*. Modern War Institute. https://mwi.usma.edu/baltic-trainspotting-railways-natos-logistics-problem-northeastern-europe/

Khan, Y. (2023, February 22). Ukraine Grain Shipments Slow as Export Deal With Russia Nears End. *Wall Street Journal*. https://www.wsj.com/articles/ukraine-grain-shipments-slow-as-export-deal-with-russia-nears-end-dedc00d0

Lertpakdeewong, M. (2022, July 27). *Lithuania's Confrontation with China Over Taiwan: Lessons from a Small Country*. Global Taiwan Institute. https://globaltaiwan.org/2022/07/lithuanias-confrontation-with-china-over-taiwan-lessons-from-a-small-country/

National Cyber Security Strategies—Interactive Map. (n.d.). [NCSS Map]. ENISA. Retrieved May 9, 2023, from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

New "Prestige" ransomware impacts organizations in Ukraine and Poland. (2022, October 14). *Microsoft Security Blog*. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Nowikowska, M. (2022). The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland. In K. Chałubińska-Jentkiewicz, F. Radoniewicz, & T. Zieliński (Eds.), *Cybersecurity in Poland: Legal Aspects* (pp. 223–241). Springer International Publishing. https://doi.org/10.1007/978-3-030-78551-2_15

Outage disrupts Polish trains as Ukrainian refugees head west | Reuters. (n.d.). Retrieved April 17, 2023, from https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/

Outlook zero day linked to critical infrastructure attacks. (n.d.). Cybersecurity Dive. Retrieved April 17, 2023, from https://www.cybersecuritydive.com/news/zero-day-vulnerability-outlook-critical-infrastructure/645196/

Pancevski, B. (2023, February 10). Second Suspect in Germany Intelligence Breach Was Questioned in U.S. *Wall Street Journal*. https://www.wsj.com/articles/second-suspect-in-germany-intelligence-breach-was-questioned-in-u-s-1915d6df

Poland creates cyberspace defence force—English Section—Polskieradio.pl. (n.d.). Retrieved May 9, 2023, from https://polskieradio.pl/395/7784/artykul/2898356,poland-creates-cyberspace-defence-force

Poland Details $49.8 Billion Military Modernization Plan 2026. (n.d.). Retrieved May 9, 2023, from https://www.defensemirror.com/news/24383/Poland_Details__49_8_Billion_Military_Modernization_Plan_2026#.ZFqio3ZlAQ8

Poland ICT Cyberattacks in Poland take place every 9 minutes. (n.d.). Retrieved April 18, 2023, from https://www.trade.gov/market-intelligence/poland-ict-cyberattacks-poland-take-place-every-9-minutes

Poland says Russian hackers attacked tax website. (2023, March 1). *Reuters*. https://www.reuters.com/world/europe/poland-says-russian-hackers-attacked-tax-website-2023-03-01/

Poland to slow coal phase-out process, maintain 2049 end-date. (2022, November 8). Www.Euractiv.Com. https://www.euractiv.com/section/energy/news/poland-to-slow-coal-phase-out-process-maintain-2049-end-date/

Polish Cyber Defenses and the Russia-Ukraine War. (n.d.). Council on Foreign Relations. Retrieved April 17, 2023, from https://www.cfr.org/blog/polish-cyber-defenses-and-russia-ukraine-war

Rasmussen, S. E. (2023, April 13). Norway to Expel 15 Russian Diplomats Accused of Espionage. *Wall Street Journal*. https://www.wsj.com/articles/norway-to-expel-15-russian-diplomats-accused-of-espionage-aede77e2

Reuters. (2023, April 16). EU warns against unilateral steps after Poland, Hungary ban Ukrainian grain. *Reuters*. https://www.reuters.com/world/europe/polish-ban-ukrainian-grain-food-imports-apply-transit-says-minister-2023-04-16/

Russian Cyberattacks. (n.d.). Special Services. Retrieved April 18, 2023, from https://www.gov.pl/web/special-services/russian-cyberattacks

Russian hackers claim responsibility for cyberattack on Lithuania. (n.d.). Retrieved May 9, 2023, from https://www.aljazeera.com/news/2022/6/27/russia-hackers-claim-responsibility-for-cyber-attack-on-lithuania

Russian spy ships suspected of gathering intelligence in Nordic waters, investigation finds | CNN. (n.d.). Retrieved May 23, 2023, from https://www.cnn.com/2023/04/19/europe/russia-spy-ships-nordic-waters-intl/index.html

Salvo, D. (2022, December 5). Oh, the Irony…Russia Spreads Disinformation about Polish Annexation of Western Ukrainian Regions. *Alliance For Securing Democracy*. https://securingdemocracy.gmfus.org/oh-the-ironyrussia-spreads-disinformation-about-polish-annexation-of-western-ukrainian-regions/

Significant Cyber Incidents | Strategic Technologies Program | CSIS. (n.d.). Retrieved April 18, 2023, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Team, T. C. S. I. R. (n.d.). *The Computer Security Incident Response Team*. The Computer Security Incident Response Team. Retrieved May 9, 2023, from https://csirt.gov.pl/cee

telecommunications, N.-S. of. (n.d.). *CSIRT NASK*. NASK - Sense of telecommunications. Retrieved May 9, 2023, from https://en.nask.pl/eng/activities/csirt-nask/3424,CSIRT-NASK.html

Territorial Defence Forces—Ministry of National Defence—Gov.pl website. (n.d.). Ministry of National Defence. Retrieved May 7, 2023, from https://www.gov.pl/web/national-defence/territorial-defence-forces

Ukraine's bumper grain exports rile allies in eastern EU. (2023, April 14). *POLITICO*. https://www.politico.eu/article/ukraine-grain-glut-cause-poland-support-waver-war-russia/

US Cyber Forces as a Model for the Polish Ones. (2022, March 28). *Warsaw Institute*. https://warsawinstitute.org/us-cyber-forces-model-polish-ones/

Warsaw, I. (2023, March 2). Policy Brief. Kremlin Watchers Movement Report. *Warsaw Institute*. https://warsawinstitute.org/policy-brief-kremlin-watchers-movement-report/

WOT zaczyna budowę komponentu "CYBER." (n.d.). Wojsko-Polskie.Pl. Retrieved May 9, 2023, from https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2019-06-102-wot-zaczyna-budowe-komponentu-cyber/

Zagórski, M. (n.d.). *CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND*.

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)—Ministerstwo Cyfryzacji—Portal Gov.pl. (n.d.). Ministerstwo Cyfryzacji. Retrieved May 9, 2023, from https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt

Latvia:

A year of Russian hybrid warfare in Ukraine. (n.d.). https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

Antoniuk, D. (n.d.). Pro-Kremlin hackers target Latvia's parliament after declaring Russia a sponsor of terrorism. https://therecord.media/pro-kremlin-hackers-target-latvias-parliament-after-declaring-russia-a-sponsor-of-terrorism

Antoniuk, D. (n.d.). Latvia confirms a phishing attack on the Ministry of Defense, linking it to a Russian hacking group. https://therecord.media/latvia-confirms-phishing-attack-on-ministry-of-defense-linking-it-to-russian-hacking-group

CONSTITUTION PROTECTION BUREAU OF THE REPUBLIC OF LATVIA 2021 ANNUAL REPORT. (n.d.). https://sab.gov.lv/files/Public_report_2021.pdf

CONSTITUTION PROTECTION BUREAU OF THE REPUBLIC OF LATVIA 2022 ANNUAL REPORT. (n.d.). https://www.sab.gov.lv/files/Public_report_2022.pdf

Coolican, C. (n.d.). The Russian Diaspora in the Baltic States: The Trojan Horse that never was. https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Russian-Diaspora-Baltic-States.pdf

CYBERSECURITY: INCREASED VIGILANCE AT ALL LEVELS. (n.d.). https://www.luxembourgforfinance.com/portfolio/cybersecurity-increased-vigilance-at all-levels/

Cyber attacks on Latvian public sector quadrupled last year. (n.d.). https://eng.lsm.lv/article/society/defense/26.04.2023-cyber-attacks-on-latvian-public-sector-quadrupled-last-year.a506410/

Derek, M. (n.d.). Estonia, Latvia, and Lithuania: Background and U.S.-Baltic Relations.

https://crsreports.congress.gov/product/pdf/R/R46139https://crsreports.congress.gov/product/pdf/R/R46139

William, D. (n.d.). How AI can help improve intrusion detection systems.

https://gcn.com/cybersecurity/2020/04/how-ai-can-help-improve-intrusion-detection-systems/


SOUTHEASTERN EUROPE
Romania
Moldova
Bulgaria
Türkiye

Case Studies

Southeastern Europe: Moldova, Romania, Bulgaria, and Türkiye

Introduction

The rise of hybrid warfare has introduced a new set of challenges to countries worldwide, and Moldova, Romania, Bulgaria, and Türkiye are no exception. Sitting in between Europe and the Middle East, these countries face hybrid warfare threats that require a deep understanding of their distinctive security landscape.

Moldova, being a landlocked country in between Romania and Ukraine, encounters hybrid threats stemming from geopolitical positions and internal complexities. The ongoing conflict in Transnistria has left Moldova susceptible to disinformation campaigns, cyberattacks, and economic coercion which in turn have caused political instability. Romania is a key NATO member of the Eastern border of the European Union and because of that, it experiences cyberattacks targeting critical infrastructure, disinformation campaigns aimed at bringing political unrest, and malign influence from outside factors seeking to exploit societal dynamics. Romania's proximity to the Black Sea region has further exposed the nation to threats due to regional power struggles and geopolitical tensions. As for Bulgaria, the cyberattacks on critical infrastructure and energy networks pose great risks to Bulgaria's security and economy. Additionally, disinformation has heightened ethnic tensions amongst groups within and around Southeastern Europe. Lastly, Türkiye has experienced a vast number of threat challenges specifically tied to their military capabilities and regional influence.

The hybrid warfare threats faced by Moldova, Romania, Bulgaria, and Türkiye underscore the need for advanced strategies to protect their cybersecurity and political stability. With an awareness of the vulnerabilities present, policymakers

can prioritize measures like promoting media literacy and enhancing cybersecurity capabilities. These changes can fortify the country's defenses, ensure resilience of society, and shield national sovereignty.

Case Study
Moldova
Alan Zheng

Introduction

Moldova, as a country bordered by Romania and Ukraine, is at the frontline facing Russia's hybrid warfare, experiencing multiple waves of disinformation, cyberattacks, malign influence, and economic coercion campaigns. Russia's hybrid warfare in Moldova has primarily aimed to undermine the country's sovereignty, stability, and integration with Western institutions like the European Union and NATO. Similar disinformation campaigns can be observed in other European countries that have been affected by the hybrid warfare, for instance, flooding propaganda on TV channels, radio, and social media that agitate the legitimacy of Russia's invasion of Ukraine. As one of the poorest countries in Europe, Moldova is having trouble finding qualified cybersecurity experts to improve its national cybersecurity to fight against the current hybrid warfare. Though NATO stepped in to assist the country in enhancing its cybersecurity capabilities in January 2021, one year earlier before the invasion happened (NATO, 2021), Moldova still has a relatively low national cybersecurity index among other countries, with a ranking of 53rd in 2021 (European Commission, 2022). When Russia's hybrid warfare started, it dropped to 73rd, according to the National Cybersecurity Index database. As a response to the disinformation and a social cohesion campaign, the European Commission issued €8 Million to strengthen Moldova's resilience (European Commission, 2022).

Hybrid Threat Landscape

Cyberattacks

Moldova has suffered more cyberattacks from Russia due to its location and its close relationship with NATO and the EU. Its government and critical infrastructure were hit by waves of cyberattacks since the Russia-Ukraine War began. It has been largely impacted by Russia “using energy, cyberattacks, staging protests, and other disruptive activities” to destabilize the nation, according to Moldovan President Maia Sandu during one of the recent joint press conferences (Bir, 2023). Since the first quarter of 2022 when the invasion started, Moldova and Montenegro have been increasingly targeted by pro-Russian hacktivist groups, and the percentage of cyberattacks increased from 0.7% to 2.7% at the end of 2022. Besides disinformation, manipulation of public opinion, economic warfare, sabotage, and guerrilla tactics, massive waves of DDoS attacks targeting critical infrastructure and government websites can be observed, leading to more data leaks and theft, and espionage (Bonnet, 2023).

As a close partner with NATO and the neighboring country of Ukraine, Moldova's location and loyalty are important to NATO security. Data theft and espionage by Russia are likely to lead to NATO’s intelligence leakage.

Disinformation

Russia’s hybrid warfare against Moldova can be traced back to a period before the Russian-Ukraine War. Moldova has faced a disinformation campaign since the 2020 presidential election (EUvsDisinfo, 2021). There was a disinformation trope about “threatened values” attacking Maia Sandu, the female presidential candidate of the election. Such disinformation spread the notion that “(Sandu)… as

an unmarried woman, she would undermine the institution of the family". This came from the Moldovan Orthodox Church, which subordinated to the Russian Patriarchate. After the invasion started, the Moldova TV channels, radio, and social media faced major challenges from Russian propaganda, seeking to manipulate public opinion and undermine the country's political stability. One notable aspect of Russia's propaganda in Moldova involves promoting anti-EU and anti-NATO narratives. Russian media outlets and social media accounts have frequently portrayed these organizations as threats to Moldovan sovereignty and cultural identity. By emphasizing the negative aspects of Europeanization and NATO membership, such as potential economic hardships or loss of traditional values, Russia seeks to create doubt and fear among the Moldovan public regarding closer ties with the West. According to a research paper, "Eighty-five percent of Moldovans take their information from TV, and 57 percent consider it as their main source of information; about 40 percent consider it the most trustworthy source of information" (Boulègue et al., 2018). As a result, a video of Romania massing military equipment on the Moldovan border has reached more than 300,000 views on Telegram, which was, in fact, an "old footage that was just recast as something new" (Bond, 2023). Such inaccurate videos and disinformation are common on social media platforms. Moldova has no effective method to counter such disinformation campaigns posted on social media.

Moreover, Russian disinformation campaigns focused on targeting Moldova's history and identity, seeking to promote a narrative of shared Slavic heritage and historical ties with Russia. These campaigns often exploit existing divisions between the majority Moldovan population and the Russian-speaking minority, aiming to deepen ethnic tensions and drive a wedge between different communities within the country. Meanwhile, Russian propaganda and disinformation campaigns tend

to discredit pro-European politicians and parties by accusing them of corruption, incompetence, or even treason, further polarizing Moldovan politics and weakening the country's democratic institutions.

As a result, Moldova has suspended six TV channels, which were First in Moldova, RTR Moldova, NTV Moldova, and TV6 (Euronews, 2022), that have released disinformation on the Russia-Ukraine War as "… part of a fresh wave of sanctions against Russia." (Al Jazeera, 2022).

Response to Hybrid Threats

In the past decades, Moldova has faced serious threats from disinformation campaigns, especially after the annexation of Crimea by Russia in 2014. It has been clear that "Moldova appears to be one of the main battlefields of NATO-Russia information confrontation." (Baggiani, 2021). Considering Moldova's economy, international bodies like the United Nations, the European Union, and NATO have taken the responsibility to help Moldova in multiple aspects. In order to help Moldova develop its cybersecurity system to fight against Russian propaganda and disinformation campaigns, NATO provided funding to establish a new Cyber Incident Response Capability. At the same time, NATO founded a Cyber Response Capability Center in the capital of Moldova (NATO, 2021). After the Ukraine war started, Moldova was again hit by waves of anti-Ukraine disinformation. As the Russian threat intensified, anti-refugee videos began spreading from TikTok to Facebook (Meaker, 2022). The EU also provided financial support of €8 Million to strengthen its resilience from the pro-Russian disinformation campaign, and malign influence, as well as its capability of receiving Ukrainian refugees (European Commission, 2022). Though there has not been an invasion on Moldovan territory, there are nearly 1,500 Russian military personnel stationed in the breakaway region

of Transnistria. The defense minister Anatolie Nosatii stated that "(Moldova)…is subject to 'hybrid warfare generated by Russia' in a bid to 'overthrow state power'" (Euronews, 2023).

