HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY of WASHINGTON

TASK FORCE

The Donald C. Hellmann Task Force Program

NATO's Response to Hybrid Warfare during the Ukraine Conflict:

Navigating an Era of the China-Russia Partnership

2023

NATO's Response to Hybrid Warfare during the Ukraine Conflict: Navigating an Era of the China-Russia Partnership

Faculty Advisor
Dr. Sarah Lohmann

Evaluator
Georgios Giannoulis
Deputy Director of COI Vulnerabilities and Resilience,
The European Centre of Excellence for Countering Hybrid Threats

Chief Liaison
Pai-Sing Sun

Editors
Max Cheung
Aesha Hendricks

Coordinators
Penelope Beagles
Jennifer Gile
Lily Kinyon

Writers
Ryan Bulger
Erica Dahl
Vitoria Faustino
William Gilfoil
Alina Guyon
Yiqi Huang
Kimber Tanner
Kyla Tiedeman
Kristina Umanskiy
Kelsey Zapf

Jackson School of International Studies, University of Washington
Task Force Report Winter 2023
2 March 2023

Table of Contents

Introduction

Hybrid warfare has emerged as a complex and dynamic security challenge for the North Atlantic Treaty Organization (NATO). Adversaries such as China and Russia have employed hybrid warfare tactics to undermine NATO member states' security and stability through the employment of conventional and unconventional tactics, including malign influence campaigns, economic coercion, misinformation and disinformation operations, and cyber attacks. By identifying the threat landscape of hybrid warfare, this report evaluates the implications for NATO's security, the unity of the alliance, and critical infrastructure. Furthermore, case studies of NATO's response to hybrid threats are presented to illustrate the alliance's current efforts to counter Russian and Chinese hybrid warfare tactics. These case studies illustrate the complexities and challenges of responding to hybrid threats and the importance of a comprehensive approach that combines military and non-military tools. Finally, the report provides policy recommendations on how NATO can enhance its ability to address the challenges of hybrid warfare. These recommendations focus on strengthening the alliance's resilience against hybrid threats, improving information sharing and coordination among member countries, and enhancing NATO's ability to deter and respond to hybrid threats.

Overall, this report aims to provide insights and recommendations on how NATO can enhance its ability to address the challenges of hybrid warfare. By doing so, NATO can ensure the security and stability of its member countries and maintain its position as a key player in the global security landscape in the face of evolving hybrid threats.

Section 1: Malign Influence and Economic Coercion

Executive Summary

This report investigates the use of malign influence and economic coercion against NATO states and proposes several policy recommendations to strengthen NATO economies and critical infrastructure. The first part of this report highlights several recent examples of malign influence and economic coercion utilized by China and Russia against NATO states, while the second part focuses on two major case studies: Chinese malign influence through the United Front Work Department (UFWD)/China Association for International Friendly Contact (CAIFC) and Chinese economic coercion through its dominance of rare earth element (REE) supply chains.

Through the case study on Chinese REE supply chain dominance, this paper finds that it is essential for NATO's economic and military security to act immediately to mitigate the coercive danger of Chinese dominance by diversifying supply chains and developing alternative sources by partnering with other NATO states. China maintains significant economic power over the entire REE supply chain, and while China has not yet leveraged its dominance to the detriment of the NATO alliance, the future security environment prompts immediate action to reduce NATO reliance on Chinese REE exports. It is necessary to develop alternative means to access such crucial resources because REEs are critical to defense and other critical technologies. To continue to rely on China for these resources is to endanger NATO's current and future capabilities.

Further, this paper determines through the second case study on Chinese malign influence operations that UFWD/CAIFC activities present risks to allied information security and social cohesion, and thus necessitate the creation of an autonomous agency to reduce CAIFC influence and the strengthening of state laws and regulations to limit the influence operations and espionage potential of the UFWD in academic institutions. Instruments of Chinese soft power like the UFWD, Confucius Institutes (CI), and CAIFC hold great potential to strengthen the Chinese military industrial complex at the expense of the NATO alliance. These organizations export CCP ideology abroad, enable espionage, and proliferate corruption. Despite such risks, these organizations are under-regulated, under-monitored, and experience little oversight and accountability in NATO states. Therefore, it is necessary for states affected by Chinese influence operations to increase legal accountability and control mechanisms, limit the reach and legitimacy of these organizations, and create pathways to reduce corruption. These soft power instruments may appear innocuous, however they can have insidious consequences.

Hybrid Threat: Malign Influence and Economic Coercion

Russian Energy Coercion

This first address pertains to a critical aspect of a state's economic security and its ability to guarantee its energy supply. The interconnection of energy and fuel grids means that foreign states may be able to interfere with the supply of power, granting another lever by which to influence policy. It is therefore essential that any state diversify and secure its energy supply in order to ensure strategic security.

The Nord Stream 1 pipeline constructed through the North Sea played an integral part in German gas imports in the years preceding the war in Ukraine. Commissioned in 2011, the pipeline was created through a joint effort by the Russian state energy corporation Gazprom and a German foundation established by the state of Mecklenburg-Vorpommern (Solomon, Bennhold 2022). Nord Stream 1 drastically increased Europe's energy reliance on Russia, with it being the largest pipeline carrying LNG imports to Europe in 2022 (Al Jazeera, 2022). The delay of gas flows through Nord Stream 1 and eventual decommissioning of Nord Stream 2 drastically increased tensions, with Putin warning that sanctions would bring increased gas prices to Europe (Al Jazeera, 2022). The 'special military operation' declared in 2022 highlighted this vulnerability, as a huge proportion of Germany's energy supply was now dependent on a hostile state.

The German government launched efforts to build a new LNG terminal on its North Sea coast, completing it in a record eight months. In early 2023, finance minister Christian Lindner announced that the country was no longer reliant on Russian gas, instead meeting its needs through increased imports from the United States and Norway, among others (Hill, 2023). Germany has had to take drastic measures, reopening coal plants and delaying the shutdown of its last three nuclear reactors (AP, 2022).

Although Germany was able to act rapidly, its reliance on Nord Stream imports illustrates how energy supply can pose a critical risk to a nation's economy. A reliance on Russian energy imports became difficult to maintain with the invasion of Ukraine, with Germany initially unwilling to act due to the risk of losing access to vital energy resources. Although able to diversify and add suppliers, the process was far from painless, causing economic losses and disrupting heating throughout the country. In cities such as Hannover, families may have to pay as much as €1000 extra per year due to levies, as well as bans on heaters, radiators, and portable air conditioners (Wehrmann, 2022).

Russian Economic Coercion and Diplomatic Malign Influence

Another recent example of the use of malign influence and economic coercion against NATO states has been Russia's leveraging of its economic dominance and control in the grain industry to exacerbate the global food crisis. During the invasion of Ukraine, Russia has used kinetic attacks to restrict Ukrainian grain production and exports, which has raised prices internationally and contributed to the global food crisis (Chan and Wiseman, 2022). In addition

to these kinetic attacks, Russia has also leveraged its economic and diplomatic power to further reduce global grain supply, thus raising prices, which has threatened greater hunger and starvation in countries that depend on Ukrainian and Russian grain exports. Within NATO, this supply reduction contributed to an increase in food prices, compounding the increase in energy prices due to the energy crisis. This endangers NATO security by negatively impacting allied economies and raising the cost of living, which increases social vulnerability. Additionally, price instability and reduced exports impair states' abilities to access crucial food products.