Besides international bodies, Moldova has sought support from the United States to solve the repercussions of the Ukraine war in the areas of economics, energy, security, and defense (DOS, 2023). Nearly $300 million has been promised to help Moldova overcome the impacts of the war and a further $300 million aid was planned for energy assistance to eliminate Russian malign influence (DOS, 2023). To counter disinformation campaigns and cyberattacks, Moldova has expressed the need to "continue enhancing cooperation on cybersecurity and digital transformation, strengthening capacities to counter and prevent cybercrime and related crimes, and implementing national cyber defense policies" with the United States' technical cooperation. On June 2, 2022, the Moldovan Parliament adopted a set of amendments to the Audiovisual Code (see IRIS 2019-3/24) that received the title: "Law on counteracting disinformation and propaganda" (Richter, 2022). The amendment forbade to "broadcast in the national audiovisual space audiovisual programs that constitute speech that incites hatred, disinformation, propaganda of military aggression, extremist content, terrorist content or content that poses a threat to national security". (CSOMETER, 2022) Accompanied by the amendment, the Moldovan government announced the banning of Russian TV news and political analysis, which have not ratified the Convention on Transfrontier Television, to fight against Russian propaganda in June (Reuters, 2022). On December 10th, 2022, Moldova temporarily banned six TV channels First in Moldova, RTR Moldova, Accent TV, NTV Moldova, TV6, and Orhei TV for airing "incorrect information about the country and Russia's war in Ukraine" (Reuters, 2022).

According to an assessment report of Moldova National CIRT, the Moldovan government is currently focused on implementing a Computer Incident Response Team (CIRT/CERT) which enables better conditions for greater security and trust in digital space (ITU, 2022). This implementation was part of its National Strategy for Information Society Development “Digital Moldova 2020”, created in 2015. The project aims to implement a governmental CERT and a military CERT. Many countries have developed their own emergency response team around the world, for instance, the United States (US-CERT), the United Kingdom (UK-CERT), India (CERT-In), Australia (AusCERT), and many others. It is a vital component of a nation’s cybersecurity because it facilitates critical information sharing about potential vulnerabilities and ongoing threats among governmental agencies, private entities, and the Moldovan public, fostering a broad culture of cybersecurity awareness. Moreover, implementing a CIRT allows the Moldova government to participate in vital global cybersecurity cooperation efforts, sharing and receiving threat intelligence, and coordinating responses to transnational cyber incidents.

However, the Moldovan government still faces challenges while implementing a national CIRT. As one of Europe's less developed nations, resource constraints can be a significant issue, as establishing and sustaining a robust CIRT requires a substantial investment in terms of both financial resources and qualified personnel. Furthermore, jurisdictional issues can confound response efforts, particularly in the context of international cyber threats. Building effective relationships with the private sector, which often owns and operates critical infrastructure, is another obstacle, as these entities may be hesitant to share information about security incidents out of liability or reputation concerns. These challenges highlight the need for ongoing investment, collaboration, and capacity building in Moldova's cybersecurity efforts with international bodies like NATO and

the EU. An increased focus on the partnership with the United States would be beneficial to Moldova's cybersecurity goals as well. Overall, the implementation of the national CIRT offers Moldova a significant improvement in cybersecurity and demonstrates the nation's dedication to bolstering its defenses against cyber threats, a crucial step for the protection of its cybersecurity and national interests.

Conclusion

Moldova, as one of the less developed countries in Europe, heavily relied on international bodies like NATO and the EU for assistance in improving its cyber security capabilities against Russian disinformation campaigns and cyberattacks. The United States has offered financial and strategic assistance to help Moldova overcome the obstacles and malign influence of the Ukraine War. The idea of a national Cyber Incident Response Team (CIRT) has been introduced to Moldova, which is commonly used in other NATO countries. NATO also established a new Cyber Response Capability Center in the capital of Moldova due to its geopolitical factor being sandwiched between Romania and Ukraine. Moldova is also at the frontline of information confrontation between NATO and Russia. Waves of disinformation campaigns have hit Moldova since the beginning of the war because of the geographical tensions and many believe Moldova is the next hotspot for Russian interception of ideas, technology, and territorial challenges. Being one of the former Soviet satellite states, Moldova is heavily influenced by Russian malign influence and economic coercion. The lack of energy independence, the existence of Transnistria, and continuing disinformation campaigns are constant sources of instability. Therefore, Moldova must strengthen the stability of the nation by fostering economic independence and information resilience to counter Russia's hybrid warfare and the potential possibility of direct military threats.

Case Study

Romania and Bulgaria

Alijah Neal

Introduction

The invasion of Ukraine by Russia in February 2022 has posed threats to countries in the surrounding Black Sea region, including Romania and Bulgaria. These two NATO member countries have encountered hybrid threats of cyberattacks, disinformation operations, and malign influence and economic coercion that ripple from Russia's attacks on Ukraine. Sovereign powers Russia and China have become highly influential in Romania and Bulgaria and are the main performers of these hybrid threats. These sovereign powers aim to disrupt Romania's alignment with NATO and the West by threatening the online and physical spaces of Romania as well as culturally and economically influencing the country.

Bulgaria is another NATO member country of the Black Sea region that has encountered cyberattacks, disinformation operations, malign influence and economic coercion echoing Russia's attacks on Ukraine. Russia and China have been involved in Bulgarian energy, trade, and investment in infrastructure projects – even going as far as shutting off natural gas to Bulgaria for their support for Ukraine. As allies against Ukraine, Russia and China are also highly influential over news that reaches the Bulgarian public, with their pushing of pro-Russia and pro-China rhetoric and suppression of support for Ukraine. This chapter will outline the major threats both Romania and Bulgaria are experiencing and how the two countries are working to combat the challenges they are facing in the heat of intensified hybrid warfare tactic usage.

Hybrid Threat Landscape

Romania

Since the Russian invasion of Ukraine, Romania has faced cyberattacks primarily carried out by a Russian cybercrime group named 'Killnet'. On April 29th, 2022, Killnet carried out Distributed Denial of Service (DDoS) attacks against the websites of Romanian public bodies and private organizations under claims that Romania supported Ukraine in the military conflict with Russia. Killnet disrupted the services of a number of these Romanian websites by flooding them with internet traffic from multiple sources so that they would become unreachable (Colceriu, 2022). Killnet easily taking control over public bodies, political parties and private entities with no repercussions or improved cybersecurity measures on Romania's end exposes cyber security vulnerabilities and brings forward opportunities of higher threat and/or more frequently occurring cyberattacks against Romania.

Disinformation reaches vast audiences in Romania through mainstream television channels and social media, especially Facebook and TikTok. With many news outlets being funded by political parties, only 20 percent of Romanians report having high confidence in news outlets, making the trust in the press very weak and Romania very vulnerable to propaganda (Metamorphosis Foundation, 2023). Narratives created by Russia that have been pushed in Romanian media since the invasion of Ukraine include depicting Ukrainians as corrupt or greedy, even labeling Ukrainians as Nazis or Ukraine as an authoritarian state that discriminates against its Romanian minority (Metamorphosis Foundation, 2023). Disinformation does not only affect the citizens of the country it is spread in, but also Ukrainian refugees that may be residing there and how they are perceived. Promoting ideas such as

these are intended to lessen support towards Ukraine and instead shift alliances of NATO member states towards Russia.

China mainly holds economic influence in Romania through investing in infrastructure and energy projects, like interest in investment of the only two nuclear reactors operating in Cernavoda, Romania, along with high-speed railways or 5G technologies as part of China's Belt and Road Initiative (Zamfir & Tiut, 2022). China also has the ability to influence young Romanian people through its Confucius Institutes within four Romanian universities, funded by the Chinese Communist Party (Zamfir & Tuit, 2022). These Confucius Institutes are outlets of soft power with aims of establishing a "bilateral cultural relationship" between China and Romania and promote the teaching of Chinese language and culture to Romanian youth (The Confucius Institute, 2018). Confucius Institutes avoid discussing topics that are considered "sensitive" in China like the Tiananmen Square Massacre and the Cultural Revolution and avoid addressing human rights abuses or other controversial subjects that may portray China negatively (Edwards, 2021). Students are lured by Confucius Institutes as their expenses for classes are covered, they are provided scholarships, and are encouraged to study abroad in China (Edwards, 2021). By creating a group of elites that are educated in a biased Chinese curriculum funded by the CCP, students' knowledge of China's history is selective, their academic freedom is suppressed, and their political stances are influenced to be pro-People's Republic of China and against Western democracy. With recruitment for espionage occurring at Confucius Institute locations in the United States, there are raised concerns about Romanian Confucius Institutes as well. According to a report made by NPR, CIs in the US have been recruiting spies to access classified government and military secrets, high-tech companies and university research, as well as monitor Chinese students (Myre, 2019). China's softer

approach to economic investments in Romanian projects and students, as well as using Confucius Institutes as a propaganda tool allows China to have a presence and influence within Romania without taking direct action or exerting their power intensely as their ally Russia might.

Romania is in a vulnerable spot physically as the country is near Ukraine and their Exclusive Economic Zones (EEZ) border each other. On February 24th, 2022, at the start of the Russian invasion of Ukraine, Russia had military ships on the northern border of Romania's EEZ – Ukraine's Snake Island – and occupied its land from February with bombardment from Ukraine forces until Russia withdrew from the island in June of that same year. Ownership of this island has been passed between Russia, Romania, and Ukraine with it now being Romania's EEZ, though Ukraine has authority over it (Scutaru et al., 2022). Ukraine's EEZ is already under Russian control, but Russia has long-term plans of regaining control over Snake Island (ARX Mouldings, 2022). Russian ownership over Snake Island could threaten foreign trade and access of Ukrainian and Romanian ports to the Black Sea that this island provides and could put Romania's offshore energy infrastructure into Russia's control.

Bulgaria

Bulgaria has experienced its own DDoS attacks performed by Killnet in October of 2022. Killnet confirmed blocking ten government websites, including the president's, with the intent of shaming the Bulgarian government for its supposed betrayal of Russia (BBC, 2022). Being attacked by the same cybercrime group as its neighbor Romania, Killnet's easy blockage in the name of "hacktivism" reveals Bulgaria's cyber vulnerability and increases incentive of attacks to occur. In addition, Bulgaria has faced phishing operations with 80% of all reported online

incidents being phishing attacks involving fake emails, direct messages or websites that are disguised as real ones and can extract personal information and access to important accounts of the user by the click of a button (Radio Bulgaria, 2022).

Bulgaria has experienced several disinformation operations within the past year following the Russian invasion of Ukraine in February 2022. For one, the Kremlin (a term used to describe the Russian government) paid journalists, political analysts, and other influential citizens 2,000 Euros a month to post pro-Russian content online through propaganda pieces and articles and social media websites like Facebook (Sunday Star, 2022) (AEJ, 2023). A great deal of fake accounts, bots, and trolls were also used to spread disinformation and Russian propaganda in Bulgaria, especially since Bulgaria has appeared to side with Ukraine and open itself up to Westernization in Russia's eyes by joining both NATO and the EU (Sunday Star, 2022). Some of the pro-Russia propaganda that has been spread includes videos promoting migrating to Russia and listing the amenities of Russian culture as well as spreading messages that put down the Bulgarian regime, even going as far as calling Bulgaria, "the black hole of Europe and rags of European civilization," (Юркова, 2023). Additionally, Russia has used its embassy in the Bulgarian capital of Sofia to spread anti-Western conspiracy theories, such as the United States may be running secret biological warfare laboratories in Ukraine (Sunday Star, 2022).

China, one of Russia's top allies, has taken advantage of social media and Chinese online and print outlets that operate in the Bulgarian language as an effort to make Bulgaria pro-China. For example, the weekly newspaper China Today and the Bulgarian edition of Russia Today are published by the same team and Bulgarian newspapers and national television channels produce Chinese content (Dimitrova-Martinyuk, 2022). Spreading pro-Russia and pro-China propaganda as

well as pinning blame for the Ukrainian invasion on the West and any countries that may be Western aligned is not a hard task for allies Russia and China, as they have substantial media presences in Bulgaria. Disinformation from these two allies aims to turn Romania, Bulgaria, and other NATO members against Ukraine, the West, NATO, and themselves.

Malign influence and economic coercion have occurred in Bulgaria with both Russia and China as perpetrators. As part of Russia's, "gas blackmail of Europe," it was reported that on April 26th of 2022 Russia had suspended natural gas imports to Bulgaria (France 24, 2022). For gas imports to resume, Russia requested that "unfriendly countries" like Bulgaria make payments in Russian rubles (France 24, 2022). This was designed to make Bulgaria vulnerable, but Dundee Precious Metals Inc. reassures that only, "approximately five percent of Bulgaria's total energy supply is generated from natural gas," and that Bulgaria's power supply would not be severely affected by the cutoff of Russian natural gas (Dow Jones International News, 2022). Despite only five percent of Bulgaria's total energy supply being generated from natural gas, the cut off raised concerns about fuel prices and the economy. In addition, the gas blackmail being executed by Russia displays what leverage they may have over a country and how they could threaten one's energy security if they do not align with Russia or support its actions. With concerns over espionage, Bulgaria expelled seventy Russian diplomats in July of 2022, which resulted in the Russian government threatening to end diplomatic relations (Sunday Star, 2022). There is a clear pattern with Russia: if there is opposition to their actions, they will threaten to cut ties with those who oppose them and rely on them. As for economic coercion, Russia's embassy in Sofia, Bulgaria invited Bulgarian citizens to donate private funds to support the Russian army in invading Ukraine, an action that upset the Bulgarian government (Sunday Star, 2022).

In the years leading up to the invasion until now, China has managed to plant its feet in Bulgaria and work towards increasing pro-Beijing attitudes among its citizens. In 2018, China Development Bank provided $1.75 billion in loans to companies in Bulgaria as well as investments in infrastructure projects as part of the 16/17+1 economic initiative between China and Central and Eastern European Countries (C-CEEC). There are also plenty of partnerships between China and Bulgaria with the development of a Bulgarian-Chinese Innovation Center in Sofia, exchange visits of representatives between the two countries, associations like the Bulgarian-Chinese Business Development Association and a Bulgarian-Chinese Chamber of Commerce, and its own Confucius Institute in Sofia (Dimitrova-Martinyuk, 2022). China has invested in Bulgaria's agriculture and related industries, information technology, and real estate and has shown interest in energy and infrastructure projects, but China's most visible economic success has been through trade, considering that Bulgaria has a large trade deficit with China (Shopov, 2022). In addition to being involved in trade with Bulgaria, China has expressed interest in port and transportation infrastructure, especially investing in Bulgaria's Varna and Burgas ports, as well as the construction of bridges over the Danube River – all of which gives China a grasp on the movement of Bulgaria's food and goods and control over port access (Shopov, 2022). Malign influence and economic coercion in Bulgaria cause the country to be divided politically in Russia, China, Ukraine, or its own nation. As joint forces, Russia and China's desire to keep Bulgaria away from the West is mutually beneficial, but difficult for Bulgaria to tackle and defeat.

To repel these hybrid threats, it is important to analyze who is launching the attacks as well as who the targets are, what technology or policy is currently being used and what new technology or policy should be introduced, when they should

be implemented, where they are currently being used or where they should be used if they don't already exist, and why they should be used. Through this examination, it can become clear what needs to be implemented and who is going to oversee the implementation.

Response to Hybrid Threats

1. **Actors**

The cybercrime group 'Killnet' from Russia was the primary executor of DDoS cyberattacks made against Romania and Bulgaria. The websites of Romanian institutions such as the Government, the Ministry of Finance, the Ministry of Defense, the Ministry of Health, the Ministry of Internal Affairs were affected by Killnet DDoS attacks carried out on April 29th of 2022 (Chirileasa, 2022). There were further threats made by Killnet saying that newspapers, major public institutions, hotels, boarding houses, booking sites and political parties were next to be targeted (Chirileasa, 2022). A few of the targets of cyberattacks made against Bulgaria include Bulgarian government ministries' websites, the National Revenue Agency, telecommunications companies, airports, and banks (The Sofia Globe, 2022). What these targets have in common is that they are either related to their country's government or provide information and connections to the public. Russia and ally China have targeted the online and physical publics of these countries through social media propaganda spreading as well as occupying Romania's EEZ, teaching pro-People's Republic of China curriculum to Romania's youth, and shutting down Bulgaria's natural gas supply to lessen Western alignment within the Black Sea region.

2. **Policy Response**

To counteract cybercrime, the European Cybersecurity Competence Center (ECCC) planted its own headquarters in Bucharest, Romania in May of 2023. The ECCC has aims of improving cybersecurity and resilience against attacks in Europe by bringing together top-tier experts and resources from across the EU to develop innovative solutions to cyber threats (Dumitrescu, 2023). Romania and Bulgaria already have national Computer Emergency Response Teams in place (CERT-RO and CERT-BG) that identify and analyze cyberattacks and aids with preventing future attacks (Cert.Ro, n.d.) (Govcert.bg, n.d.). It could be helpful to receive funding from EU's Internal Security Fund towards these CERTs, as well as towards development of cyber early warning systems to improve detection and prevention of cyberattacks. Additional cybersecurity support can be provided through improved training of employees working at these CERTs or through conducting more frequent vulnerability assessments and implementing stronger firewalls and intrusion prevention systems (IPS) that increase preparation for cyber exploitation and intrusion.

Advanced training and investment in such cyberattack preventative measures are recommended to be implemented as soon as possible to prepare and prevent Black Sea region countries like Romania and Bulgaria from future cyberattacks. SANS institutes hold cybersecurity events all over the world, including Romania in September 2023, with a mission of delivering relevant cyber security knowledge and skills. SANS provides courses, training, and certifications in the latest cybersecurity education. This is advised for those who are currently in the cybersecurity field and actively working to protect their country from cyberattacks but could also be beneficial to citizens who want to take basic preventative measures themselves. Tighter connections with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) could also greatly improve cyber defense in

Romania and Bulgaria as it is a NATO-accredited cyber defense hub that focuses on research, training and exercises and has expertise in areas of technology, strategy, operations, and law (CCDCOE, n.d.)

Bulgaria has taken some initiative on limiting disinformation spreading across its media with the fact checking website Factcheck.bg. The Association of European Journalists-Bulgaria (AEJ) created this platform and a team of non-partisan professional journalists who verify what is fact versus what is disinformation within Bulgarian social media, traditional media, public statements by officials and other information sources (Factcheck, n.d.). BROD, the Bulgarian-Romanian Observatory of Digital Media, has recently created another fact checking site, Brodhub.eu, that filters through articles of Romania and Bulgaria specifically (Brod, n.d.). For Confucius Institutes that spread propaganda through curriculum at physical universities, having an academic administrator from the department the Confucius Institutes operates to oversee what is being taught or omitted may be one course of action to eliminate pro-China propaganda.

It is recommended that constant filtering and fact checking of disinformation in Romanian and Bulgarian media occurs, as one web post or article issuing false information can reach the mind of millions of people in seconds. Filtering and fact-checking are currently being taken care of by a couple of organizations, a prime example being the Bulgarian-Romanian Observatory of Digital Media, which have taken charge of combatting disinformation in both countries with Brodhub.eu. Physical monitoring of Confucius Institutes, though, may be harder to enact because it would have to occur over a prolonged period of time to really observe what takes place day to day. Monitoring and potential changes made to CI operations is advised to take place as soon as possible as they present themselves

as educators and are currently shaping the perspectives of China, biases, and political positions of the youth.

Lastly, it is necessary that Romania acquires increased security over their EEZ as they are in a precarious geological placement, with other Black Sea EEZs bordering and overlapping and port access may be restricted if Russia were to invade Ukraine again or take control of Romania's EEZ directly. This can be done by sending Romanian military personnel and necessary equipment to the EEZ to survey and protect the area from invasion and working with the Cyber Defense Command (CApC) for improved maritime security.

3. **Benefits and Obstacles**

Encouraging cybersecurity literacy in Romania and Bulgaria as well as heightening security around Romania's EEZ are ways of preparing these countries for addressing potential future hybrid threats intelligently and rapidly. Providing support and funding towards Computer Emergency Response Teams as well as developing Cyber Early Warning Systems could also greatly prepare Romania and Bulgaria for cyberattack prevention. Eliminating disinformation and propaganda in the media and in physical teachings will decrease alignment towards Russia and China. Increased protection over Black Sea ports and EEZs (specifically Romania's) should be achieved in case of another invasion that may take EEZs out of their possession and decrease access to ports or halt the transport of goods.

Conclusion

In summary, Romania faces challenges extinguishing Russian and Chinese influence that flows throughout the country. Eliminating their presence in media,

decreasing economic investment in projects, and monitoring cultural exchange and espionage within institutions may be beneficial steps in ridding Romania of Russian and Chinese influence. Additionally, improving maritime security with increased military defense could keep their ports and offshore energy protected and decrease the chance of potential invasion of their Exclusive Economic Zone.

In Bulgaria, Russia continues its malign influence after stopping natural gas exports, but Bulgaria continues using China's economic investment. The promotion of anti-Western beliefs and spreading of anti-Ukraine propaganda can be stopped with keeping Confucius Institutes accountable in addition to media filtering and fact checking. Bulgaria has shown defiance towards Russia by expelling their diplomats and supporting Ukraine, even when gas imports were at risk – meaning there is possibility for Bulgaria to cut ties in other areas where Sino-Russian influence is present and doing so could greatly liberate them, especially in combination with support from NATO.

Due to this, the following recommendations are encouraged to deter further hybrid warfare and secure the economies and sovereignty of Bulgaria and Romania from Russian and Chinese actors.

1. **Monitor** Confucius Institutes for propaganda and espionage recruitment.
2. **Strengthen** military defense within Romania's EEZ by collaborating with Cyber Defense Command (CApC) for improved maritime security.

In addition to media filtering and fact checking, employing an academic administrator from the university which is tied to the Confucius Institutes to oversee the material being taught. Lastly, strengthening military defense within

Romania's EEZ by collaborating with Cyber Defense Command (CApC) could improve maritime security and set an example for other Black Sea Region EEZ.

Case Study
Türkiye
Michika Fukumori

Introduction

Türkiye's geographical position is significant because it shares a maritime border with Ukraine and Russia. As a NATO ally, Türkiye has been supporting Ukraine by sending drones produced in Türkiye (CNBC, 2023). Although collaboration and support through NATO has been enacted, Türkiye continues to hold strong economic ties with Russia. Türkiye has faced a plethora of hybrid warfare tactics since the beginning of the Ukraine conflict.

Since the war began, cyberattacks on Türkiye have significantly increased. In terms of cyber threats, Türkiye has limited cyber law regulations and implementations of cyber standards across sectors are only in the nascent phases ((Balcıoğlu Selçuk Ardıyok Keki, 2022). Positively, Türkiye has an advanced level of artificial intelligence (AI) that could be used as part of Cyber Early Warning Systems to fight cyberattacks for Türkiye and the remainder of Europe. Additionally, through cooperation with NATO, Türkiye could share new information and capitalize on joint cybersecurity training.

This section will highlight the main hybrid threats being used against Türkiye and discuss how the nation has responded to such threats. With increased collaboration with NATO on cyber defense, Türkiye will be able to defend their sovereignty from the threats facing the Turkish society.

Hybrid Threat Landscape

Cyberattacks

In February 2023, a 7.8 magnitude earthquake hit Syria and Türkiye, killing over 50,000. NATO sent its strategic airlift capabilities to Türkiye as part of the

broader aid effort; however, the airlift was targeted by the Russian hacking group, Killnet. They launched a distributed denial of service (DDoS) attack on NATO which disrupted communications with an aircraft carrying aid to Türkiye (Plummer, 2023). The Killnet group's objective is to attack the websites and assets of countries supporting Ukraine (HC3, 2023).

According to WatchGuard, all-source cyberattacks against Türkiye are increasing. The number of malware attacks against Türkiye increased by 61% in 2022, prompting experts to call for advanced measures to protect networks and data (RaillyNews, 2023).

Malign Influence and Economic Coercion

Türkiye has gained benefits from close economic relations with Russia while other NATO countries have tried to stop economic cooperation with Russia. As the chapter of Türkiye in *What Ukraine Taught NATO about Hybrid Threat* mentioned, the Akkuyu Nuclear Power Plant in Türkiye which is constructed, owned, and operated by a Russian state-owned nuclear energy monopoly Rosatom is a remarkable example of a close economic tie between Russia and Türkiye (Lohmann, 2022). Rosatom will contribute to supporting Türkiye to secure necessary human resources for the Akkuyu Nuclear Power Plant by inviting Türkish students to get trained in Russia (Glinsk, 2023). Since this nuclear power plant's location is important to Russia to keep up the logistical needs of Russian naval ships on the Mediterranean, they are more likely to get Türkiye's approval for the construction of commercial ports and terminals. There would be a possibility that Russia would install a military defense system there (Glinsk, 2023). In short, because of the Russian cooperation for the Akkuyu Nuclear Power Plant, Türkiye needs to keep Russian influence inside of their country to maintain infrastructure.

In addition, the presidential election in Türkiye is critical for its relations with Russia. The topic of the election that will have an impact on transatlantic relations includes Türkiye's standpoint as a NATO ally, and its relationship with Russia and the U.S. If Erdoğan would lose the election, Russia might be unable to have the same economic influence on Türkiye as it has now. However, since the election will happen in an unstable situation where Türkiye is still recovering from the earthquake, Erdoğan will emphasize that amid the turmoil, Türkiye has benefited from economic and technological assistance from Russia (Stamouli, 2023).

Response to Hybrid Threats

Cyberattacks

1. **Actors**

The close Putin and Erdoğan relationship has not prevented cyberattacks against Türkiye from Russian hackers, specifically the Killnet group. In addition, NATO's increased vigilance toward Russia and previous disputes between Russia and Türkiye over Syria, Libya, and Nagorno-Karabakh keep Türkiye on insecure footing with Russia (Glinski, 2023). Türkiye, therefore, continues to act as an intermediary between Western countries and Russia to protect Türkiye's interests (Glinski, 2023). The airlift incident shows how Türkiye has been caught in the cross hairs of the conflict even as it tries to maintain strong relations with Russia.

Since many NATO member countries share cyber threats, the Computer Emergency Response Team of Türkiye (TR-CERT) could use The NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), and NATO CMX crisis management exercise to share information and get trained to prevent further cyberattacks.

2. **Policy Response**

Currently, Türkiye does not have a law that requires cybersecurity s for all sectors (Balcıoğlu Selçuk Ardıyok Keki, 2022). However, the National Cybersecurity Strategy and Action Plan (2020-2023) includes the importance of creating a regulation on cybersecurity. It should be implemented by the end of 2023, or Türkiye would announce how and when the legislation will be in place (One Trust DataGuidance 2021). The regulation on cybersecurity determines the basic framework for how to protect their network and data for both the public and private sectors.

In terms of technology, Türkiye is focusing on the development of AI technology. According to Türkiye's first strategic artificial intelligence (Al) plan, it states that by 2025, the AI industry will account for 5 percent of the country's GDP, and it will employ 50,000 people. Both the National Cybersecurity Strategy and Action Plan (2020-2023) and the National Artificial Intelligence Strategy (2021-2025) call for AI technology to be used in the cybersecurity field. For example, it states that advanced AI skills should be used to train people who are in the cybersecurity field (NAIS, 2021).

3. Benefits and Obstacles

Creating a cybersecurity law would benefit small and medium size companies that do not have the resources to protect their network. One of the vulnerabilities is that cyberattacks are constantly changing using the latest technology, and even if a law is created, that law may not keep up with the evolution of cyberattacks.

If Türkiye could use AI for cybersecurity, it can effectively enhance cybersecurity. AI can analyze trends in threats based on extensive data from past cyberattacks. Then, AI will use that data to find the most effective ways to prevent cyberattacks and provide early warning of unknown types of cyberattacks (Cyber

Talk.org, 2023). According to the NEC, AI reduces the time needed to find the cause of cyberattacks from several days per case by human hands to an average of 1.5 hours and reduces the number of cyberattack false positives from several dozen per terminal to an average of 0.27 per terminal per day (NEC, 2017). If Türkiye could utilize AI well, it could thus strengthen its cybersecurity and Cyber Early Warning Systems.

However, one of the vulnerabilities can be that it is impossible to leave the task completely to AI alone, and it is difficult for small and medium-sized companies to secure the human resources that can utilize AI, which is constantly evolving (NEC, 2017).

Economic Coercion

1. **Actors**

Economic coercion in Türkiye is also being exerted by Russia. For example, a Russian state-owned company operates the Akkuyu Nuclear Power Plant. The area around the plant is geographically attractive to Russia, which is seeking to build a port for commercial use. If the plan takes effect, Russia may use the port for military purposes (Glinsk 2023).

2. **Policy Response**

Türkiye has no policy to deal with economic coercion from Russia because it seeks to maintain economic cooperation with Russia. However, Türkiye could get rid of Russian influence on the Akkuyu Nuclear Power Plant, if Türkiye cooperates with NATO to seek technical assistance and human resource development instead of letting Russia train Turkish students (Glinsk 2023).

3. **Benefits and Obstacles**

Türkiye could utilize NATO's Partnership Training and Education Centres, and the Energy Security Strategic Awareness course at the NATO School to receive joint

training (NATO,2022) (NSO, 2023). This gives Türkiye some support from NATO allies. On the other hand, it would be difficult to convince Russia to withdraw from operating the nuclear power plant.

Conclusion

Although Türkiye supports Ukraine as a NATO ally, Türkiye is attempting to maintain a close relationship with Russia to protect national interests. Türkiye is openly against the Russian sanctions and has made that clear in recent media and news.

Currently Türkiye does not have cross-sector regulations on cybersecurity, and Russian economic influence remains strong. To protect Türkiye from the Russian threat and fulfill its role as a NATO ally, it is necessary for Türkiye to increase its engagement with NATO and close the gap where Russia still possesses influence. Türkiye could achieve this by introducing new cybersecurity laws, furthering cybersecurity system development, and securing the necessary human resources to comply with those regulations. By creating a common regulation on cybersecurity, small and medium sized private companies exempted from Türkiye's Computer Emergency Response Team of Turkey (TR-CERT) are also protected. Incorporating their evolving AI technology into Cyber Early Warning Systems is essential to fight cyber threats which are continually evolving. The Computer Emergency Response Team of Türkiye (TR-CERT) could collaborate with the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), and NATO CMX Crisis Management Exercise for joint training and sharing information. To mitigate Russian economic influence, Türkiye could enable engineer-specific training using NATO courses such as the Energy Security Strategic Awareness Course.

To encourage Türkiye to become more engaged as a NATO ally, NATO needs to work in partnership with Türkiye to propose effective measures that will allow

the country to not work against its national interests and deter further Russian aggression.

Southeastern Europe Conclusion and Policy Recommendations

The Southeastern countries of Moldova, Romania, Bulgaria, and Türkiye have all been challenged with an increased presence of hybrid warfare since the Russian invasion of Ukraine. Specifically, they have experienced high levels of cyberattacks relating to the economic prosperity, social unity, and further development of these lesser-developed European nations. Critical infrastructure has been impacted and the repercussions of the damage are too crucial to ignore. Additionally, disinformation campaigns have hit heavily populated media outlets, with Russian influence attempting to change narratives surrounding the Russian invasion and the involvement of these countries in response to it. With such an extensive list of hybrid warfare threats to the region, specific regional recommendations have been created to help mitigate future risk for Moldova, Romania, Bulgaria, and Türkiye.

1. **Receive** funding from EU's Internal Security Fund towards Romania and Bulgaria's Computer Emergency Response Teams, as well as towards development of cyber early warning systems in these countries to rapidly detect and prevent cyberattacks.
2. **Establish** tighter connections with NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) to improve cyber defense in Romania and Bulgaria.
3. **Encourage** acquisition in the latest cybersecurity education, training, and certification.
4. **Strengthen** nations' information resilience by implementing nation-wide counter-disinformation education programs under MD-CERT supervision. These will help the public to raise awareness of disinformation, and invest in independent, reliable, and high-quality media that can provide an alternative to misleading or biased information sources.

These recommendations will advance the Southeastern European countries' cybersecurity capacities and enable a more secure and trusted society in relation to the ongoing hybrid warfare threats.

Southeastern Europe Citations

2022 Million Cyber Attacks Happened in Turkey in 1. (2023, January 10). RaillyNews. Retrieved April 17, 2023, from https://raillynews.com/2023/01/turkiyede-2022de-1-milyon-siber-saldiri-gerceklesti/

202301301200_KillNet Analyst Note_TLPCLEAR. (2023, January 28). HHS.gov. Retrieved May 4, 2023, from https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf

About brod—Brod. (n.d.). Retrieved May 10, 2023, from https://brodhub.eu/en/about/#HWhatisBROD

AEJ. (2023, February 8). АЕЖ-България. https://aej-bulgaria.org/en/russian-propaganda-in-bulgaria/

Al Jazeera. (2022, December 17). *Moldova suspends six TV channels over Russia-ukraine war coverage*. Russia-Ukraine war News | Al Jazeera. Retrieved April 19, 2023, from https://www.aljazeera.com/news/2022/12/17/manipulate-public-opinion-moldova-suspends-six-tv-channels

As Turkey imposes a harsh "disinformation" law, critics fear the worst. (2022, February 23). The Economist. Retrieved May 5, 2023, from https://www.economist.com/europe/2022/11/03/as-turkey-imposes-a-harsh-disinformation-law-critics-fear-the-worst?utmmedium=cpc.adword.pd&utm_source=google&ppccampaignID=17210591673&ppcadID=&utmcampaign=a.22brand_pmax&utm_content=conversion.direct-response

Baggiani, G. (2021, July 1). *The new NATO Cyber Incident Response Center in Moldova*. NATO Defense College Foundation. https://www.natofoundation.org/balkans-black-sea/the-new-nato-cyber-incident-response-center-in-moldova/

Balcıoğlu Selçuk Ardıyok Keki. (2022, September 05). Turkey DATA PROTECTION & CYBER SECURITY LAW. *The Legal 500 Country Comparative Guides*, (2022 Legalease Ltd).