In the early stages of the war, Russia employed direct economic coercion tactics by restricting its own crucial exports of grain and, more importantly, fertilizer, of which it is the top global producer (Wong and Swanson, 2023). Before the war, Russia and Ukraine together accounted for 1/3 of the world's grain exports, and by restricting its own grain exports, Russia has dramatically worsened the global food crisis (Chan and Wiseman, 2022). Yet more important is the restricted export of fertilizer, a key resource necessary for food production, which impacts the entire international community. Russia has argued these restrictions were a result of harsh economic sanctions by the west, however this was refuted by Western leaders who clarified that the sanctions do not interfere with food exports (Chan and Wiseman, 2022). These export restrictions have reduced the global supply of crucial resources that support the food system and thus contributed to a rise in food prices, negatively affecting the entire international community.

Recently, Russia has expanded to using diplomatic power to slow Ukrainian grain exports and maintain the food insecurity heightened by the war. After agreeing to the Black Sea Grain Initiative, which allows some Ukrainian grain to be exported via the Black Sea to Istanbul, Russia threatened to leave the deal when it came up for renewal, a diplomatic move that caused another spike in prices of 5-6% globally (Wong and Swanson, 2023). Eventually Russia acquiesced to the deal, but diplomatic inconsistency led to greater economic instability by raising food prices once again. Furthermore, Russia (within the implementation of the deal) has used its right of inspection to deliberately slow port inspections of legal Ukrainian grain shipments, which has left some ships waiting as long as a month to dock (Kucukgocmen and Spicer, 2022). In addition to slowing Ukrainian grain exports, Russia prevents access to 7 out of 13 Ukrainian ports, which further inhibits crucial grain exports, as the Black Sea is the dominant shipping route to export grain (Wong and Swanson, 2023). Additionally, throughout the war, Russia has been stealing and smuggling Ukrainian grain to avoid Western sanctions and fund its war

(Biesecker et al., 2022). Russian state-owned companies have stolen Ukrainian wheat, exported it through Ukrainian Black Sea ports, and then utilized ship-to-ship transfers in order to combine the illegal, sanctioned grain with legal grain in order to sell it to legitimate supply chains (Biesecker et al., 2022). These diplomatic roadblocks have slowed the export of Ukrainian grain, a crucial commodity that 400 million people rely on worldwide, which has led to continued reduced supply and higher prices (Chan and Wiseman, 2022).

This economic coercion and diplomatic malign influence that serves to prolong and exacerbate the global food crisis threatens NATO security and autonomy by manufacturing economic harm and social vulnerability. Increased prices have put greater strain on economies already suffering from the energy crisis and attempting to end dependence on Russian energy, which only adds to the rising cost of living in NATO countries. If instability in food prices and supply continues, this will have immense long term international consequences, from worsening starvation and famine in hunger-ridden countries to increasing the economic fragility of NATO states (Chan and Wiseman, 2022).

Chinese Economic Coercion in Telecommunications

In recent years, China has utilized its foreign policy to spread influence and dominate high-tech sectors overseas. The Nordic region has become an especially popular target for China's foreign direct investments in Europe regarding telecommunication systems.
Such investment poses significant cybersecurity risks when Chinese investors have close ties to the Chinese government or military, potentially exposing critical infrastructure information. This is often the case, as said investors are often either run or subsidized by the Chinese state (Cristiani et al, 2021, p. 35). Sweden and Finland are examples of countries that have recognized these threats and actively imposed preventative measures to mitigate high-risk Chinese acquisitions in telecom, including various forms of screening protocols. By coordinating screening regulations with the EU, the governments of Finland, Denmark, and Norway are able to block foreign acquisitions on the grounds of national security and public order (Cristiani et al, 2021, p. 41). In response to this, China has engaged in economic coercion that pressures countries to be less hostile. For example, when Sweden banned the use of equipment from Huawei and ZTE, China's Ministry of Foreign Affairs threatened that Swedish companies would risk consequences and vowed to take "all necessary measures" (Cristiani et al, 2021, p. 36). Despite the national security risks associated, European telecom companies are skeptical of

heavy restrictions on Chinese firms. This is due to investment opportunities as well as cheaper and more accessible Chinese equipment compared to domestically-sourced systems. Consequently, the private sector can be a source of political support for Chinese economic interests at the expense of national security interests.

Despite the protectionist stance towards Chinese firms adopted by Nordic countries, the presence of Chinese telecommunications equipment in the greater European region, including many NATO members, is still a threat to the security and autonomy of nation-states. The hesitancy by European governments to rigorously distance themselves from Chinese telecom suppliers, in addition to their slow responses to enact security measures, has allowed countries such as Germany and Italy to still heavily rely on Chinese systems. It is without doubt that telecommunication is a highly important component of a state's critical infrastructure. Underestimating the cybersecurity risks associated with the use of Chinese systems is not only a threat to NATO members' national security but also to the NATO alliance as a whole. In the context of economic coercion, telecommunication is just one sector that exposes NATO vulnerabilities. Dependence on Chinese technology and materials such as rare earth minerals must be addressed in conjunction in order to effectively mitigate against economic coercion.

Chinese Economic Coercion in Rare Earth Metals

Member states throughout the NATO alliance currently possess significant exposure to economic coercion due to an overreliance on China in the production and processing of rare-earth elements (REE) (Hart, 2020). China enjoys outsized market power along the entirety of the REE supply chain — allied states' continued dependence on China for their vital REE supplies forfeits industrial self-sufficiency and undermines NATO's security and economic capacities.

REEs are utilized as vital industrial inputs across a wide spectrum of strategic industries, with such sectors as defense and sustainable technologies in particular requiring significant volumes of REEs. In regards to defense, REEs are integral in producing guidance and control systems for munitions, capacitance and amplification systems for directed-energy weapons, magnetic elements for motors, and signals equipment for communications. An F-35 Lightning and a Virginia-class nuclear submarine, both central elements of allied air and sea power, respectively require approximately 427 kg and 4.2 metric tons of REEs per unit on average (Lord and The Senate Committee on Armed Services, 2020, pp.11-13). In addition to defense applications, REEs are important components in such sustainable technologies as wind turbines,

solar photovoltaics, and lithium-ion batteries, among other technologies crucial to green energy infrastructure (Hund et al., 2020, p.46). As such, REEs occupy a central role in any competitive industrial base.

In this context, China's dominance in the REE supply chain poses a significant challenge to ensuring allied economic security. Overall, China accounts for approximately 60 percent of global mined REE production and 85 percent of processing capacity. Further, China is firmly embedded in derivative industrial processes such as the production of REE magnets, accounting for over 90 percent of high-strength magnets manufactured (Yao, 2022). In this manner, China not only possesses an outsized presence in REE supply chains, but also exerts vertical dominance across REE value chains and their derivative industrial goods. China's market power is evident in its exports to states throughout the alliance — in 2019, the United States received roughly 57 percent of China's lanthanum exports, and the Netherlands received roughly the same proportion of China's europium exports (Hart, 2020). As such, China's market dominance in REEs has allowed it to gain significant influence over allied supply chains and industrial activities.