Bir |, B. (2023, March 29). Russia 'increasingly' trying to destabilize Moldova: EU leader. *Anadolu Agency (Turkey)*. Available from NewsBank: Access World News – Historical and Current: https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&docref=news/19093A6BCFC59518

Bond, S. (2023, March 9). *From TV to telegram to Tiktok, Moldova is being flooded with Russian propaganda*. NPR. Retrieved April 19, 2023, from https://www.npr.org/2023/03/09/1162045645/from-tv-to-telegram-to-tiktok-moldova-is-being-flooded-with-russian-propaganda

Bonnet, M. (2023, March 29). From Ukraine to the Whole of Europe: Cyber Conflict Reaches a Turning Point. *Business Wire*. Available from NewsBank: Access World News – Historical and Current: https://infoweb-newsbank-om.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&docref=news/1908FA448B9BD8F8.

Boulègue, M., Lutsevych, O., & Marin, A. (2018, November). Civil Society under Russia's threat: Building resilience in Ukraine, Belarus and Moldova. European Sources Online. https://www.europeansources.info/record/civil-society-under-russias-threat-building-resilience-in-ukraine-belarus-and-moldova/

Bulgarian computer security incidents response team about us. (n.d.). Retrieved May 11, 2023, from https://www.govcert.bg/EN/Pages/AboutUs.aspx

CCDCOE. (n.d.). CCDCOE. Retrieved May 5, 2023, from https://ccdcoe.org/organisations/nato/

CCDCOE. *National Cybersecurity Organisation: ROMANIA.* (2022) https://ccdcoe.org/uploads/2020/11/NCS_organisation_ROM-2020_FINAL.pdf

Cert. Ro. (n.d.). Retrieved May 10, 2023, from https://www.cybersecurityintelligence.com/certro-2731.html

Chirileasa, A. (2022, May 2). *Romania under cyberattack coming from Russia's Killnet.* Romania Insider. https://www.romania-insider.com/romania-cyberattack-russia-killnet-2022

Corneliu-Aurelian Colceriu. (2022, May 02). List of IP addresses used for cyber-attacks amid Ukraine war grows exponentially - experts. *TCA Regional News* https://www.proquest.com/wire-feeds/list-ip-addresses-used-cyber-attacks-amid-ukraine/docview/2658316816/se-2

CSOMETER. (2022, June 7). Moldova adopts new anti-disinformation law. CSOMETER. https://csometer.info/updates/moldova-adopts-new-anti-disinformation-law

Dimitrova-Martinyuk, S. (2022, September 6). Chinese influence in bulgaria. StopFake. https://www.stopfake.org/en/chinese-influence-in-bulgaria/

DOS. (2023, March 23). Joint statement on the u.s.-moldova strategic dialogue - united states department of state. U.S. Department of State. https://www.state.gov/joint-statement-on-the-u-s-moldova-strategic-dialogue/

Dumitrescu, R. *The European cybersecurity competence center opens in Bucharest.* (2023, May 9). Romania Insider. https://www.romaniainsider.com/european-cybersecurity-competence-cent er-opens-bucharest-2023

Digital Transformation Office of the Presidency of Turkey - National Artificial Intelligence Strategy 2021-2025. Retrieved May 4, 2023, from https://cbddo.gov.tr/en/nais

Edwards, L. (n.d.). *Confucius institutes: China's trojan horse. The Heritage Foundation.* Retrieved May 6, 2023, from https://www.heritage.org/homeland-security/commentary/confucius-institutes-chin as-trojan-horse

Euronews. (2023, March 15). Moldova defence minister says country threatened by Russian propaganda. euronews. https://www.euronews.com/2023/03/15/moldova-threatened-by-hybrid-warfare-generated-by-russia-to-destabilise-government

Euronews. (2022, December 19). Six TV channels suspended amid "misinformation" allegations. euronews. https://www.euronews.com/2022/12/19/six-tv-channels-suspended-in-moldova-amid-misinformation-allegations

European Commission. (2022, May 2). *New support to the Republic of Moldova on cyber-security, addressing disinformation and social cohesion*. Service for Foreign Policy Instruments. (2022, May 2). Retrieved April 19, 2023, from https://fpi.ec.europa.eu/news-1/new-support-republic-moldova-cyber-security-addressing-disinformation-and-social-cohesion-2022-05-02_en

EUvsDisinfo. (2021, December 21). Disinformation & Elections in Moldova. EUvsDisinfo. https://euvsdisinfo.eu/disinformation-elections-in-moldova/

EU says 'era of Russian fossil fuels in Europe is coming to an end.' (2022, April 27). France 24. https://www.france24.com/en/europe/20220427-live-ukraine-says-russia-beginning-gas-blackmail-of-europe-as-poland-bulgaria-cut-off

Gaber, Y., Lewis, D., & Herd, G. P. (2023, March 7). *Ukraine and Emerging Trends in Russian and Turkish Foreign Policy*. George C. Marshall European Center For Security Studies. Retrieved April 18, 2023, from https://www.marshallcenter.org/en/publications/clock-tower-security-series/strategic-competition-seminar-series-fy23/ukraine-and-emerging-trends-russian-and-turkish-foreign-policy

Glinski, S. (2023, March 6). *Turkey Strengthens Ties With Russia, NATO Ahead of Elections*. Foreign Policy. Retrieved April 12, 2023, from https://foreignpolicy.com/2023/03/06/turkey-elections-russia-erdogan-putin-nato/

Gosselin, E., & Wendel, S. (2022, November 22). *Turkey's Russian-built nuclear plant could amplify Moscow's regional influence*. Al-Monitor. Retrieved May 4, 2023, from https://www.al-monitor.com/originals/2022/11/turkeys-russian-built-nuclear-plant-could-amplify-moscows-regional-influence

Halisdemir, E. (2021). *Turkey: Cybersecurity | Insights*. (n.d.). DataGuidance. Retrieved May 5, 2023, from https://www.dataguidance.com/opinion/turkey-cybersecurity

Highlights: Russia Chelyabinsk Media 17-23 Oct 22. (2022, Nov 03). *BBC Monitoring Former Soviet Union* https://www.proquest.com/wire-feeds/highlights-russia-chelyabinsk-media-1 7-23-oct-22/docview/2731304080/se-2

How artificial intelligence is revolutionizing cyber security. (2023, March 27). CyberTalk.org. Retrieved May 17, 2023, from https://www.cybertalk.org/2023/03/27/how-artificial-intelligence-is-revolutionizing-cyber-security/

ITU. (2022, December). Assessment report of Moldova National Computer Incident Response Team (CIRT-MD) in Moldova. United Nations. https://moldova.un.org/en/216556-assessment-report-moldova-national-computer-incident-response-team-cirt-md

Юркова, О. (2023, January 14). 330 shades of Russian disinformation: Exploring the media landscape of eastern europe. *StopFake.* https://www.stopfake.org/en/330-shades-of-russian-disinformation-exploring-the-media-landscape-of-eastern-europe/

Lohmann, S. J. (2022). *What Ukraine Taught NATO about Hybrid Warfare*. United States Army War College Press, Strategic Studies Institute.

Meaker, M. (2022, April 8). *An "explosion" of Anti-Ukraine Disinformation is hitting Moldova*. Wired. https://www.wired.com/story/moldova-disinformation-war-ukraine/

Metamorphosis Foundation. (2023). Interview with Romanian anti-disinformation activist reveals disinformation campaigns often target refugees from Ukraine. (2023, February 21). *Global Voices.* https://globalvoices.org/2023/02/21/interview-with-romanian-anti-disinformation-activist-reveals-disinformation-campaigns-often-target-refugees-from-ukraine/

Myre, G. (2019, July 17). As scrutiny of China grows, some U.S. Schools drop a language program. *NPR*. https://www.npr.org/2019/07/17/741239298/as-scrutiny-of-china-grows-some-u-s-s chools-drop-a-language-program

National Artificial Intelligence Strategy (NAIS) 2021-2025. Retrieved May 4, 2023, from https://cbddo.gov.tr/SharedFolderServer/Genel/File/TRNationalAI Strategy2021-2025.pdf

National Cybersecurity Organisation: TURKEY. CCDCOE. Retrieved May 4, 2023, from https://ccdcoe.org/uploads/2021/08/TUR_country_report_final_clean_ver_2408 pdf

NATO. (2021, January 21). *Cyber incident response capability established in the Republic of Moldova with NATO support*. Service for Foreign Policy Instruments. Retrieved April 19, 2023, from https://www.nato.int/cps/en/natohq/news_180758.htm

NATO. (2021, January 21). *NATO assists Moldova in improving its cyber security capabilities*. eforum.ncia.nato.int. https://www.ncia.nato.int/about-us/newsroom/nato-assists-moldova-in-improving-its-cyber-security-capabilities.html

NATO's response to Russia's invasion of Ukraine. (2023, April 4). NATO. Retrieved May 4, 2023, from https://www.nato.int/cps/en/natohq/topics_192648.html

NCSI (2023). *Moldova's National Cyber Security Index.* Retrieved April 19, 2023, from https://ncsi.ega.ee/country/md/

Necsutu, M. (2022, June 20). Moldova bans Russian media to counter propaganda over Ukraine. Balkan Insight. https://balkaninsight.com/2022/06/20/moldova-bans-russian-media-to-counter-propaganda-over-ukraine/

Plummer, K. (2023, February 13). *Russian hackers 'disrupt Turkey-Syria earthquake aid' in cyber attack on Nato*. The Independent. Retrieved April 13, 2023, from https://www.independent.co.uk/news/world/europe/turkey-syria-earthquake-russian-hackers-b2281278.html

Press Release: Dundee Precious Metals' Bulgarian Operations Unaffected by Reduced Natural Gas Supply to Bulgaria. (2022, Apr 27). *Dow Jones Institutional News* https://www.proquest.com/wire-feeds/press-release-dundee-precious-metal s-bulgarian/docview/2655997961/se-2

Radio Bulgaria. *Over a quarter of Internet traffic in Bulgaria is malicious: Ministry of E-Government.* (2022, September 27). News. ttps://bnr.bg/en/post/101711160/over-a-quarter-of-internet-traffic-in-bulgaria-is-malicious-ministry-of-e-government

Reuters. (2022, December 17). Russia denounces Moldova's ban of TV channels as "political censorship." Reuters. https://www.reuters.com/world/europe/russia-denounces-moldovas-ban-tv-channels-political-censorship-2022-12-17/

Scutaru, A. C., Alexander Crowther, Joel Hickman, George. (2022, September 27). *The strategic importance of snake island.* CEPA. https://cepa.org/comprehensive-reports/the-strategic-importance-of-snake-island/

Shopov, V. (2022, March 22). *Let a thousand contacts bloom: How China competes for influence in Bulgaria.* ECFR. https://ecfr.eu/publication/let-a-thousand-contacts-bloom-how-china-competes-for-influence-in-bulgaria/

Stamouli, N. (2023, April 17). *2023's most important election: Turkey – POLITICO*. POLITICO. Retrieved April 18, 2023, from https://www.politico.eu/article/turkey-2023-election-erdogan-kilicdaroglu/

The Confucius Institute. (2018, December 3). *UniBuc - Universitatea Din București.* https://unibuc.ro/despre-ub/resurse-educationale/institute/institutul-confucius/?lang=en

The Potential of AI to Propose Security Countermeasures : NEC Technical Journal | NEC. (n.d.). NEC Corporation. Retrieved May 6, 2023, from https://www.nec.com/en/global/techrep/journal/g17/n02/170216.html

The Sofia Globe. (2022, October 16). *Official: Cyber attack on Bulgarian government websites traced to Russia.* The Sofia Globe. https://sofiaglobe.com/2022/10/16/official-cyber-attack-on-bulgarian-government-websites-traced-to-russia/

The war on misinformation. (2022, Jul 17). *Sunday Star - Times* https://www.proquest.com/newspapers/waronmisinformation/docview/2690261057/se-2

Tiut, R. Z., Andrei. (2022, August 17). *Chinese influence in Romania*. CEPA. https://cepa.org/comprehensive-reports/chinese-influence-in-romania/

Topic: Education and training. (2022, June 2). NATO. Retrieved May 6, 2023, from https://www.nato.int/cps/en/natohq/topics_49206.htm

Who we are | Factcheck.bg. (n.d.). Factcheck.Bg – Проверка На Факти. Retrieved May 10, 2023, from https://factcheck.bg/en/who-we-are/

Why snake island has become the maritime security hotspot. (2022, August 2). *ARX Mouldings.* https://arxmouldings.com/why-snake-island-has-become-the-maritime-security-hotspot/

Zarandah, M. (2023, March 28). *Killer drones: Turkey's growing defense industry is boosting its global clout*. CNBC. Retrieved May 3, 2023, from https://www.cnbc.com/2023/03/28/killer-drones-turkeys-growing-defense-industry-is-boosting-its-global-clout.html


Luxembourg
Germany
France
Hungary
CENTRAL AND
WESTERN EUROPE

Case Studies

Western and Central Europe:

Luxembourg, Hungary, Germany, and France

In an ever-evolving global security landscape, traditional warfare tactics have been challenged by the emergence of hybrid warfare. Cyberattacks, disinformation campaigns, and malign influence all pose unique challenges to nations worldwide. This case study focuses on the potential hybrid warfare threats faced by Luxembourg, Hungary, Germany, and France, shedding light on the complexities these countries encounter in safeguarding their national security.

Luxembourg's status as a financial hub makes it vulnerable to cyberattacks and economic disruption. Additionally, disinformation campaigns targeting the country's multicultural society can undermine social cohesion and weaken public trust. Hungary's geographical position between the crossroads of Eastern and Western Europe poses great danger to the threat of hybrid warfare. Threats such as cyber espionage and government-backed disinformation campaigns have exploited societal divisions and created political polarization. Hungary's close ties with Russia also raises concerns about potential interference in its internal affairs.

With Germany having Europe's largest economy and being a key political player, they serve as a prime target for hybrid warfare. Cyberattacks on critical infrastructure such as energy and transportation systems pose a significant threat to their national security. Moreover, disinformation campaigns run by pro-Russian groups have eroded societal trust. Germany's pivotal role in both the EU and NATO further amplifies the need for proactive measures to counter hybrid warfare threats. France is overwhelmed with hybrid warfare threats as well, including cyberattacks to key sectors including defense, finance, and telecommunications. As the leader in cybersecurity across Europe, France is held responsible for creating

and enacting new policies to maintain a strong defense posture, foster international cooperation, and invest in new technology to effectively protect both themselves and the rest of Europe. With a comprehensive understanding of these threats, Western and Central European countries will be able to protect their national security, democratic institutions, and cohesion of society in a time when countries are struggling to defend themselves.

Case Study
Luxembourg
Shern Sze Lim

Introduction

Luxembourg has the highest per capita gross domestic product (GDP) in the world (IMF, 2022). This economic strength is dependent on its banking sector, where its financial system is the third most competitive in Europe after London and Zurich (The Global Financial Index, 2017). However, Luxembourg faces increased economic malign influence from China's growing internalization of state-owned banks across the EU. This has propagated into Belt and Road Initiatives (BRI) projects within Luxembourg and beyond. Specifically, China's investment in the EU's critical infrastructure has prompted national security concerns from the acquisition of the Luxembourg energy sector to strategic ports across the EU. This paper begins by examining the disproportionate influence of Chinese banks in Luxembourg by studying its unique dual-banking structure. The paper then analyzes the interplay between China's banking presence and the geopolitical-driven development of BRI projects. Finally, policy analysis and recommendations are provided to ensure Luxembourg's economic autonomy and national security.

Hybrid Threats Landscape

Malign Influence

The rise of China and its accession to WTO has propelled China's state-driven investment strategy in Luxembourg. More than 40% of Chinese investment in Europe is made via Luxembourg and six out of the seven largest Chinese banks are stationed in Luxembourg (Balmas and Dorry, 2022)**.** Against this backdrop, Chinese banks' comparative banking structure advantage threatens Luxembourg's

economic autonomy through the acquisition of EU banks and the Belt and Road Initiative (BRI) in the EU.

Luxembourg's economic threat stems from China's dual branch-subsidiary structure in Luxembourg. The dual banking structure not only helps Chinese corporations overcome China's restriction on capital outflows, but it also allows Chinese banks to circumvent EU's risk management rules (Balmas and Dorry, 2022). This comparative advantage allows the highest efficiency in the flow of Chinese FDI and acquisitions. This is evident in the Chinese's acquisition of 3 European banks: Banque Internationale à Luxembourg by Legend Holdings in 2017; the German bank Hauck and Aufhäuser by Fosun Group in 2015; and the Danish Saxo Bank by Geely in 2017 (Balmas and Dorry, 2022). In 2022, Luxembourg also granted Chinese financial services EU equivalence status (Shillito, 2022). Both signify China's ambition to raise its economic foothold over the EU economic powerhouse.

Chinese acquisition of EU banks has important political, economic, and security implications on Luxembourg's economic autonomy. Chinese banks' alignment with state interests is defined by the 'window guidance' (Dikao and Volz, 2021). A 'window guidance' refers to "a policy instrument to effectively direct and control the growth of lending by commercial banks" (Dikao and Volz, 2021). This framework is important because China's internalization of banks means that capital is flowing towards politically driven development projects as opposed to purely profit manner (Balmas and Dorry, 2022). This can inflate asset prices and distort market allocation. Epstein (2017) also highlights that the increase of banks' foreign ownership correlates with the weakening relationship between the host state (Luxembourg) and its banking sector. In this case, acquisition of EU banks implies a higher degree of Chinese state penetration over Luxembourg's banking management, key decision-making, and sensitive information. For instance, China's

economic influence could indirectly strengthen lobbying power that serves the Chinese state's interests over the EU banking sector and the European Bank Authority (Balmas and Dorry, 2022).

Both the weakening ties of state-banks and the 'window guidance' have facilitated China's Belt and Road Initiative (BRI) across Europe. BRI represents China's geostrategic ambitions to expand global influence through a multitude of investments to enhance trade and digital networks (ECA, 2020). Though BRI promotes growth and global trade, China's high concentration of investments in strategic sectors such as freight, ports, and energy facilitated by Luxembourg's banking sector threatens NATO security (Hanemann and Huotari, 2018). For instance, in 2018, the state-owned China Southern Power Grid also bought over 25.48% of Encevo Group, one of Luxembourg's key energy players (Reuters, 2018). Moreover, Luxembourg's friendly economic conditions for Chinese liquidity have also manifested in the Chinese takeover of key European ports such as Valencia, Rotterdam, Antwerp, and Piraeus. Most recently, COSCO Shipping Corporation Ltd (COSTCO), a Chinese SOE, has even received Berlin's support for plans to purchase 24.99% stakes of a Hamburg terminal (Politico, 2023).

Chinese BRI's penetration into EU critical sectors through Luxembourg's financial center heightens NATO's insecurity. In the case of ports acquisition, a German official on the acquisition of Hamburg terminal highlighted that "the investment disproportionately expands China's strategic influence on German and European transport infrastructure as well as Germany's dependence on China" (Brookings, 2023). This reveals an existential risk as China gains influence over EU maritime infrastructure and access to dual-use port facilities that could disrupt NATO maritime operations. Moreover, China's access to critical sectors may facilitate technology transfer from the EU to Chinese entities. This is evident when

the European Chamber of Commerce in China reported that 20% of EU members have been compelled to transfer technology for market access in China (Reuters, 2019). This threatens NATO security as China gains more information about NATO operations and sensitive technology. Furthermore, past BRI projects have allured concerns over economic sustainability and transparency operations that jeopardize the states and NATO's economic autonomy. A telling example is the BRI-built highway in Montenegro that raised its nation's debt from 63% of GDP in 2012 to almost 80% in 2019. If Montenegro were to default, this gives China the right to access Montenegrin land as collateral (Valerie and James, 2019). This challenge resulted from the 17+1 framework that allows China to engage directly with Central and East European states without the mediation of the EU (Brattberg, 2018). This compromises the EU's degree of operational transparency and unity when dealing with foreign loans. For instance, EU unity was compromised as China was able to influence Greece to help prevent the EU from issuing a unified statement against Chinese aggression in the South China Sea (Horowitz and Alderman, 2017). This reveals how Chinese economic influence feeds into its political prowess over the EU community.

Cyber Threats

Luxembourg's critical infrastructure has been a victim of cyberattacks. Glover (2022) revealed that Encevo Group, an energy conglomerate based in Luxembourg dealt with cyberattacks by a Russian ransomware gang called Blackcat. Though energy supplies have not been affected, core digital services were disrupted for 12 days after the attack. Beyond critical infrastructure, hackers are targeting Luxembourg's banking sector. According to Luxembourg for Finance (2022), the number of corporate cyberattacks increased by 50% between 2020 and 2021, with phishing attacks increasing by 600%. This resulted from the rise of corporate hybrid

working policies that increased hackers' access to sensitive company information and software. This tarnished the banking industry's reputation and undermined trust with customers.

Hybrid Threat Response

1. Actors

China's disproportionate economic influence and presence over Luxembourg's banking sector is clear. In 2020, China ranked 3rd with the greatest number of banks in Luxembourg, just behind France and Germany (Statista, 2023). This resulted from the internationalization of Chinese SOEs across Luxembourg that propagated into acquisitions of local banks and investments in strategically critical infrastructure. To counter this, Annemie Turtelboom, member of the European Court of Editors (ECA) highlighted that "an effective response to the geopolitical shift would require the EU to step up its strategy on China, and Member States to act together with the EU institutions as a Union" (ECA, 2022). Thus, a unified action from Luxembourg's Ministry of Finance (MoF) and the European Central Bank (ECB) is paramount. This helps to prevent EU market distortion and an unequal investment playing field from foreign actors (ECA, 2022).

2. Policy Response

China's economic expansion stems from Luxembourg's approval of China's dual branch-subsidiary banking structure. This resulted in 40% of Chinese FDI being through Luxembourg and has increased Chinese FDI across Europe's critical infrastructure. In response, the ECB and MoF should review and update the screening mechanism of its Foreign Direct Investment (FDIs) to protect Luxembourg's national security. Actions are underway. On September 15, 2021,

Luxembourg Parliament introduced a bill to establish a FDI screening mechanism on 'critical' sectors that may adversely affect Luxembourg's national security (Nicolau and Poinsignon, 2023). The bill identified dual use goods, energy, transport, water, telecommunications, healthcare, data storage, aeronautic defense, finance, and media as 'critical' sectors. This bill only applies to FDIs in Luxembourg firms and infrastructure projects (Nicolau and Poinsignon, 2023). Accordingly, the bill requires foreign investors with more than 10% stake in Luxembourg firms to notify the Luxembourg Ministry of Finance. The bill proposes 5 key frameworks to guide FDI approval:

1. Integrity, security, and continuity of supply of critical infrastructure.
2. Sustainability of activities related to critical technologies and dual-use goods.
3. Supply of essential inputs including raw materials and food safety.
4. Access to sensitive information, including personal data, or the ability to control such information.
5. Media freedom and pluralism

3. Benefits and Obstacles

This FDI screening mechanism is advantageous as clear FDI regulations help to prevent the cascading effects of Chinese FDIs and influence. It serves as an "ex ante control" before the approval of an investment and avoids the high transaction costs of unwinding deeply entrenched investors in Luxembourg (Grunwald, 2022). China's acquisition of the port in Piraeus, Greece is a case in point. According to Brookings (2022), China's economic influence began with its initial goal of collaborating with the EU Trans-European Transport Network Initiative. It then propagated to Chinese investment in EU multimodal transportation projects across Northern and Southern Europe. In 2008, then President Hu Jintao launched a $5.5

billion landmark agreement for Chinese shipping group COSCO to run two of Piraeus' container terminals (Piers 2 and 3) for a period of 35 years. Eight years later, Chinese SOE' COSCO acquired 67% in Pier 1 of Piraeus Port Authority (Gresh, 2022). This example illustrates that if Luxembourg is not cautious with its FDI screening mechanism, China could not only take over its banking industry but also sensitive critical infrastructure as well.

However, the FDI screening mechanism's exhaustive regulations may threaten Luxembourg's competition on the global stage. Leon Gloden, a specialist in EU competition law emphasized, "on the one hand, as a small country, we need foreign investment…but on the other hand, we also must protect our infrastructure" (Grunwald, 2023). With new regulations in place, Luxembourg may lose out on lucrative investment and acquisition opportunities that had once built its banking empire. Thus, revealing the delicate balance between economic prosperity and national security.

Furthermore, Germany's continued approval of China's COSCO acquisition of 24.99% of Hamburg terminal questions the efficacy of Germany's own FDI mechanism. This is alarming considering the mechanism's new infrastructure law that considers ports as "critical infrastructure" (Politico, 2023). Its approval in May 2023 is no coincidence. Specifically, the German and Chinese officials plan to meet in a summit on June 20 in Berlin (Politico, 2023). Without a rigid accountability mechanism, this reveals that a FDI mechanism may not be sufficient to prevent China from controlling Europe's critical infrastructure.

With competing views, Luxembourg's FDI mechanism implementation has been sluggish. To prevent further Chinese influence, ECB and MoF should create stringent deadlines to speed up the process. Additionally, an accountability

mechanism must be placed to abide by what constitutes “critical infrastructure”. Luxembourg’s FDI mechanism can then serve as a model for other allied countries facing increased foreign FDIs in critical sectors. Thus, improving the overall national security of the EU.

Conclusion

As Luxembourg’s financial industry serves as the EU’s gateway to global FDI, strong regulations to counter disproportionate foreign economic influence are critical. This requires a pragmatic approach to the long-term sustainability of FDI from China. As proposed, such an approach could come through expediting an FDI screening mechanism with a rigid accountability mechanism on what constitutes ‘critical infrastructure’. This will help prevent China’s growing acquisition of critical infrastructure that impedes NATO’s ports and railroad operations. Furthermore, this regulation allows Luxembourg to reassess its FDI regulations and serves as a model for EU-wide FDI regulations.

Case Study
Hungary
Michika Fukumori

Introduction

Hungary is one of the few European Union member states that maintains close relations with Russia. Prime Minister Orbán has visited Moscow and avoided personal criticism of President Vladimir Putin. While other European countries have seen their supply of Russian oil and gas reduced or cut altogether, Hungary signed a contract in 2021 that guarantees it 4.5 billion cubic meters (bcm) of Russian gas per year through 2036 (Than and Gyori, 2023). On the other hand, while accepting refugees from Ukraine, relations between Ukraine and Hungary have deteriorated dramatically in recent years due to Ukraine's attempts to counter Russian influence over ethnic minorities, including those from the Transcarpathian region of Ukraine, which Hungary ceded after World War I (Nattrass, 2022 & ÖZKAN, 2023). As a result, Hungary is not in favor of the support sought by Ukraine.

Under the Russian-leaning Orbán administration, the media has proven to be heavily biased and has permitted Russia access to sensitive national and NATO information, showing a lack of awareness of its defense as a NATO ally. This section first examines the Russian-leaning Orbán administration as the source of the hybrid threats in Hungary, looks at the case study of Hungary's cybersecurity and disinformation, and finally, provides policy recommendations to ensure Hungary's role as a NATO ally.

Hybrid Threat Landscape

Cyberattacks

In March of 2023, the investigative journalism website Direkt36 reported that the Hungarian Ministry of Foreign Affairs' communication channels had been

hacked by Russian intelligence since 2013. This allowed Russia to have direct access to staff mailings and other information, such as sensitive data sent from Hungary's embassy. They mentioned that the Russian Federal Security Service and the Military Intelligence Service had been involved in these attacks. They used spear phishing to gain access to IT systems through e-mails claiming to be from official NATO events. The actions the government should take in the event of a cyberattack are to investigate the cause and stop further damage, warn allies, inform the public, etc., but the Orbán government did not take the necessary preventative steps and hid these events from the public. Opposition parties accused Prime Minister Orbán of being complicit in giving Russia access to the information (Szabolcs, 2022).

In addition, Hungary's financial institutions and telecommunications infrastructure were targeted by a powerful cyberattack from computer servers located in Russia, China, and Vietnam in September 2020. The hackers used a distributed denial of service (DDoS) attack, attempting to overwhelm networks with “unusually high volumes of data.” Magyar Telecom, one of the primary targets of the attack, said that the volume of data was 10 times that of a normal DDoS attack. The attack interrupted some services before ultimately being repelled by the company, underscoring the importance of having dedicated incident response teams to respond to cyber threats (Komuves, 2022).

Disinformation

Since 2018, the government has integrated 476 media outlets under the Central European Press and Media Foundation (KESMA), which is controlled by a former Fidesz leader. The Fidesz party is known to be pro-Russian, and because of this integration, 79% of the media outlets voiced the views of the Russian-leaning Fidesz party in 2019 (ShePersisted, 2023). This consolidation has made it difficult for

media outlets to operate, as the government only distributes public funds to media outlets under the consolidation (ShePersisted, 2023).

One example of disinformation carried out by the Orbán administration was a report in 2019 that accused the European Commission of supporting illegal immigration. However, the European Commission announced it was disinformation (BBC, 2019). The ongoing attempts by the Hungarian government to redefine the wants and needs of European homogeny shows a greater purpose to misinform their citizens. Concurrently, in October 2022, Hungary's streets, Facebook, and news media were filled with propaganda. Posters with pictures of bombs saying "sanctions", along with the phrase "Brussels' sanctions will ruin us!", appeared in public. This was an attempt by Prime Minister Orbán, who opposes the current EU political and economic sanctions against Russia, to create a false impression among the public that the sanctions against Russia are harming them (Heil, 2023).

Response to Hybrid Threats

Cyberattacks

1. **Actors**

Cyberattacks against Hungary are from Russian hacking groups under the Russian Federal Security Service and the Military Intelligence Service. Their objective is to access data inside the NATO network (Szabolc, 2022). Thus, the NATO Cybersecurity Centre, the NATO Cooperative Cyber Defense Centre of Excellence, and the National Cybersecurity Center should work closely together to prevent the issue from happening further.

2. **Policy Response**

Since the publication of the National Cybersecurity Strategy in 2013, Hungary has established The National Cybersecurity Center (NCSC) to provide a secure

network to both the Hungarian government and local authorities, as well as to raise public awareness of cybersecurity (Cyberwiser, 2013).

The National Cybersecurity Strategy emphasizes the importance of international cooperation in cybersecurity (Cyberwise, 2013). As an example of this, Hungary is working with NATO countries to improve their cybersecurity systems. The Foreign Commercial Service of the U.S. Embassy in Budapest held a workshop called Strengthening Cybersecurity Capabilities in Hungary to discuss trends in cybercrime. The workshop shared information on cybercrime trends and what Hungary needs to improve (U.S. Embassy, 2022).

However, according to Government Decision No. 1139/2013 (21 March) on the National Cybersecurity Strategy of Hungary, the National Cybersecurity Strategy clearly states that the strategy is initiated by the Prime Minister's Office. Its responsibility is to take the necessary actions to operationalize the National Cybersecurity Strategy, such as creating a National Cybersecurity Center (Cyberwise, 2013). Considering the accusations of Orbán's government allowing Russia to have access to their information, the new policy which makes the National Cybersecurity Center independent from the Prime Minister's Office should be implemented. The National Cybersecurity Center could be set under the responsibility of the parliament, and it would be important to establish a system that allows opposition parties to monitor progress which could eliminate Orbán's government from having sole control over the National Cybersecurity Center.

3. Benefits and Obstacles

This policy benefits NATO in that it can contribute toward the network being secured without intervention from Russian influence. One vulnerability is that the National Cybersecurity Strategy does not provide a secure network for the private

sector (National Cybersecurity Strategy, n.d). A private company needs to attain proper knowledge and recognize the vulnerabilities in its network on its own.

Disinformation

1. **Actors**

Hungary's disinformation is conducted by Orbán's government which is pro-Russia. The targets are the Hungarian public, and they are controlling media to spread pro-Russian narratives. The EU created The Digital Services Act (DSA), which aims to combat disinformation and will be enforced in 2024. This is said to have a favorable effect on limiting Orbán's government from spreading disinformation freely (Matirosyan, 2023).

2. **Policy Response**

In 2020, Orbán's Fidesz party passed a new law that gave the government the power to govern media indefinitely without the parliament's advice with a two-thirds majority of votes in favor. The law criminalized journalists who spread news criticizing the government's fight against the COVID-19 virus. However, the International Peace Institute pointed out that this law is not only about COVID-19. The institute claims that Orbán's intention is to censor journalists who are critical of the government and not a part of the media consolidation (IPI, 2020). Hungary needs new policies to detach press control from the ruling government to ensure freedom of press and so that the executive is unable to spread disinformation.

3. **Benefits and Obstacles**

This policy can remove government influence from the Hungarian media, allowing them to report news freely. However, the difficulty is that given the new law was passed by parliament with a two-thirds majority, it is unlikely that a law restricting government influence in the media will be passed in the near future. To do so, Hungarian people need to be educated on media literacy and be made

aware of what the government is doing in reaction to poor media literacy rates. Proper education surrounding social media and the sorting and recognition of information people receive online is the first step to a more aware public. Introducing classes on basic information in media at the primary level helps build the foundation of defense for the public, as they are the most vulnerable and the first target of disinformation.

The next stage of the policy will be for middle and high school programs. Once they possess the basic knowledge of disinformation, they need to start thinking critically about the information they receive on social media. They should then possess the skill sets to filter the misleading information they might find on social media and utilize technology to build a wall for themselves from disinformation. This policy would benefit Hungarian people to have the ability to judge information before trusting material being shown to them through mainstream media.