In addition to its pre-existing dominance in REE production, China has taken steps to prolong allied reliance on Chinese REE supplies. China has leveraged its dominant market position and attendant price-setting powers to erect barriers to new entrants and would-be competitors — periodically, China has strategically flooded the REE market to price out potential competitors (United States Department of Defense, 2018, p.29). Further, China has utilized disinformation campaigns to prevent the opening of rival REE mines by instigating public controversy and alleging false environmental and health effects of REE mining (Go, 2022). Finally, China has utilized overt economic coercion by leveraging REE exports to achieve its foreign policy goals. In 2010, territorial disputes over the Senkaku Islands led China to suspend REE exports to Japan until a WTO ruling compelled China to revoke its export curbs (Bradsher, 2010). And although China has yet to employ such overtly coercive tactics against NATO states, the Chinese government has explored the potential effects of restricting REE exports to the EU and the US. Chinese officials went so far as to specifically inquire after how the US defense industry, with an emphasis on F-35 production, may be impaired by export restrictions (Sevastopulo et al., 2021). In this regard, allied states may have to prepare for similar export restrictions and supply chain disruptions should NATO-China tensions escalate.

Failing to address supply chain vulnerabilities and existing exposure to Chinese economic coercion threatens NATO security and policymaking autonomy by compromising the integrity of the allied industrial base. An inability to secure vital supply chains and effectively administer manufacturing and other economic processes constitutes a failure to maintain economic security and weakens NATO's capacity to provide collective security to its members.

Chinese Malign Influence by the United Front Work Department (UFWD)

In examining further examples of malign influences, the PRC's use of the United Front Work Department (UFWD) represents a less explicit form of threat toward NATO allied nations. The UFWD was an instrument initially employed by the Communist Party during the Chinese Civil War to co-opt non-party actors and marginalized communities within China to isolate the Nationalist Party into defeat (Fedasiuk, 2020). Although the UFWD has since expanded to also serve China's overseas national interests, its core function has remained the same: propagating the Chinese Communist Party's (CCP) ideology.

Today, the UFWD co-opts overseas ethnic Chinese individuals and communities to carry out influence operations abroad. Its purpose is to induce foreign actors and states to take actions or adopt policies that are favorable to the interests of the CCP. UFWD foreign operations are largely conducted through UFWD-affiliated foreign institutions, namely Confucius Institutions (CI) and Chinese Student and Scholar Associations (CSSA). Currently, there are hundreds of CIs operating globally as academic hubs for Chinese language, culture, and history education; CIs are staffed by CCP-selected instructors who teach a sanctioned curriculum (Bowman, 2019). As of 2020, the U.S Department of State has reported an estimate of 66 CIs embedded in higher education institutions and over 500 K-12 programs operating within the United States (Hartman, 2020). Faculty at CI host universities have reported threats from CIs to remove funding for individuals and activities that are deemed critical of the CCP (State Department, 2020), thereby eroding academic freedom and influencing future policy-making decisions with implications on state autonomy. But more importantly, these overt UFWD tactics have highlighted the CCP's desire to control the narrative of China's international image and potentially employ a divide-and-conquer strategy within NATO states to encourage domestic dissent. In response, the U.S. Department of State has designated the CI network as a foreign mission of the PRC to enable greater levels of transparency on CI operations in the U.S. (State Department, 2020).

Similarly, the prevalence of CSSAs on university campuses has been of increasing

concern to NATO, representing a salient covert threat to national security. There have been several reports of CSSAs in NATO states having connections with the UFWD. For example, *Le Monde*, a French newspaper, reported that a CSSA in Leuven was in fact an economic espionage network operating for the CCP (Luard, 2005). In addition, Foreign Policy reported that the Georgetown University CSSA had received half of its annual budget from the CCP (Allen-Ebrahimian, 2018). U.S. counterintelligence has also claimed that a member of the University of California, Berkeley CSSA was working as a Ministry of State Security informant to report on the activities of other Chinese students in the university (Dorfman et al., 2018).

The UFWD is a CCP instrument that poses a pervasive and profound threat to the security and autonomy of NATO countries. The use of CIs to engage in overt influence operations, motivated by a divide-and-conquer strategy, has prompted the German government to shut down CIs as a response (Hartman, 2020). Moreover, the use of CSSAs as a covert instrument—co-opting citizens to conduct espionage for the CCP—will be an increasingly difficult threat for NATO to address, potentially jeopardizing sensitive information from critical industries.

Case Study of NATO Response

To illustrate the dual importance of both malign influence and economic coercion as crucial hybrid threats, this section will focus on two case studies, one to recommend policies to counter Chinese economic coercion and the other to recommend policies to improve NATO resistance against Chinese malign influence operations. First, the current coercive threat posed by Chinese economic dominance in the REE supply chain will be described and recommendations will be outlined, clarifying when and where the proposed policies could be implemented. Second, this section will discuss the threat posed by Chinese influence operations-primarily the UFWD and CAIFC- and offer several policies to reduce the threat of espionage and the export of CCP ideology.

Chinese Economic Coercion

Who is Employing Economic Coercion Tactics?

China’s dominance in global rare-earth element (REE) supply chains represents a potential avenue of economic coercion for the NATO alliance. Due to its immense market power along all stages of the REE supply chain, every state within the alliance would be vulnerable should China choose to restrict REE exports or otherwise obstruct allied access to REE supplies.

Although China has yet to leverage its dominance in REEs to implement overt economic coercion against NATO states, its capability to do so has been demonstrated against Japan, a crucial US ally and NATO partner in the Indo Pacific (Bradsher, 2010). Yet, China has inquired into how similar measures may be employed against allied states, with the Ministry of Industry and Information Technology reportedly studying the effects of hypothetical export restrictions against the US and European defense contractors. Specifically, Chinese authorities sought to gauge the extent to which export restrictions would affect allied capacity to produce advanced defense assets such as the F-35 stealth fighter (Sevastopulo et al., 2021). As such, China may already be in the process of preparing coercive economic measures to utilize against NATO states in the event of heightened tensions or allied confrontation.

In this context, NATO possesses an overriding security interest in securing REE supply chains and insulating the allied industrial base from Chinese coercion. Within the alliance structure, responsibility for coordinating NATO-wide efforts to assess economic vulnerabilities and promote supply-chain security lies with the Economics and Security Committee (ESC). Under this proposal, the ESC would be the primary coordinating body for allied risk assessment and joint strategic planning. Regarding implementation, given that NATO's institutional mandate lies predominantly within the realm of defense, the alliance may seek to work with the European Raw Materials Alliance (ERMA), an EU body tasked with bolstering European supply chains and economic security, in incorporating allied economic and security strategy into actionable policy.

What Policies Should Be Implemented to Address Economic Coercion Threats?