Since the government has been known to conduct disinformation, it could be difficult to implement an educational system on media literacy led by Orbán and his constituents. However, NATO and the Center for Media Literacy provide webinars for media literacy, and these webinars could be administered through the Hungarian education system with little intervention from the Orbán government (CML, n.d).

Conclusion

Hungary has proven to have close relations and a large Russian influence on society in recent years. The Orbán administration continues to collaborate and conduct disinformation campaigns against economic sanctions being placed on Russia by the EU and NATO. Hungary's historical tensions with Ukraine persist. The National Cyber Security Center led by the pro-Russian Orbán administration has

provided great access to many pro-Russian narratives. Hungary needs to separate the national cybersecurity center from the cabinet office of the prime minister to combat cyber threats from Russia. The National Cyber Security Center could be under parliament so that the minority and ruling party monitor each other.

Cooperation between NATO and the Hungarian parliament is essential to monitor the progression of cybersecurity measures. To fight disinformation, disassembling media integration is essential to avoid government control. Also, introducing a new education system on the threats of disinformation and how to detect it could be a vital step in the fight against pro-Russian propaganda in Hungary. This could be done by cooperating with NATO and the Center for Media Literacy education programs. If Hungary would be able to improve their freedom of speech and secure cyber networks without government interference, Hungary could mitigate Russian influence, and be able to engage in international cooperation to maintain regional security.

Case Study
Germany
Taylor Bell

Introduction

Since the onset of the Russian invasion of Ukraine, the Russian government and state-backed actors have escalated their long standing cyber, disinformation, and influence campaigns, seeking to cause harm, spread confusion, and enfeeble and divide target states in the region (Tisdall, 2022). The main target of cyberattacks has been on European critical infrastructure. By exploiting vulnerabilities in critical infrastructure, Russia has created fear and uncertainty within the EU and NATO. However, this fear and uncertainty has also provided the impetus for the development of more robust security strategies to defend against Russian hybrid warfare tactics. This section analyzes the cyber and disinformation campaigns directed at Germany, charts their responses to an increasingly hostile threat environment, and discusses the benefits and obstacles Germany still faces regarding hybrid warfare.

Hybrid Threat Landscape

Cyberattacks

As Europe's largest economy and a major supporter of Ukraine, Germany has long been targeted by cyberattacks and coordinated disinformation campaigns emanating from Russia. In June 2021, cyberattacks targeting political candidates and voters, successfully accessed, and extracted sensitive data that allowed Russia to tailor and customize a subsequent disinformation campaign. (Eddy, 2021). Russian state media used this information to promote its favored narrative across media channels (Germany Notes Increase in cyberattacks by Russian Actors, 2021). Russia has also sought to disrupt Germany's critical infrastructure. In the third

quarter of 2022 alone, German airports, public administration bodies, and financial sector organizations, were targeted by 52 distributed denial-of-service (DDoS) attacks (Thales, 2023). These attacks were designed to overwhelm the target systems and prevent the system from functioning normally with proper internet traffic (AFP, 2023). Killnet, a Russian-backed hacking group, took credit for the attacks.

Disinformation

Russia also wants to control the narrative surrounding its invasion and has targeted Germany with disinformation and propaganda spread by "Russian government-controlled media and pro-Russia websites, as well as by official diplomatic and pro-Kremlin Twitter accounts" (*Disinformation Related to the Russian War of Aggression against Ukraine*, n.d.). A major German news outlet, *Der Spiegel,* was affected by fake accounts which posted seemingly genuine remarks on the commentary page. These accounts posted inaccurate or misleading information and doctored videos promoting pro-Russian narratives about its reasons for invading Ukraine (Germany Concerned over Fake Sites with Pro-Russian Disinformation, 2022). This example outlines the ease and simplicity of Russian disinformation and its immersion into German society. The fake accounts caused no serious harm to individuals or organizations but demonstrated the purpose of pro-Russian groups wanting to influence European citizens in unhealthy ways.

Economic Coercion

Aside from the disinformation affecting Germany, the increased levels of cyberattacks on essential energy sources, like critical gas pipelines and offshore wind farms, and other critical infrastructure in the country has caused turmoil and unrest for Germany and the rest of Europe, too, as it has been a sign that Putin and

the Russian government have effectively weaponized energy (Kochis, 2022). The first major attack on European energy sources stemmed from the shutdown of natural gas resources by Russian governments that Germany and other European countries relied on prior to the invasion. The lack of access to natural gas and oil from Russia has pushed Germany to rush new green energy initiatives ahead of schedule to lower its dependency. Before the war, 55% of Germany's oil imports came from Russia. Those numbers fell to 20% at the start of 2023, with imports plummeting further due to an EU ban on Russian seaborne oil products that occurred in February of 2023 (*World Economic Forum*, 2023).

The decline in dependence has not solved the issue of dwindling energy sources and because of this, levels of CO2 are increasing due to the new reliance on coal power as the country waits for the green energy technology to be developed and installed. In addition to the energy crisis, Germany has also fallen victim to cases of economic coercion given that the German economy is the epicenter of the European economy. Thus, economic measures like sanctions put on natural gas and other major products important to the critical infrastructure of Europe, have detrimentally affected the power and legitimacy that the German economy had before the war. Prices are rising and the supply chain demands are causing larger issues in businesses and corporations all around Germany (Schmelzer, 2023). With the continued difficulty of economic coercion, Germany has had to adapt and look to neighbors of the EU to support and aid in the rebuilding of the economy and the citizen's confidence in the economy.

The most recent collaboration between Germany and another country in the European Union has been Belgium. Following the first annual Belgian-German Energy Summit in February 2023, the two countries have agreed to link hydrogen networks, doubling the gas flow into Germany. This has the possibility of adding an

additional high-voltage electricity interconnector for better cross-border flow (Kyllmann, 2023). The increased levels of liquified natural gas (LNG) that Germany will have access to could deflate rising prices and start to stabilize the economy.

Response to Hybrid Threats

1. Actors

In response to the hybrid warfare threats occurring in Germany, the main culprits of cyberattacks and disinformation campaigns have been tied to Pro-Russian individuals and groups. Russian groups have been called 'hacktivist' groups, working closely to target opponents of the Russian invasion of Ukraine (Kass, 2023). Killnet, along with an ally group named XakNet, are defined as groups who are more focused on the protection of social and political causes rather than financial gain. Russia is utilizing disinformation and propaganda to justify its military invasion and cement its narrative of the "anti-Russian West" ideals. Organizations and groups like the German Defense Ministry and NATO Cybersecurity initiatives are working together to create new policies and safeguard the vulnerabilities that still exist in relation to critical infrastructure and Russian-forward disinformation (Serrano and DisinfoLab, 2023).

2. Policy Response

As for the combat of cyberattacks and disinformation in Germany, initiatives have been built to create more secure information-sharing and overall cybersecurity. Additionally, Germany continues to rely on enforcement laws such as the Network Enforcement Law that was enacted in 2017, which aims to fight hate crime and omit criminally punishable fake news from social media within Germany (der Justiz, 2017). As for cybersecurity, Germany has been involved in new initiatives brought forth by the European Union, with the Network and Information Security

(NIS) Directive being one of the main policy changes since the onset of the invasion. The NIS was an EU-wide legislation designed to achieve a high common level of cybersecurity across the Member states by strengthening security requirements, addressing the security of supply chains, and streamlining reporting obligations (Niethammer, Rieks, Saerbeck, Norbu, 2022). Although the NIS Directive was a start to improving cybersecurity policies in Europe, the EU legislation decided that a second, more updated version of NIS needed to be enforced. The second version would put more emphasis on stricter supervisory measures and harmonized sanctions across the EU and would be the responsibility of the Committee of Industry, Research and Energy (ITRE) (Negreiro, 2023). The urgency of passing cybersecurity policies heightened with the start of the Russian invasion and has since then begun to appear on all levels of governing, but specifically in higher level organizations like the European Union and NATO.

Cybersecurity and disinformation are not newly discovered methods of hybrid warfare. However, as technology has advanced and the methods of attaining success in both sectors has simplified, countries like Germany have had to act fast in reforming previous policies and initiatives to better match the threats that are present today. One way in which Germany has attempted to uncover and fight disinformation and 'fake news' is through organizations with initiatives to end disinformation. CORRECTIV, an organization working towards combining hoax debunking and investigative journalism, and DPA-FACTCHECKING, the disinformation police of Germany's leading news agency, Deutsche Presse Agentur, utilize special teams and advanced screening technologies to filter information being released to the public (Serrano and DisinfoLab, 2023). At Deutsche Presse Agentur, the process of a fact check starts with a claim by some nationally recognized news or information, an evaluation of such information using the

International Fact Checking Network (IFCN) principles, and ultimately the facts which prove a claim to be true or not true (*Fact Checking at Dpa*, n.d.). This ensures that the public opinion is shielded from the attempts by pro-Russian news outlets to share false information or skewed opinions on topics relating to Russian involvement and the Ukrainian response (Serrano and DisinfoLab, 2023).

The previously discussed NIS Directive, which was originally passed by the EU Parliament in 2016 to introduce policies and recommendations surrounding cybersecurity, has been recently renovated and updated. In December 2022, the European Union proposed the NIS-2 Directive and by January 16, 2023, the policy was enacted. The new directive highlights stricter legal measures to boost the overall level of cybersecurity in the EU. One specific addition to the directive mitigates the issue of Member States' lack of preparedness from the last NIS directive by requiring them to be appropriately equipped with systems that protect cybersecurity such as Computer Security Incident Response Teams (CSIRT) and national Network and Information Systems authority. Furthermore, a cooperation group has been set up to support and facilitate strategic cooperation and the exchange of information among Member States (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) | Shaping Europe's Digital Future*, 2023). Countries now have until October 2024 to enact the directive into national law by national legislators (Dolle, 2023). The quick timeline of the updated directive provides evidence of the urgency EU members are seeing in relation to cybersecurity and the effects that attacks are having on economies and civilians. In Germany, the new directive affects significantly more companies, and the framework has created more fines that hold companies accountable for the choices being implemented to fight against cybersecurity issues (Dolle, 2023). With Germany being the hub for European economic growth, directives like NIS-2 are

crucial to the continuation of growth rather than the fatal future of Russian influence and continued cybersecurity vulnerability.

3. Benefits and Obstacles

New legislation and policies are being implemented in both the security and media sectors of Germany, including governmental offices, private sector businesses, and public news outlets. With the creation of the 2021 Cybersecurity Strategy for Germany, the Federal Minister of the Interior and Community became responsible for the maintenance and trajectory of cybersecurity regulations in Germany, with different stakeholders being involved in the execution of the new policies (“Cybersecurity Strategy for Germany 2021,” 2021). Civil society stakeholders active in cybersecurity tend to be associations and foundations built to compile political analyses and propose recommendations for cyber risks. This is encouraging more awareness of cybersecurity risks among the general population. In the private sector, companies are working alongside research firms to develop innovative technical solutions, contributing to the development of standards and norms, and enforcing networking and skills development (“Cybersecurity Strategy for Germany 2021,” 2021).

Governmentally, the responsibility of German cybersecurity has been broken into two levels: strategic and operational. Domestically, the Federal Ministry of the Interior, Building and Community is responsible for coordinating issues within Germany while the Federal Foreign Office is responsible for coordinating international cybersecurity policy. Cyber defense is run and maintained by the Federal Ministry of Defense (“Cybersecurity Strategy for Germany 2021,” 2021). The German government has a group called the Military Counterintelligence Service (MAD) that protects the Bundeswehr from espionage attacks and sabotage from

extremism in cyberspace (“Cybersecurity Strategy for Germany 2021,” 2021). These departments have been highlighted and continually used into 2023 with the invasion of Ukraine. Their goals are to establish cybersecurity as a joint task between the stakeholders discussed, reinforcing digital sovereignty between the government, private industry, and research firms, and setting measurable, transparent objectives in relation to the surveillance of cybersecurity within Germany. The division of labor and responsibilities amongst these government departments are providing more control and surveillance of German cyber risks which has given the private sector players a larger role in the public-private collaboration of research and development for cybersecurity. Although promising, further implementations of stricter policies surrounding the security measures required to be included in communication systems and other information systems is crucial to add another vital layer of protection to German companies and the government.

By utilizing and updating policies related to cybersecurity, Germany and the rest of the European Union can combat the vulnerabilities that are being found in critical infrastructure and other sectors of German society. Having certain departments and ministries assigned to specific branches of cybersecurity is a compact method to reinforce the importance of increased security measures, especially in times of heightened attacks both through cyber and in terms of disinformation. Using policymaking in the fight against hybrid warfare creates opportunities for the public to be aware of the decisions being made surrounding hybrid warfare. It also creates accountability for the public and private entities to which the new policies apply. Although the policies and disinformation-seeking organizations are working towards a better, more secured country, Germany also needs to work alongside stronger technology-driven systems to counteract the

hacking groups' actions. With the advanced technology being introduced into the hybrid warfare realm, cybersecurity has become the forefront for many countries' defense ministries and Germany is no different.

Conclusion

Germany has been affected by extensive disinformation campaigns, detrimental cyberattacks, and serious economic coercion in response to the start of the Russian invasion of Ukraine. Because of the sheer size and impact that the German economy has on the rest of Europe, pro-Russian groups have increased activity within German borders. The fight against Russian energy sources has been extremely difficult for Germany and has forced new collaborations with neighbor countries to limit their dependence on Russian imports. With such a high level of vulnerabilities, German cybersecurity strategies have been revamped to protect against the modern hybrid warfare and deter major attacks from shutting down crucial centers like airports and hospitals. Despite considerable efforts to eliminate hybrid warfare threats from German society, vulnerabilities still exist, and further implementation of advanced cybersecurity systems are needed to fully rid Germany of the present risks.

Case Study
France
Taylor Bell

Introduction

France has been the leader in all things cybersecurity; from enacting new policies long before the Ukraine war began, to revising and updating current guidelines to better fit the vulnerabilities being faced. With the extended threats such as cyberattacks, disinformation, and malign influence, the French government has had to rely on new initiatives and more offensive capabilities to deter from further attacks. Cyberattacks have negatively affected government websites, and disinformation campaigns have effectively altered the opinions of the French people regarding the participation of Russia in the invasion. Along with the introduction of advanced technology making it more difficult for countries to defend themselves from hybrid warfare threats, collaboration amongst public and private stakeholders is crucial to learn and adapt more quickly. The initiation of NATO member state-run strategies has also enabled more secure critical infrastructure in France and beyond.

Hybrid Threat Landscape

Cyberattacks

France has been increasingly targeted by cyber and disinformation campaigns since Russia's invasion of Ukraine. Prior to the invasion, reports uncovered a three-year long cyberattack that was conducted and credited to Russian hackers tied to the Russian military intelligence branch. This attack intruded into the networks of French company Centreon which provides monitoring software to clients such as the French Ministry of Justice and the oil and gas giant, Total (Cerulus, 2021). Although this attack was not related to Ukraine

relations, the professionalism shown by Russian hackers warned France of their cybersecurity vulnerabilities and expedited the introduction of new cybersecurity measures which are now being utilized. France has since focused heavily on ensuring cyber resilience and the capacity to defend and act in hybrid fields. Since the onset of the invasion, France's President Emmanuel Macron has revised and recreated the French security strategy by utilizing and aligning France's goals with the newly updated NATO strategic concept to combat hybrid threats, which was published in early 2023. Among some of Macron's changes, "asserting influence will rank as a new strategic function in the defense policy of France against the backdrop of disinformation campaigns and foreign interference" (Süß, 2022). The updated French policy also emphasizes the 'secure' pillar of the four pillars – act, secure, invest, and partner – outlined in the Strategic Compass of the EU, a common EU document built for the prevention of threat perception (Süß, 2022).

With the agile and forward actions of Macron and the French government in relation to protecting themselves from increased hybrid threats, other countries within NATO and the EU have relied on the skills and attributes France possesses to model their own policies and security regimens. For example, German defense minister, Christine Lambrecht, stated in a speech back in September 2022 that the new German strategy would closely mirror that of France to adopt policies that will lessen the economic, political, and social impacts of hybrid threats by hostile competitors (Süß, 2022). Although France has been a leading power in cybersecurity and defense against disinformation attempts and malign influence, the strong pull to create "European autonomy" has caused criticism from fellow NATO members with commentary stating that France is attempting to appear closer to Russian officials than other NATO members are comfortable with. This is happening in a time when France's military defense and cybersecurity awareness

could play a significant role in the trajectory of the Ukraine-Russian war. The war has created a divide in European nations, with the Eastern countries being filled with “rejuvenated mistrust and suspicion towards Russia” while Western European countries are being roped into the anti-Russia mindset by supplying military relief and economic aids in relation to the United States’ involvement in the invasion (Dwivedi, 2023).