A compelling allied strategy to address vulnerabilities emanating from REE supply chains would advisably satisfy two primary criteria. Firstly, allied strategy could seek to assess and address existing supply chain vulnerabilities faced by allied states—current trade exposure to China in REEs for each NATO state would be considered, and means by which states can minimize said exposure would be developed. Secondly, allied strategy could take into account that demand for REEs is variable and will likely increase over time, and would thus include provisions to accommodate increased future demand for REEs. As such, allied strategy would advisably include not only the diversification of existing supply chains, but also the development of new supply chains to both minimize coercive risk and accommodate growth in demand. As

such, this task force recommends the following three-part plan to bolster allied supply chain security:

1. Establish an economic security sub-committee within NATO's Economics and Security Committee to perform a comprehensive review of allied REE supply chains and consult allied governments on supply chain diversification and risk mitigation.
2. Promote the development of alternative supply chains, in collaboration with the European Raw Materials Alliance, by increasing mutual trade and investment in REEs between allied states and non-NATO partners.
3. Encourage allied states to establish or enlarge REE strategic reserves.

The sub-committee established by the first measure would perform a comprehensive and detailed assessment of NATO's strategic supply chains, in particular those relating to defense, in order to provide an accurate appraisal of NATO's economic vulnerability to Chinese REE coercion. Based on such findings, the sub-committee would then serve in an advisory role in consulting allied governments on supply chain diversification and the minimization of exposure to Chinese REE sources. Finally, the sub-committee would develop contingency strategies to be implemented in the event of severe supply chain disruptions. Considering rising NATO-China tensions and the possibility of a crisis in the Taiwan Strait, which would invariably affect Chinese REE exports, the sub-committee would investigate means by which the impact on the allied industrial base might be minimized.

The second measure would allow the minimization of allied dependency on REE exports by developing alternative supply chains within a grouping of NATO and NATO-aligned states. It would entail NATO cooperation with the European Raw Material Alliance (ERMA) for the promotion of trade between alliance members and with NATO partners in the EU to offset Chinese exports, as well as the coordination of investment and the support of new REE production capacities to guarantee supply chain security. Investment efforts would target firms engaged in REE exploration, mining, and refining operations to ensure coverage of all stages of the REE supply chain.

The last measure would entail the establishment or enlargement of dedicated REE strategic reserves. Such reserves would function much in the same manner as the US's strategic petroleum reserve — REEs would be accumulated in the reserves during periods of relative price stability and released in the event that market prices for REEs breach a certain threshold, and

thus impacting the ability of allied states to secure an adequate supply of REEs. The enlargement of strategic reserves could also be utilized as a stabilizer for the aforementioned second measure, by which an expansion of allied demand for the purpose of enlarging reserves can offset the market distortions created by directed investment and production subsidies. In this respect, strategic reserves may be operated in tandem with supply-side measures to provide a guaranteed market for expanded production capacities.

Timeline for Policy Implementation

In order to minimize the risks of coercion stemming from tensions with China that are likely to escalate in the foreseeable future, the task force recommends these measurements be set in motion immediately, in order to have an adequate REE supply chain by 2027. The time frame to establish these policies and structures is set on the basis of increasing concerns that China will eventually seize Taiwan, sooner rather than later. One of several reasons why this may happen around 2027 include a symbolic invasion ahead of China's 100th anniversary celebrating the People's Liberation Army (PLA) in 2027 (Grossman, 2021). In addition, it is projected that in 2024, Taiwan will hold a presidential election that could potentially involve a pro-independence figure, current vice president Lai Ching-te as a nominee. If Lai were to be elected under the Taiwan-centric Democratic Progressive Party, China would likely view his victory as an unacceptable step towards Taiwanese independence (Grossman, 2021). It is highly likely that China would weaponize politics to justify an attack on Taiwan after 2024 if this scenario were to become reality. With this in mind, the 2027 aim is a reasonable timeline that NATO could begin to move forward in order to be ready for these potential events that could lead to a costly war. In order to meet these obligations, accountability mechanisms could be implemented by the EU, an entity capable of legislating and enforcing economic policy. By working in collaboration with NATO, frequent joint meetings will outline each step necessary to create durable and diversified supply chains. This process would allow transparency, mobility, legislation and regulation across borders to ensure that the allied industrial base is adequately protected by 2027.

Where Could the Policies Be Implemented?

To promote supply chain diversification, largely-untapped REE reserves in Norway and Sweden could be utilized to meet NATO's industrial demands. EU initiatives have already prioritized the development of REE production in Northern Europe, with targeted investment in Norway and Sweden already underway (Norge Mining, 2023). As such, NATO may seek to

coordinate with existing EU initiatives to develop new supply chains centering on Northern Europe's significant REE reserves.

LKAB, a Swedish state-owned mining firm, announced in January the discovery of new REE reserves containing an estimated 1 million tons of rare earth oxide deposits. The new Per Geijer deposit, located in Sweden's northern Kiruna region, is the largest known rare earth oxide deposit in Europe (Reuters, 2023). However, although LKAB is due to submit an application to exploit the reserves in 2023, the stringency of existing Swedish and European mining regulations may delay the commencement of actual mining operations to 2033 or beyond (Institute for Energy Research, 2023). Nevertheless, Sweden has accelerated new investment in REE processing to accommodate new extraction capacities in Northern Europe; LKAB recently acquired a controlling interest in processing technology firm REEtec, and plans to open two commercial-scale plants to accommodate new mining operations by 2026 (Myles, 2023).

Norway has enjoyed similar success in REE exploration; the Norwegian Petroleum Directorate has discovered significant REE deposits in Norway's territorial waters, and Norwegian firms are currently in the process of exploring REE deposits in the Fen Complex in Telemark County (Jakobsen & Amundsen, 2022; Paddison, 2023). The Fen Complex in particular possesses large deposits of carbonatite with significant proportions of neodymium and praseodymium, both of which are crucial in the production of advanced magnet technology (Jakobsen & Amundsen, 2022).

In this regard, Norway and Sweden could serve as the center of a new Northern European REE supply chain. The EU, acting through the European Raw Materials Alliance (ERMA), has already taken the initiative in mobilizing and directing investment towards REE projects in Northern Europe — as of 2022, ERMA oversees 14 raw materials projects representing EUR 1.7 billion in investment (International Energy Agency, 2022). Two Norwegian firms, Rare Earths Norway and Norge Mining, have already received ERMA funding for the purpose of REE production (Jakobsen & Amundsen, 2022; Norge Mining, 2023). NATO expertise in defense logistics and production, as embodied within the Economics and Security Committee (ECS), could thus operate in tandem with the ERMA to ensure that the material needs of the allied defense industrial base are met. By integrating input from allied defense planning into ERMA REE initiatives, NATO's capabilities would be insulated against Chinese economic coercion through the joint development of a Northern European REE supply chain.

Why Should the Policies Be Implemented?

REEs are a vital industrial input in a wide variety of strategic sectors, with advanced defense technologies in particular requiring large quantities of REEs. In consideration of the significant challenges of the current security environment, ensuring that NATO can maintain access to integral defense technologies is of the utmost importance, and requires a consistent and secure supply of REEs. In this sense, China's dominance of REE markets, and thus the potential for Chinese economic coercion, represents a significant threat to NATO's economic security. This report recommends NATO take immediate action to insulate its industrial base from China and achieve a secure and independent REE supply chain capable of meeting the alliance's defense and industrial needs.

The above-mentioned three-part plan seeks to address allied vulnerability to China by identifying, mitigating, and eventually eliminating reliance on Chinese REE exports entirely. In essence, the plan represents an industrial policy aimed at offsetting and replacing Chinese presence within the allied REE supply chain by cultivating allied production capacities and crowding out Chinese exports. Increased trade between NATO and NATO partners would encourage the development of alternative REE supply chains, while mutual investment and subsidization of REE production would lower economic barriers of entry for REE firms and blunt the effect of Chinese gatekeeping measures such as market dumping, which have been employed to restrict the number of competing REE firms outside of China. Additionally, the implementation of a strategic reserve scheme would allow the alliance to accumulate REE supplies and provide guaranteed markets for the excess supply that may be generated from investment and subsidization of REE production.

It should be acknowledged that, as an industrial policy, implementation of the three-part plan would necessitate the distortion of naturally-occurring market equilibria. If not managed carefully, supply-side measures such as the subsidy and investment scheme could distort REE markets and thus destabilize market prices for REEs. Although the strategic reserve scheme is designed to mitigate against these effects, an industrial policy nevertheless carries the risk of market distortion. However, in consideration of the strong allied interest in guaranteeing the

security of REE supply chains and shielding allied states from economic coercion, it is necessary for NATO to act boldly in reshaping supply chains to the advantage of the allies.

Chinese Malign Influence

Academic Influence of United Front Works Department

The United Front Work Department (UFWD) is a critical tool that the Chinese government uses to spread its influence abroad, as well as monitor both rival states and its own citizens in other countries. An important aspect of this monitoring is the extensive levels to which the UFWD funds and supports Chinese-national students studying at foreign universities. Through organizations such as the Chinese People's Political Consultative Conference (CPPCC) and the China Scholarship Council (CSC), the UFWD funds hundreds of thousands of students to study abroad in other countries every year. Other groups such as the Chinese Association for Science and Technology (CAST) conduct outreach programs to convince students to bring their expertise back to Chinese firms which are often state-run enterprises (Lloyd-Damnjanovic, Bowe, 2020).

Many of these scholarship and study abroad programs are coordinated through the CPPCC, which is in turn led by a standing member of the CCP's politburo committee, the highest authority within the Communist Party (Bowe, 2018). The CPPCC is a body that organizes and coordinates outreach and influence groups under the CCP's leadership. It funds and operates many elements of the UFWD, including those that provide covert influence, intelligence, and overseas military and industrial espionage. One crucial element of this is through funding student groups that bring talent from western universities back to Chinese firms associated with the military industrial complex.

The CSC is an online platform that hosts job offers from Chinese firms, many of which are closely associated with or directly related to the PLA or CCP. CSC has hosted job advertisements for China's nuclear weapons program as well as for the "seven sons of national defense", a group of seven universities directly subordinate to the Ministry of Industry and Information Technology and deeply integrated into the military industrial complex (Bowe, Lloyd-Damnjanovic, 2020). In addition to offering scholarships, the CSC connects students with industries integral to the Chinese military. These students are trained at western universities, usually in STEM-related fields, before integrating into the Chinese military industrial complex. Another way that China uses western institutes to develop its military capability is by sending

researchers directly involved in military fields to study at universities abroad, notably in Australia and the USA. These universities are often unaware of their students' ties to the PLA, assuming that they were vetted through their visa process (Bowe, Lloyd-Damnjanovic, 2020).

Since the Tiananmen Square Massacre, the CCP has sought to ideologically control and monitor its students, both abroad and in China. CSSAs, or Chinese Student and Scholar Associations, are state-funded organizations that act as social hubs and influence groups that monitor Chinese students and export CCP ideology. These groups mobilize and co-opt student groups into compliance with the CCP. CSSAs often receive funds directly through embassies and consulates, providing services to Chinese students abroad such as finding housing and roommates. However, the groups also conduct industrial espionage and report other students. In the mid-2010s, US intelligence reported that a CSSA member was reporting other members to the MSS (Bowe, 2018). These CSSAs allow MSS and Chinese intelligence to monitor its students abroad through reports from other members.

Confucius Institutes, or CIs, are another form of Chinese influence group. The CIs are funded by the CCP propaganda department and work closely with the UFWD in order to export Chinese language, culture, and history, particularly history that aligns with CCP views. These groups serve as a soft-power export mechanism, which the CCP uses to build positive opinions of China and disseminate CCP propaganda. Confucius Institutes provide counter-narratives to western ones about China, and often organize protests against topics deemed contrary to CCP narratives (Bowe, 2018). Confucius Institutes require partner universities to sign an eight-pointed agreement requiring them to be allowed to propagate CCP propaganda, and often attempt to censor any material related to Taiwan, Tibet, and Xinjiang.

What Policies Can Be Implemented?

In order to counter the effects of PRC agents in western institutions conducting intelligence and influence operations, certain measures could be taken by allied states. States could conduct additional screening, particularly for students involved in matters related to national security. Students who transfer into fields related to national security could also be screened by the State Department/Ministry of Education, a loophole that is being exploited in the US (Bowe, Lloyd-Damnjanovic, 2020). It is essential that states do not implement total bans on students coming from China, as they bring needed funds and expertise to western universities. However, screening and background checks could be conducted by the departments and

ministries of education to ensure exchange students do not have ties to the Chinese military industrial complex. Groups such as CSSAs could be recognized as foreign institutions by NATO states, and denied state funding or university resources unless they comply with government requirements, such as not being funded by CCP. CSSAs that do receive funding from Chinese state-aligned groups could be required to state where their funds come from. Dissemination of CCP propaganda could also be monitored and prevented under state security laws, particularly when being exported to students.

When Should the Policies Be Implemented?

For these recommendations to be most effective, the proposed policies could be implemented by the relevant government authority, likely the allied states' departments and ministries of education. These institutions within affected NATO states could implement screening requirements for students at a national level, ensuring there will be universal student screening irrespective of the university. The state DOE/MOE also could be responsible for officially labeling Chinese soft power academic organizations as foreign institutions, thereby formally designating their Chinese affiliation and clarifying their aims to the public. These policies are most relevant to the NATO states that currently have a significant number of active Chinese educational organizations; mitigating measures would ideally begin in such highly-exposed states. Overall, however, we recommend all NATO states formally designate Chinese educational institutions as foreign institutions in a timely manner so that universities and the general public can be made aware of the true purpose of these organizations. Due to the discriminatory potential of student screening processes, it is important to ensure that students are not being denied acceptance at universities due to their Chinese nationality and that screening will only affect those students who have substantive ties to the Chinese military industrial complex. While this screening policy is important for restricting Chinese students from studying strategic subjects in NATO countries to then use against the alliance, we recommend the policy be carefully planned and executed to ensure no unjust discrimination occurs.

Why Should the Policies Be Implemented?