France’s ability to ward off cyberattacks and shut down disinformation campaigns early on has positively affected their security and defense from major Russian attacks since the Ukraine invasion, but it does not denote that France is completely safe from attacks. In the ESET World Conference held in June 2022, the threat and software vulnerability research firm outlined and discussed major cyberattacks that had occurred in France. There was a serious cyberattack tied to a North Korean regime hacking group named Lazarus. This attack was targeted at French aerospace and defense contractors by utilizing fake recruitment processes to gain valuable information from current and past employees (*ESET Research*, 2022). Although Russia has not been connected to the Lazarus attacks directly or indirectly, analyses have been done to link Lazarus with distributing cyberattacks using network accesses held by Russian-speaking cybercriminals (Sheridan, 2020).

Disinformation

Most recently, in March 2023, the French National Assembly website was successfully attacked by a Russian hacking group who goes by ‘NoName’. The hackers used a distributed denial-of-service (DDoS) system to temporarily take away functionality to all users, posted Pro-Kremlin comments about Macron’s continuation to “serve Ukrainian neo-Nazis” and coined the purpose of the attack to the organization’s support of Ukraine (Kayali, 2023). Additionally, in April of 2023,

France accused Russia of disinformation and blackmailing about its role in Ukraine. The Russian Foreign Ministry spokeswoman claimed that France's president, Macron, "knows how much the alliance (NATO) did to destabilize the situation in Ukraine – If he knows all that, then it's just a substitution of concepts, hypocrisy, and the spread of untruth." This reiterates the narrative of Russia being the aggressor against Ukraine in the war and that Kyiv is having to defend "its sovereignty and its territorial integrity" (Donmez, 2023). Instances such as the breach of the French National Assembly and political blackmail highlight the extreme danger and unrest that hybrid warfare, including cyberattacks, disinformation, and malign influence, is having on the allies of Ukraine in a time of rapid technological advancements and unknown consequences to those advancements. The vulnerabilities that France has encountered in the past 12 months have disrupted the economy and lessened the confidence of civilians in the government's ability to deter future attacks from occurring.

Response to Hybrid Threats

1. Actors

Even with France's elevated presence in the cybersecurity space, as a country, they are still targeted with hybrid warfare attempts, specifically heightened with the Russian invasion of Ukraine. The main perpetrators of French-related attacks have stemmed from pro-Russian groups and hacking organizations involved with the Russian government. The motives behind these attacks follow the same narrative. Pro-Russian groups are wanting to punish countries showing support for Ukraine and responding to news of aid packages and weaponization assistance with hacking major government agencies and private companies. In France, the responsibility to protect their critical infrastructure and overall societal peace

should fall on the government to continue the process of enacting new policies and reforming existing ones to strengthen their knowledge in cybersecurity.

2. Policy Response

With the leading cybersecurity measures in Europe, France is held to a high standard when it comes to acting on renewing cyber policies and enacting innovative ideas and solutions to the ever-evolving world of advanced hybrid warfare with the engagement of technology. France has had a longer history than most other European countries in their response to hybrid warfare and cybersecurity more specifically. The onset of French cybersecurity was highlighted in the White Paper on Defense and National Security, approved by the President in 2008, and later led to the creation of the National Information Systems Security Agency (ANSSI) in July 2009 (*Assurer La Cybersécurité et Coordonner La Cyberdéfense*, 2022). ANSSI was built to ensure an area of awareness and prevention, intended to inform the various audiences of the cyberspace threats that existed along with an axis that is centered on the reaction to attacks and the return to normalcy for affected systems (*Assurer La Cybersécurité et Coordonner La Cyberdéfense*, 2022).

Since then, Emmanuel Macron has been active and assertive with changing the cybersecurity landscape for France, and ultimately the rest of Europe. In January 2019, long before the Russian invasion, France pivoted its military cyber strategy from a majority defensive approach to one that equalizes defensive and offensive approaches. The creation of The Cyber Committee (COMCYBER) in collaboration with the General Directorate of Armaments were given a doctrine to develop offensive computer warfare capabilities to be used with engagement of the armed forces (Faesen et al., n.d.). The offensive cybersecurity doctrine showed that France was not afraid of using cyber weapons and would use the publicity of this

announcement as a sign of cyber power (Faesen et al., n.d.). France has had confidence in an offensive hack-back approach since 2019 and the Russian invasion did not change that stance. In late 2022, Macron updated the French national security strategy to better reflect the vulnerabilities they were facing from the past draft which was enacted from 2017 to 2021 (Süß, 2022). The new security strategy focuses on ten main priorities with the top five being: 1. Robust and credible nuclear deterrence 2. A united and resilient France 3. Defense economy 4. Cyber resilience 5. Euro-Atlantic relationship (Süß, 2022).

An example of strong cooperation with outside stakeholders to exemplify the necessity of cybersecurity reform is shown in the recent collaboration led by Thales, a French-based multinational company who develops and manufactures electrical systems, to create a cyber threat intelligence platform (*Thales and 10 Partners Launch French Cyber Threat Intelligence Platform to Support Greater Autonomy and Resilience*, 2023). The platform is designed to provide cyber threat intelligence services to companies and government entities to support greater autonomy and resistance to vulnerabilities. With the French government's announcement of stronger cybersecurity support in both the 2030 investment plan and the national cyber strategy, Thales and its collaborating partners will have the freedom to explore opportunities to provide innovative technologies to ensure France's sovereignty and eventually the sovereignty of Europe, too, in the field of cybersecurity. The quick actions being taken by both public and private actors in the French battle against hybrid warfare has been an inspiring motivation for fellow NATO and EU members to mirror policy recommendations and security services to strengthen their own countries' exposure to the vulnerabilities found in the cyberworld.

3. Benefits and Obstacles

Although France has implemented policies to eliminate the threat of cybersecurity, the invasion of Ukraine expanded the target on their back. For that, the French government has had to act in response to Russian attacks and cyber threats to relevant and crucial critical infrastructure. Initiatives such as Macron's changes to the National Security Strategy were done at the end of 2022, with expedited implementation beginning at the onset of 2023 (Mackenzie and Ferran, 2022). It is important to note that France along with other NATO member states are aware of the ongoing and ever-changing cyber threat environment which is causing destruction and worsening confidence for countries around the world but are keenly aware that flexibility in plans and initiatives are key to making a better tomorrow (Mackenzie and Ferran, 2022). On a national level, France has also pivoted towards offering more assistance to local police and investigative authorities with access to information and identifying cyberattack perpetrators with new laws on the insurability processes. As of April 24, 2023, France's Orientation and Programming Law (LOPMI) now enforces a 72-hour period on all cyberattack insurance claims (Bigel and Akli, 2023). Prior to the amendment, French authorities were finding that claims would be filed far too late, and no accurate or useful information could be gathered from ongoing cyberattacks because of the time between when the incident occurred and when the investigation began (Apostle, Carr, Kawkabani, 2023). The dedication and fearless attitude towards change in the realm of cybersecurity has boosted France's ability to stabilize the economy in an unpredictable time with new changes to the political scene daily.

The initiatives discussed have been implemented and practiced within French government entities such as the creation of ANSSI. Along with the government-based policies, France has also coordinated with EU-based initiatives to fight disinformation like the European External Action Service's work with

EUvsDisinfo, a service meant to highlight and analyze reported disinformation campaigns that target EU members (EUvsDisinfo, 2020). France's involvement in organizations like these encourages greater surveillance of hybrid warfare and creates opportunities to learn about the vulnerabilities that still exist, leading to more advanced solutions. Although involvement in disinformation tracking has helped, the French public is still ingesting false information. The French government needs to create stronger defenses towards anti-French disinformation.

The most contemporary development in France's battle against cybersecurity is the addition of initiatives with the inclusion of private sector stakeholders. In the International Cybersecurity Forum (FIC) that took place on April 5-7, 2023, Thales announced a collaboration with 10 other industry players with approval from the French National Security Strategy to utilize the resources, research, and technology at their fingertips to help enable a safer France, encourage fewer opportunities for cyber-related security issues, and promote strategic autonomy in this field of cybersecurity (*SCRED, a Unique Collaborative Project for Cybersecurity*, 2023). The widespread access to both public and private outlets for cyber threat improvements has granted France a unique position in the world of cybersecurity. There is willingness to implement regional, national, and international solutions to slow the progression of cybersecurity threats in the future.

The implementations that France has enacted in response to the heightened cyber threats have had a significant impact on not only the French cybersecurity strategies but those of surrounding countries as well as NATO member states. The new policies have encouraged cooperation amongst other governments to collaborate in ways in which certain cyber threat measures have proven successful and how to combat vulnerabilities that still exist. Along with the benefits of collaboration, Macron has decided to take an offensive cybersecurity approach on

changing previous policies to maintain a contemporary stance on the rapidly advancing technology being used by adversaries. Opportunities to be leaders in cybersecurity quickly follow as countries find inspiration in the actions the French government is taking to defend their lands and the safety of their civilians. Although new policies have provided support and protection from cyber threats, the fear of advancing technology with artificial intelligence is creating wariness among the government and public. Countries like France are going to need to continue revising current security systems and policies to have control over the next generation of hybrid warfare.

Conclusion

The heightened awareness surrounding France's vulnerabilities to hybrid warfare and the overwhelming willingness to discuss and change policies to better the security of the country has given France a well-deserved leg up on the rest of Europe. Newly formed security strategies and collaborative campaigns against disinformation allow for greater autonomy within the country and have created a platform for others to mirror. Although vulnerabilities to critical infrastructure still exist in France, and the threats concerning disinformation and malign influence are still high, the measures created since the start of the Russian invasion in Ukraine have showed immense progress. France is not vulnerability-free, but with the steps being taken to mitigate large risks, the future is a lot brighter for the French people and the rest of Europe.

Western and Central Europe Conclusion and Recommendations

Many NATO member states have experienced vast destruction and vulnerabilities to critical infrastructure in their countries since the invasion of Ukraine. The Western and Central European countries of Luxembourg, Hungary, Germany, and France have all faced hybrid threats. Threats such as cyberattacks on energy sources like critical natural gas pipelines and offshore wind farms, disinformation campaigns coming from both pro-Russian groups, and at times, their own governments, and detrimental economic coercion to critical economy sectors. These discrepancies have hindered economies, with gas and oil prices rising and have created a weakening confidence in the ability to discourage cyber-related attacks. Due to the ongoing effects of hybrid warfare threats on these countries, recommendations have been created to strengthen the national security of these countries and attempt to mitigate the risks presented through hybrid warfare.

1. **Strengthen** the coordination of the newly formed NATO military Cyber Operations Centre (CYOC) which is meant to enable offensive and defensive capabilities in response to cyberattacks. Generating a baseline response will ensure that the ethical reasoning behind attacking the attacker or ignoring a threat is in line with the morals and standards that NATO countries agree to uphold. By promoting an offensive policy, NATO member states will have more control over cyber threats and broaden their levels of response.
2. **Implement** Cyber Early Warning Systems on both private and public sectors. When considering both states' long term cyber defense, states should collaborate with the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) to implement next generation CEWS with intelligence sharing

through joint cyber operations. NATO-wide cyber operations would facilitate an accountability mechanism to foster common knowledge in the latest risk analysis, best practices, and practical institutions to protect critical infrastructure.

3. **Evaluate** new critical infrastructure systems through the NATO Science and Technology Organization (STO) to ensure that new systems being introduced to NATO countries are free of vulnerabilities which could be attacked.

With the implementation of these recommendations, the trajectories of these countries' national security are heightened. The threats faced by Luxembourg, Hungary, Germany, and France represent a complex challenge to security, and they are not fully immune to multifaceted tactics used in hybrid warfare such as cyberattacks, disinformation, and economic coercion. But with the recognition of the interconnected nature of these threats and adoption of strategies that encompass intelligence sharing and international cooperation, these countries will be able to overcome the risks and secure the well-being of their citizens.

Western and Central Europe Citations

A PERFECT PROPAGANDA MACHINE. (n.d.). ShePersisted. Retrieved May 4, 2023, from https://she-Persisted.org/wpcontent/uploads/2023/ 03/ShePersisted_Hungary.pdf

A year of Russian hybrid warfare in Ukraine. (n.d.). https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/0 3/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

AFP. (2023, January 26). *Cyberattacks Target Websites of German Airports, Admin*. SecurityWeek. https://www.securityweek.com/cyberattacks-target-websites-of-german-airports-admin/

Alexander Niethammer, David Rieks, Stefan Saerbeck, Isabella Norbu. (2022, November 14). *International Comparative Legal Guides* (United Kingdom) [Text]. International Comparative Legal Guides International Business Reports; Global Legal Group. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany

Assurer la cybersécurité et coordonner la cyberdéfense. (2022, November 23). SGDSN. http://www.sgdsn.gouv.fr/nos-missions/proteger/assurer-la-cybersecurite-et-coordonner-la-cyberdefense

Asia Pacific - Chinese market. (n.d.). https://www.arendt.com/jcms/dev_10884/en/asia-pacific-chinese-market

Bayer, L. (2022, March 9). *Hungary has become the EU home of Kremlin talking points*. POLITICO. Retrieved April 10, 2023, from https://www.politico.eu/article/russia-war-narrative-hungary-disinformation/

Bigel, D. P.-L., & Akli, H. (2023, March 27). *France: Changes to insurability of cyber losses*. Lexology. https://www.lexology.com/library/detail.aspx?g=a57f6067-1204-484c-b41e-38c54684e0e3

Bonnie, G. (n.d.). *Zhengzhou and Luxembourg: An Improbable Partnership*. https://thediplomat.com/2018/08/zhengzhou-and-luxembourg-an-improbable-partnership/Balmas, P., & Dorry, D. (n.d.). *Chinese bank networks in Europe: FDI-oriented by legal and strategic design*. https://www.tandfonline.com/doi/full/10.1080/15387216.2023.2182805?src=

Brattberg, E., & Soula, E. (n.d.). *Is Europe Finally Pushing Back On Chinese Investments?* https://carnegieendowment.org/2018/09/14/is-europe-finally-pushing-back-on-chinese-investments-pub-77259

Cerulus, L. (2021, February 15). France identifies Russia-linked hackers in large cyberattack. *POLITICO*. https://www.politico.eu/article/france-cyber-agency-russia-attack-security-anssi/

Claudia, G. (n.d.). *Luxembourg energy provider Encevo Group battles ransomware attack by BlackCat*. https://techmonitor.ai/technology/cybersecurity/encevo-group-cyberattack-luxembourg-blackcat-ransomware

CYBERSECURITY: INCREASED VIGILANCE AT ALL LEVELS. (n.d.). https://www.luxembourgforfinance.com/portfolio/cybersecurity-increased-vigilance-at-all-levels

Cyber Security Strategy for Germany 2021. (2021). *Federal Ministry of the Interior, Building and Community*, 133. *China's investment strategy: the EU should step up its response, say Auditors*. (n.d.). https://www.eca.europa.eu/Lists/ECADocuments/INRW20_03/INRW_EU_response_to_China _EN.pdf

Data protection agency investigates gov't sending personal data of Hungarian citizens to Russia. (2017, April 17). 444. Retrieved May 17, 2023, from https://444.hu/2017/04/17/data-protection-agency-investigates-govt-sending-personal-data-of-hungarian-citizens-to-Russia

der Justiz, B. (2017). *Netzwerkdurchsetzungsgesetz*. Bundesministerium der Justiz. https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future. (2023, May 16). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Disinformation related to the Russian war of aggression against Ukraine. (n.d.). Federal Ministry of the Interior and Community. Retrieved May 4, 2023, from https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/disinformation-related-to-the-russian-war-of-aggression-against-ukraine.html;jsessionid=324D724263B1EAC177419F184DF4BD0F.2_cid364?nn=9386226

Dolle, M. F., Wilhelm. (2023, February 14). *Cyber security in the EU: NIS-2 directive raises security level - KPMG Germany*. KPMG. https://kpmg.com/de/en/home/insights/2023/02/cyber-security-in-the-eu-nis-2-directive-increases-security-levels.html

Donmez, U. (2023, April 7). *France accuses Russia of disinformation about French position in Ukraine war*. https://www.aa.com.tr/en/europe/france-accuses-russia-of-disinformation-about-french-position-in-ukraine-war-/2866740

Dwivedi, S. (2023, January 13). *Analyzing European Strategic Autonomy Through the French Lens*. The Geopolitics. https://thegeopolitics.com/analyzing-european-strategic-autonomy-through-the-french-lens/

Eddy, M. (2021, September 10). Germany Investigates Russia Over Pre-Election Hacking. *The New York Times*. https://www.nytimes.com/2021/09/10/world/europe/germany-russia-hacking-investigation.html

ESET Research: Lazarus attacks aerospace and defense contractors worldwide while misusing LinkedIn and WhatsApp. (2022, June 1). ESET. https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-lazarus-attacks-aerospace-and-defense-contractors-worldwide-while-misusing-linkedin-a/

EUvsDisinfo. (2020, April 22). *"To Challenge Russia's Ongoing Disinformation Campaigns": The Story of EUvsDisinfo*. EUvsDisinfo. https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-the-story-of-euvsdisinfo/

Epstein, R. (n.d.). *Banking on markets: The transformation of bank-state ties in Europe and beyond*. https://books.google.com/books?hl=en&lr=&id=ZFExDwAAQBAJ&oi=fnd&pg=PP1&ots=DQyI6dn87H&sig=mSzt3n8XDSgdbsX2FzNLP55r3Y#vonepage&q&f=false

EU. (2022, October 27). *Russian influence in Hungary ING2 Committee Hearing on Russian interference in the EU: the distinct cases of Hungary and Spain.* European Parliament. Retrieved April 17, 2023, from https://www.europarl.europa.eu/cmsdata/256493/OJ%20item%204_peter_kreko_ing2_hearing_20221027_speaking_points.pdf

EU blasts Hungary 'fake news' on migrants. (2019, February 19). BBC. Retrieved May 5, 2023, from https://www.bbc.com/news/world-europe-47294183

Fact checking at dpa. (n.d.). Dpa.Com. Retrieved May 16, 2023, from https://www.dpa.com/en/fact-checking-at-dpa

Faesen, L., Klimburg, A., van Hoeve, S., Minicozzi, R., Siemens, S. P., & Tesauro, G. (n.d.). *Uncovering the Stated & Perceived Offensive Cyber Capabilities of States*.