The UFWD and associated Chinese soft power instruments like CIs and CSSAs are important examples of Chinese malign influence, yet they are often under-regulated and are able to operate freely such that influence operations can institutionalize and normalize their actions in NATO states. To counter the spread, espionage potential, and normalization of these groups, it is

important to both clarify their status and intentions to the wider public and to take regulatory actions to limit their reach in academic institutions. The act of designating these groups as foreign institutions alone, while primarily symbolic, can lead to greater regulation of these groups in the future, for example by implementing disclosure requirements. Such designation is a crucial first step. Further, it is important for the general public to see the government officially name these groups and clarify their aims so that citizens can have an informed understanding of what these organizations do. With respect to student screening processes, it is necessary for NATO's military security to reduce the number of Chinese students connected to the Chinese military industrial complex studying strategic topics, as this could significantly endanger NATO security for years to come.

Diplomatic Arm of the United Front Works Department

Aside from targeting academic institutions, China's UFWD also operates to proliferate its influence at the higher echelons of foreign governments. Specifically, the China Association for International Friendly Contact (CAIFC) has been acting as the Chinese government's proxy to engage in covert influence operations abroad. On the surface, the CAIFC maintains an innocuous visage, aiming to promote people-to-people exchanges and serving as a facilitator to promote economic cooperation between China and the rest of the world (CAIFC Site, n.d). Yet, in truth, the CAIFC works to influence defense policies in foreign countries by developing relations with former leaders, military officials, and diplomats (Kroll and Choma, 2017). John Garnaut, adviser to the Australian Prime Minister, described the CAIFC as a Chinese tool to target "self-interested or naive intermediaries" (Garnaut, 2018).

The CAIFC co-opts high-value foreign individuals, employing a wide range of tactics. For example, the Biden family was reported by the New York Post as having an extensive relationship with a former CAIFC leader, Ye Jianming. In 2017, one month after then-Vice President Biden left the office, Hunter Biden began working for Ye as a counselor and advisor, while James Biden had already received funds from Ye—a further $5 million was provided by Ye to the Biden family as an interest-free unsecured forgivable loan to fund operations in Hunter Biden's firm (Schweizer, 2022). To further illustrate, the Sanya Initiative, established in 2008, is a CAIFC initiative aimed at influencing former senior U.S. flag and general officers. The CAIFC was previously successful in influencing Admiral William A. Owens to publish an op-ed opposing the Taiwan Relations Act, who at the time had business interests in China and Hong

Kong (Gershaneck, 2020).

What and Where Policies Should Be Implemented?

In addressing CAIFC influence operations, NATO states could act to mitigate the risk of CAIFC-compromised individuals. The CAIFC targets former officials to circumvent corruption laws. Thus, NATO states could employ stricter anti-corruption and anti-influence mechanisms by establishing an autonomous agency. The agency will be imbued with statutory powers to enforce laws that will implicate even the highest levels of civil service positions. In this context, this task force recommends the enactment of the following policies:

1. The agency will enforce laws on foreign financial transactions and lobbying, imposing a lifetime ban on presidents and vice presidents with a decreasing time period for lower-level officials.
2. The agency will monitor current and former civil service officials to ensure transparency in engagement, disclosure of funding, and editorial conflicts of interest related to CAIFC.

In light of heightened tensions between NATO and its adversaries, the consequences with regard to sensitive information leakage have risen. Thus, the proposed agency should seek to enforce a greater level of scrutiny on former officials that have worked in foreign policy-sensitive areas, such as the military, defense department, foreign service, and legislative branch. Furthermore, the agency should seek collaboration with law enforcement agencies with covert expertise, such as the United States' FBI or Germany's Bundesamt für Verfassungsschutz (BfV), to enhance its monitoring and enforcement capabilities. Also, strict penalties should be imposed on individuals that fail to comply, serving as a form of deterrence. Once an individual has been implicated by the agency's investigations, the enforcement arm of the agency will move to prosecute. After this time, the individual will be indicted and undergo legal proceedings.

When Should the Policies Be Implemented?

In determining the scale of implementation, NATO allies should consider their respective level of exposure to Chinese influence —the greater a state's exposure is, the more comprehensive an implementation will be. NATO states that have previously been susceptible to CAIFC, or more generally, UFW, operations —specifically the United States and Germany— should ensure the full functionality of the proposed agency. The recommended timeline, in regard to NATO states with high vulnerability, would be for immediate enactment of the policies and creation of the proposed agency, filling leadership positions with trusted senior bureaucratic

officials that have been free from infractions. Since the proposed agency will be vested with the power of enforcement and counterintelligence responsibilities, recruitment from military intelligence departments, state intelligence agencies, and law enforcement departments is encouraged. This will ensure an adequate level of expertise during the inception of the agency. In contrast, NATO states with lesser foreign policy implications for China, for example, Greece and Croatia, could consider implementation at a slower pace and smaller scale. However, the aforementioned NATO states should still consider adopting a similar implementation framework. Furthermore, NATO states could be encouraged to explore intelligence sharing agreements in the context of CAIFC operations, allowing a deeper integration of NATO security endeavors.

Why Should the Policies Be Implemented?

In many regards, former senior government officials still hold a significant level of influence. Their reputation has the potential to sway public and policy discourses, influence the government through official or unofficial advisors, and provide access for the CAIFC to engage with government officials. The recommended policies will thus provide a deterrent to individuals that are vulnerable to Chinese bribes and incentives. Though the proposed policies would certainly have implications on recruitment rates for the government, as they would deter potential individuals who are working, or may have ambitions to work, for Chinese businesses from entering the civil service in NATO countries. Nevertheless, if done correctly, the benefits of having a government independent from Chinese influence can outweigh the costs.

Conclusion

Foreign economic coercion and malign influence will increasingly threaten to destabilize allied security. As a result, NATO states must act quickly to limit the widespread use of malign influence and economic coercion strategies by foreign adversaries. China and Russia, in particular, will continue to pursue policies in pursuit of their national interests to become leaders in global governance. The contention between the Russia-China "no limits" partnership and the NATO alliance will uncover new avenues for hybrid warfare, compelling NATO states to identify economic and diplomatic vulnerabilities in their institutions. The challenge for NATO states is thus to protect their interests against a possible increase in state-sponsored malign influence and economic coercion while also finding ways to cooperate with China and Russia in the context of global governance.

Section 2: Disinformation

Executive Summary

Disinformation is the deliberate construction and spread of fabricated information to deceive the public as well as undermine governing institutions. These falsehoods can be spread through various methods, ranging from the use of social media platforms to manipulate search systems (Tucker et al., 2018). As technology progresses over time, disinformation campaigns are continuously evolving in hybrid warfare making it difficult to eliminate. They consistently harm communities while undermining the stability of state autonomy and national security.

Since Russia's invasion of Ukraine, referred to as a 'military operation' by the Kremlin, beginning February of 2022, Russia has shown that they are notoriously well-versed in disinformation tactics. These schemes have sewn distrust, confusion, and deception across the globe (Zabjek, 2023). The conflict in Ukraine has exacerbated the use of disinformation as a method of hybrid warfare, with Russia continuously deploying disinformation campaigns against many NATO states and allies, such as Lithuania, Italy, and Poland.

A NATO-based Rapid Response Team (RRT) would enable collaborative partnerships with outside entities such as grassroots organizations and NGOs. This RRT would work alongside NATO's Partnerships and Cooperative Security Committee (PCSC) to ensure advantageous partnerships, collaborating with EUvsDisinfo Lab, Reboot Foundation, News Literacy Project, and the Institute for Strategic Dialogue (ISD) to foster and develop public anti-disinformation capabilities. Multiple nations, including Poland, Lithuania, Bulgaria and Romania, have begun developing teams to counter disinformation, while EUvsDisinformation has produced 'Disinformation Database' websites that are worth emulating while implementing NATO's RRT.

Many Confidence Building Mechanisms (CBMs) have been implemented into the RRT through suggested partnerships and education campaigns. These connections can provide outreach to Critical Energy Infrastructure (CEI) workers and student communities to expand education and develop critical thinking skills that enable them to question, recognize, and report disinformation effectively. Additionally, grassroots and NGOs, such as Vox Ukraine, EUvsDisinformation, and ProPublica have already established confidence with the public. Confidence can also be fostered further by improving public access to more affordable wire services such as Anadolu Agency.

NATO would benefit from adding disinformation media responses to limit the cycle of disinformation campaigns. To avoid legal ramifications with media recommendations, filtering trending topics and applying disinformation penalties through collaborating with the European External Action Service is ideal.

Hybrid Threat: NATO Disinformation Response

Disinformation can be understood as the deliberate creation and spreading of false information to deceive the public and ultimately undermine governing institutions through various methods, including selective censorship, manipulative search systems, and directly sharing disinformation via social media platforms (Tucker et al., 2018). Disinformation has been used by political bodies for decades but has had a gradually increasing presence in warfare with the growth of the internet and social media platforms. These platforms allow for easy broadcasting of disinformation campaigns worldwide and can be seen in Russia's past campaigns targeting the United States and international Russian-speaking communities, alongside campaigns to deny war crimes such as execution-style brutality in Bucha (Giannoulis, Hodges in Lohmann, 2022, p. 49; EUvsDisinfo, 2022).

Figure 1: War crimes committed by Russia that were shrouded in disinformation; https://euvsdisinfo.eu/still-at-war-russias-disinformation-targeting-ukraine/

Russia's war against Ukraine has demonstrated the range and extent of efforts that can be made by actors to spread disinformation and highlights the urgent need for methods to counteract such efforts. Russia utilizes disinformation to simultaneously bolster the purpose of their 'military operation' and control the narrative, as seen when Russia declared their victory "inevitable" to rally troops, discrediting the legitimacy of Ukraine's sovereignty, and claiming that Ukraine was the aggressor and a "NATO Proxy" (EUvsDisinfo, 2023).

The full scope of Russia's disinformation spans beyond the boundaries of combat itself. In October of 2022, many representatives and countries in the Global South believed disinformation campaigns claiming Russia's invasion of Ukraine as a proxy war against NATO and that the economic sanctions on Russia were to blame for the ongoing food crisis (EUvsDisinfo, 2022).

The combined disinformation of this 'proxy war' campaign and a false blame on the agriculture shortage could prove problematic for NATO's diplomatic efforts. In January of 2023, Russia began shifting their media coverage of the war to drive wedges between NATO states by discouraging aid from the West, framing the United States as an 'eternal enemy' to Russia, and threatening Poland with implications of a Russian-Belarus partnership (EUvsDisinfo, "Shifting the focus, engineering paranoia, manufacturing fake threats", 2023). Around this same time, Russia had been calling for 'peace proposals' during the war; these negotiations proved to be primarily PR attempts to improve their international reputation and maintain a positive image, while the reality of the war is that there are ambiguous claims in Ukrainian territory - regions that, as Russia claims, have always been and will be part of Russia (EUvsDisinfo, 2023).

Figure 2: The ambiguous claims of territory between Russia & Ukraine; https://euvsdisinfo.eu/russian-so-called-peace-proposals-are-empty-pr-stunts/

Disinformation should be classified as a security threat – both nationally and internationally – for multiple reasons, including the threats it poses to both socio-political narratives and critical infrastructure (Hammond in Moore, 1997, p. 3). Not only does disinformation have a widespread reach, but the range in which disinformation outbreaks can occurs is also vast, impacting the Internet of Things (IoT), media outlets encompassing social media, broadcasting, government-run websites, educational developments, fictitious campaign propaganda, and even false commercial advertising, as well as countless others (Giannoulis in Lohmann, 2022, p. 47). Whether the goal is to overwhelm the public or misinform altogether, disinformation has a strong influence on the public's perception and emotional responses (Stevens, 2022, 1:32; EUvsDisinfo, 2023). Based on this, disinformation is a threat to national security that will only increase in prevalence the longer it goes unaddressed and unsupervised (Giannoulis in Lohmann, 2022, p. 46-47).

The threat to national security can be seen specifically through disinformation attacks on government websites. In March of 2021, the Polish government websites for the National Atomic Energy Agency and Health Ministry were hacked to spread a disinformation campaign claiming that a supposed radioactive threat was coming from the nuclear energy plants of their neighboring ally, Lithuania (EUvsDisinfo, "Polish state websites hacked and used to spread false

info", 2021). Had this story received more traction and the workers at the nuclear energy plants decided to not work from risk of radiation poisoning, critical infrastructure would not be able to produce energy, which would in-turn lead to energy shortages and loss in revenue. Additionally, these energy shortages often affect the normalcy of public life, as well as the functioning of technological security. For nations such as France, who sourced 69% of their energy from nuclear power as of 2021, a disinformation campaign to sow distrust could prove problematic for trust in atomic energy (Statista, 2023).

The use of disinformation is destructive in establishing trust and confidence in government-connected projects, especially as disinformation campaigns have become more sophisticated and effective in the age of digital media. As technology and social media develop, so do the disinformation campaigns' ability to tailor information to each target group, making these efforts more difficult to detect (Giannoulis in Lohmann, 2022, p. 45, 47). Trust is vital in ensuring a working democracy, especially when less public resistance also means better support in establishing an efficient government apparatus.

Disinformation is used in various forms to ensure negative effects on the targeted country. Due to ever-increasing technological advances, European countries have been experiencing cyberattacks at a greater rate than previously recorded. Combatting disinformation requires defense mechanisms to detect and mitigate it. European nations, both within NATO and outside, are slowly forming agencies to combat Russian disinformation groups that target government initiatives. For example, Sweden has implemented the Swedish Psychological Defense Agency (SPDA) to safeguard against cyber-attacks, including disinformation (Suliman, 2022). This organization mitigates disinformation during election campaigns, which are common targets of disinformation operations. The SPDA is a government body that will work with the justice department to monitor and "equip the Swedish population with the skills to spot fake news." (Suliman, 2022).