Friedman, G. (2023, March 7). *Hungary and Russia*. Geopolitical Futures. Retrieved May 3, 2023, from https://geopoliticalfutures.com/hungary-and-russia/

Germany concerned over fake sites with pro-Russian disinformation. (2022, August 30). *Deutsche Press-Agentur*. Access World News – Historical and Current. https://infoweb.newsbank.com/apps/news/openurl?ctx_ver=z39.88-2004&rft_id=info%3Asid/infoweb.newsbank.com&svc_dat=WORLDNEWS&req_dat=5571AD5ADB7245A884D175640FB2C7D8&rft_val_format=info%3Aofi/fmt%3Akev%3Amtx%3Actx&rft_dat=document_id%3Anews%252F18C3BD83F4805E60

Germany notes increase in cyber attacks by Russian actors. (2021, June 21). *BBC Monitoring International Reports*. Access World News – Historical and Current. https://infoweb.newsbank.com/apps/news/openurl?ctx_ver=z39.88-2004&rft_id=info%3Asid/infoweb.newsbank.com&svc_dat=WORLDNEWS&req_dat=5571AD5ADB7245A884D175640FB2C7D8&rft_val_format=info%3Aofi/fmt%3Akev%3Amtx%3Actx&rft_dat=document_id%3Anews%252F18342DE7B3CFD6F8

Germany takes new steps to tackle the energy crisis. (2022, August 24). World Economic Forum. https://www.weforum.org/agenda/2022/08/energy-crisis-germany-europe/

Glover, G. (n.d.). *Luxembourg energy provider Encevo Group battles ransomware attack by BlackCat*. https://techmonitor.ai/technology/cybersecurity/encevo-group-cyberattack-luxembourg-blackcat-ransomware

Gustaaf, G. (n.d.). *Europe and China's Belt and Road Initiative: Growing Concerns, More Strategy*. https://www.jstor.org/stable/resrep21398?seq=1

Grunwald, A. (n.d.). *Luxembourg to screen non-EU FDI under draft bill*. https://delano.lu/article/luxembourg-to-screen-non-eu-fd

Gresh, G. (n.d.). *EUROPE'S NEW MARITIME SECURITY REALITY: CHINESE PORTS, RUSSIAN BASES, AND THE RISE OF SUBSEA WARFARE*. https://www.brookings.edu/wpcontent/uploads/2023/02/FP_20230207_europe_basing_gresh.pdf

Hanemann, T., & Huotari, M. (n.d.). *EU-CHINA FDI: WORKING TOWARDS RECIPROCITY IN INVESTMENT RELATIONS*. https://merics.org/sites/default/files/2020-04/180723_MERICS-COFDI-Update_final_0.pdf

Heil, A. (2023, January 6). *How Viktor Orban Tried To Numb 10 Million Hungarians To Putin's War Next Door*. Radio Free Europe. Retrieved May 19, 2023, from https://www.rferl.org/a/viktor-orban-numbing-hungarians-putins-war-next-door/32212401.html

Horowitz, J., & Alderman, L. (n.d.). *Chastised by E.U., a Resentful Greece Embraces China's Cash and Interests*. https://www.nytimes.com/2017/08/26/world/europe/greece-china-piraeus-alexis-tsipras.html

Hungary: Press freedom threatened as Orbán handed new powers. (2020, March 30). International Press Institute. Retrieved May 18, 2023, from http://ipi.media/hungary-press-freedom-threatened-as-orban-handed-new-powers/

Jason, H., & Liz, A. (n.d.). *Chastised by E.U., a Resentful Greece Embraces China's Cash and Interests*. https://www.nytimes.com/2017/08/26/world/europe/greece-china-piraeus-alexis-tsipras.html

Julia Apostle, Cameron Carr, Rami Kawkabani. (2023, February 3). *France Cybersecurity Update: Cyber-Attacks Must Be Reported to Authorities Within 72-Hours to Benefit from Insurance Coverage*. https://www.orrick.com/en/Insights/2023/02/France-Cybersecurity-Update-Cyber-Attacks-Must-Be-Reported-to-Authorities-Within-72-Hours

Junaid, A. (n.d.). *String of Pearls and China's Emerging Strategic Culture*. https://www.jstor.org/stable/48537578

Kass, D. H. (2023, January 30). *Russia-linked Hackers Launch DDoS Attacks on Germany and U.S. Hospitals, Threaten Canada*. MSSP Alert. https://www.msspalert.com/cybersecurity-news/russia-linked-hackers-launch-ddos-attack-on-germany-threaten-canada-for-ukraine-artillery/

Kayali, L. (2023, March 27). Russian hackers strike French National Assembly website. *POLITICO*. https://www.politico.eu/article/french-national-assembly-website-russian-cyberattack-hack-kremlin-emmanuel-macron/

Kochis, D. (2022, September 28). *Russia's Attack on Nord Stream Pipelines Means Putin Has Truly Weaponized Energy*. The Heritage Foundation. https://www.heritage.org/global-politics/commentary/russias-attack-nord-stream-pipelines-means-putin-has-truly-weaponized

Kyllmann, C. (2023, February 15). *Germany and Belgium to link hydrogen networks, double LNG transit and explore second interconnector*. Clean Energy Wire. https://www.cleanenergywire.org/news/germany-and-belgium-link-hydrogen-networks-double-lng-transit-and-explore-second-interconnector

Komuves, A., & Neely, J. (2020, September 26). *Hungary hit by large cyber attack from Asia – Magyar Telekom*. Reuters. Retrieved April 16, 2023, from https://www.reuters.com/article/hungary-cyber/hungary-hit-by-large-cyber-attack-from-asia-magyar-telekom-idUKL5N2GN03J

Mackenzie, C., & Ferran, L. (2022, November 10). Macron: France's new strategic review to meet "dangerous moment" in the world. *Breaking Defense*. https://breakingdefense.sites.breakingmedia.com/2022/11/macron-frances-new-strategic-review-to-meet-dangerous-moment-in-the-world/

Maninder, D. (n.d.). *Here Is All You Should Know About "String Of Pearls", China's Policy To Encircle India*. https://www.indiatimes.com/news/india/here-is-all-you-should-know-about-string-of-pearls-ch ina-s-policy-to-encircle-india-324315.html

Martirosyan, L. (2023, March 22). *Women politicians who criticise Hungary government face online attacks*. openDemocracy. Retrieved May 8, 2023, from https://www.opendemocracy.net/en/5050/hungary-propaganda-orban-gender-disinformation-online-women-putin-russia/

MEPs: Hungary can no longer be considered a full democracy | News. (2022, September 15). European Parliament. Retrieved May 8, 2023, from https://www.europarl.europa.eu/news/en/press-room/20220909IPR40137/meps-hungary-can-no-longer-be-considered-a-full- democracy

Nattrass, W. (2022, September 15). *Hungary's 'pro-Russia' stance was inevitable – POLITICO*.POLITICO. Retrieved April 15, 2023, from https://www.politico.eu/article/hungary-pro-russia-stance-inevitable/

Negreiro, M. (2023, February 8). *The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Nicolau, A., & Poinsignon, O. (n.d.). *Foreign direct investment reviews 2023: Luxembourg*. https://www.whitecase.com/insight-our-thinking/foreign-direct-investment-reviews-2023-luxembourg

ÖZKAN, C. E. (2023, February 13). *The Impact of the Transcarpathian Conflict on Hungary-Ukraine Relations — ANKASAM | Ankara Kriz ve Siyaset Araştırmaları Merkezi*. ANKASAM. Retrieved April 16, 2023, from https://www.ankasam.org/the-impact-of-the-transcarpathian-conflict-on-hungary-ukraine-relations/?lang=en

Paolo, B., & Sabine, D. (n.d.). *Chinese bank networks in Europe: FDI-oriented by legal and strategic design*. https://www.tandfonline.com/doi/full/10.1080/15387216.2023.2182805?src=

Rachel, E. (n.d.). *Banking on markets: The transformation of bank-state ties in Europe and beyond*. https://books.google.com/books?hl=en&lr=&id=ZFExDwAAQBAJ&oi=fnd&pg=PP1&ots=DQyI6dn87H&sig=mSx3n8XDSgdbsX2FzNLP55r3Y#v

Ronald Bearse – "Understanding Critical Infrastructure" from Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)—Strategic Studies Institute. (n.d.). Retrieved May 16, 2023, from https://ssi.armywarcollege.edu/2023/pubs/parameters/ronald-bearse-understanding-critical-infrastructure-from-enabling-natos-collective-defense-critical-infrastructure-security-and-resiliency-nato-coe-dat-handbook-1/

Russia Set to Export Large Amounts of Diesel Before EU Sanctions. (2022, December 30). *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2022-12-30/russia-set-to-export-large-amounts-of-diesel-before-eu-sanctions

Russia's FSB and GRU have hacked Hungary's foreign ministry since 2013, claims investigative news site. (2022, March 30). bne IntelliNews. Retrieved April 10, 2023, from https://www.intellinews.com/russia-s-fsb-and-gru-have-hacked-hungary-s-foreign-ministry-since-2013-claims-investigative-news-site-239750/

Schmelzer, A. G., Mattias. (2023, January 20). *The Economic Impact of the Russia-Ukraine War—KPMG Germany*. KPMG. https://kpmg.com/de/en/home/insights/2022/05/the-economic-impact-of-the-russia-ukraine-war.html

SCRED, a unique collaborative project for cybersecurity. (2023, April 5). Thales Group. https://www.thalesgroup.com/en/group/innovation/news/scred-unique-collaborative-project-cybersecurity

Serrano, R. M., & DisinfoLab, E. (2023). *DISINFORMATION LANDSCAPE IN GERMANY*.

Sheridan, K. (2020, September 16). *Likely Links Emerge Between Lazarus Group and Russian-Speaking Cybercr*. Dark Reading. https://www.darkreading.com/threat-intelligence/likely-links-emerge-between-lazarus-group-and-russian-speaking-cybercriminals

Süß, J. (2022, November 29). *France: France's New Security Strategy*. https://www.freiheit.org/european-union/frances-new-security-strategy

Shillito, J. (n.d.). *China and Australia to offer financial services in Luxembourg*. https://delano.lu/article/china-and-australia-to-offer-f

Sam, C. (n.d.). *Chinese state-owned enterprises now own 10% of Europe's container terminal capacity*. https://splash247.com/chinese-state-owned-enterprises-now-10-europes-container-terminal-capacity/

Szabolcs, P. (2022, March 29). *Putin's hackers gained full access to Hungary's foreign ministry networks, the Orbán government has been unable to stop them*. Direkt36. Retrieved April 10, 2023, from https://www.direkt36.hu/en/putyin-hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/

Szabolcs, P. (2022, July 18). *Western allies puzzled by Hungary' mild reaction to Russia's hacking*. Telex. Retrieved April 10, 2023, from https://telex.hu/english/2022/07/18/western-allies-puzzled-by-hungary-mild-reaction-to-russias-hacking

Szicherle, P., & Molnár, C. (2021). *Foreign Malign Influence in Hungary*. Political Capital. Retrieved April 15, 2023, from https://politicalcapital.hu/pc-admin/source/documents/Globsec_VI_Hungary-PolicyPaper_final.pdf

Thales and 10 partners launch French cyber threat intelligence platform to support greater autonomy and resilience. (2023, April 5). Thales Group. https://www.thalesgroup.com/en/worldwide/security/press_release/thales-and-10-partners-launch-french-cyber-threat-intelligence

The EU has banned Russian oil products, here's why | World Economic Forum. (n.d.). Retrieved May 2, 2023, from https://www.weforum.org/agenda/2023/02/eu-ban-on-russian-oil-products-ukraine/

Tisdall, S. (2022, October 23). Unseen and underhand: Putin's hidden hybrid war is trying to break Europe's heart. *The Observer*.

https://www.theguardian.com/commentisfree/2022/oct/23/unseen-and-underhand-putins-hidden-hybrid-war-is-trying-to-break-europes-heart

Topic: Women, Peace and Security. (2023, April 17). NATO. Retrieved May 8, 2023, from https://www.nato.int/cps/en/natohq/topics_91091.htm

Total number of banks in Luxembourg as of December 2020, by country of origin of the bank. (n.d.). https://www.statista.com/statistics/683409/number-of-banks-in-luxembourg-by-country-of-origin-of-the-bank/#statisticContainer

William, D. (n.d.). *How AI can help improve intrusion detection systems*. https://gcn.com/cybersecurity/2020/04/how-ai-can-help-improve-intrusion - detection-systems/ 291266/

Zhengzhou-Luxembourg Air Silk Road Forum for International Cooperation Held in Zhengzhou. (n.d.) http://www.caac.gov.cn/en/XWZX/202301/t20230106_216780.html

Conclusion

Russian espionage activities have targeted wind farms and oil refineries in the North Sea, adversely impacting energy security. Additionally, China is increasing its ownership of European logistics and banking infrastructure, providing China opportunities to transfer technology and impede NATO interoperability via their control of European ports.

As evidenced by the case studies, European countries have been disproportionately affected by hybrid warfare tactics since the beginning of the Russian invasion of Ukraine. With such extensive challenges relating to the mitigation of cyberattacks, disinformation, and malign influence, solutions have been created in response to those threats. The first solution is the ability to promote economic independence within each nation mentioned.

Defending cyberspace has become the second crucial step in the fight against hybrid warfare. Cyberattacks emanating from Russia targeting countries allied with Ukraine are increasing, disrupting energy critical infrastructure, impeding transportation and logistics, and compromising vital communication networks. Further, the expansion of smart electric grids leveraging IoT introduces numerous potential entry points that can be exploited by malicious actors to gain access to critical industrial control and communications systems. Lastly, in terms of cyberspace, private companies with public contracts are increasingly being targeted due to their lack of uniform cyber protections and reduced oversight.

The last goal of these nations is to combat disinformation. Highly specific disinformation campaigns that emphasize divisive social issues, historical trauma,

and NATO's military presence in Europe are being disseminated on social media and by Russian-aligned media outlets.

In response to the ongoing challenges of hybrid warfare and the collaboration between NATO and the EU, the following recommendations outline succinct measures that should be put in place to benefit and secure the sovereignty of the countries mentioned.

- Introduce EU-wide FDI screening mechanisms to maintain EU sovereignty over its critical infrastructure.
- Increase physical security of offshore wind farms and oil refineries in the North Sea and beyond through collaboration between NATO undersea rapid response forces and Nordic countries.
- Implement next-generation Cyber Early Warning Systems with AI and virtualization technology across NATO's critical infrastructure.
- Provide funding through the NATO Security Investment Program for private sector cybersecurity capacity building in critical infrastructure.
- Establish cybersecurity standards for private IT providers that have contracts with public CI operators to be overseen by national level CERTs or CSIRTs.
- Require all IT service providers contracting with critical infrastructure operators to undertake a mandatory security audit.
- Implement comprehensive youth education programs on disinformation by national governments.

The recommendations provided will allow stronger European autonomy and create a basis for secure cyberspace, monitored disinformation, and controlled malign influence by global adversaries. Collaboration amongst countries in connection with NATO and the EU can enhance the sharing of intelligence, new

strategies, and advanced technology which will allow countries to build and strengthen their national security. Hybrid warfare is an ever-changing military tactic used in moments of dismay and disruption, however, with the policy recommendations discussed and the extensive analysis on present threats, NATO/EU members can achieve cybersecurity and disinformation goals to better their political stability, social cohesion, and economic freedom.