Although not a new strategy, disinformation has become more elaborate, resulting in new patterns. Russia's neighbors, the Baltic nations, have repeatedly fallen victim to disinformation campaigns, as a way for the attackers to hopefully gain political influence both locally and abroad. For example, The Bronze Soldier, a monument to the Soviet Union erected in Tallinn, was moved, but Russian minority groups in Estonia spread news that the statue never existed or was "cut into pieces and taken to an unknown location," (McLaughlin, 2022).

Reliance on Russian-propagated media leaves Estonia, Lithuania, and Latvia vulnerable to disinformation campaigns as their Russian-speaking minorities in Russian-controlled media spread false information nationally and internationally (Cristopher, 2016). For instance, a popular Facebook group, Tallintsi, formed of pro-Kremlin or Russian-speaking members, posts references to supporting the invasion, such as referring to a Ukrainian town on the frontlines of the invasion, a "nest of fascists" (Duxbury, 2022). However, to combat these campaigns, Estonia was one of the first nations to establish a defense team, known as the Computer Emergency Response Team (Cyber Defense Project, 2020). Estonia's report on cyber defense consisted of organizational structures such as a cybercrime unit for police, crisis management, and a cyber diplomacy department to mitigate the effects of disinformation. Kremlin-based disinformation attacks range from media outlets operating under Russian influence by citing false claims that they are not involved in kinetic attacks that directly contradict independent media coverage, to political organizations planting propaganda in all forms of media. Their strategies have even been characterized as "the firehose of falsehood," for "high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fiction" (Paul & Matthews, 2016).

Disinformation campaigns continue to infiltrate and sabotage global news, government support, and public perspectives. The most prominent example in the present is the efforts by the Kremlin to spread disinformation and sow discord amongst countries supporting Ukraine to undermine the illegal Russian invasion. For example, a recent article posted on a non-reputable German news source website called News Front, claimed that "...Das Gebiet der Westukraine könnte an Polen gehen, wenn das Land die Schulden Kiews bei den USA begleicht…"[1] ["The region of western Ukraine could be given to Poland, if the country pays off Kiev's debts to the U.S."] (Kramert, 2023).

[1] German to English Translation: "The region of western Ukraine could be given to Poland, if the country pays off Kiev's debts to the U.S." (EUvsDisinfo, 2023)

Figure 3:
German to English Translation: “The region of western Ukraine could be given to Poland, if the country pays off Kiev’s debts to the U.S.” (EUvsDisinfo, 2023) https://de.news-front.info/2023/01/20/polen-kann-einen-teil-der-ukraine-von-den-usa-erhalten-allerdings-unter-einer-bedingung/

Russia has been known to use disinformation and propaganda prominently in their military strategy, but according to the director of research at the Social Media Lab at Toronto Metropolitan University, Anatoliy Gruzs, “the internet era has put those information operations on steroids" (Gruzd in Zabjek, 2023). This article discusses how there has been some success in Canada, when researchers found that “nearly half of Canadians believed to some extent the false claim that NATO [as an organization] had been surrounding Russia with more military bases since the end of the Cold War", and that most everyday Canadians are frequently exposed to “at least one persistent, false claim” supported by the Kremlin (Zabjek, 2023).

The Russian strategy is to “deny, deflect, and distract” as much as possible, using tools such as disinformation as the condemnation of their actions in Ukraine continues (Zabjek, 2023). Lies and disinformation were weaponized by governments wishing to undermine other government institutions and Russia has proven time and time again that the Kremlin will refuse to back down, despite condemnations from other international powers.

Disinformation is an increasingly dangerous weapon, as social media and the internet continues to skyrocket in popularity and is even more problematic in the hands of a government unafraid to use it advantageously.

As previously mentioned, disinformation campaigns and states that authorize such crusades are becoming ever more present threats in the global scene. Although disinformation is not new, the tactics that are being utilized to spread false news and claims have evolved over time alongside cyber developments.

Disinformation campaigns are not limited to social media or media platforms in general, as it can span across multiple mediums, including the implementation of cyber-attacks on government websites, to the point of espionage. These acts are a serious threat to not only cyber security, but also national security. Although some countries have the capability to recognize these efforts by foreign states for what these actions truly are, some states do not have the resources to counteract sophisticated disinformation. Therefore, as these disinformation campaigns evolve to become stronger and more harmful, the efforts to counteract these campaigns should respond in-kind.

Case Study of NATO Disinformation Response

Disinformation and propaganda remain a consistent threat in today's international affairs and are primary tactics in warfare. With the rise of social media, disinformation is being spread at a faster rate across a wider range. This frequent exposure reinforces false claims while providing a platform for authorities to manipulate information. From the 2014 Russian annexation of Crimea to its current war on Ukraine, the Kremlin has used intense disinformation campaigns to influence the public's perceptions of Ukraine and its allies, as well as the Russian agenda (OECD, 2022).

Who is Operating Disinformation Campaigns? Who is Being Targeted?

The majority of disinformation campaigns are launched by the Russian government with strategies that include fake accounts, anonymous websites, and manipulated official state media. The goals of these operations are to distribute and strengthen false narratives to benefit Russia while undermining competing governments. One of the most prevalent Russian disinformation campaigns that has been running since the Crimea annexation involves the painting of Ukrainians as neo-Nazi fascists. Referencing Nazism has "a certain resonance for Putin's core supporters in Russia" because the defeat of the Nazis during World War II has been a significant

accomplishment of Russian national identity (Tabarovsky in Farley, 2022). The Kremlin has also been known to target certain aspects of Ukrainian government and society that paint them all as dangerous or extremists as an attempt to justify the war (Farley, 2022).

With the increased alignment between Russia and China, these governments continue to amplify each other's disinformation through social media. Continuing with the neo-Nazi narrative, Chinese diplomats and media outlets have amplified Russian sources through retweets and citings of Russian state media discussing Ukrainian neo-Nazis (US State Brief, 2022). Prior to the war in Ukraine, this narrative was nonexistent in China's coverage, showing how the increased collaboration between Russia and China has brought specific disinformation campaigns to new regions. As these stories circulate, the EU and media platforms have taken some action against Russia by reducing their media outlets' abilities to reach wide audiences; however, Chinese media has provided Russia with an information pipeline that is being used to reach Russian and international organizations. (US State Brief, 2022).

As Russian propaganda is spread across the globe, it has a profound effect that is primarily targeted towards Ukraine while also influencing other countries, including Poland and Lithuania. Russia has attacked Ukraine directly with disinformation surrounding neo-Nazism and the narrative that Ukrainian leadership is corrupt and the government has abandoned their frontline forces during the war, provoking backlash and social unrest as the public loses their loyalty and trust in their government (Haines, 2015).

By targeting Poland, Russia has been spreading disinformation as a way to worsen the relationship between Poland and Ukraine. As the first country to recognize Ukrainian independence, Poland has been shown to be a strong advocate for Ukrainian membership in both the EU and NATO, which would officially provide security from Russia (Mick, 2022). As an attempt to weaken this alliance, Russia has begun spreading the claim that Poland is preparing to annex parts of western Ukraine (Kuvaldin, 2022). This narrative is dangerous in that it antagonizes Poland and Ukraine, undermines trust towards Poland, and destabilizes these relations. At the same time, it weakens Poland's security and isolates them internationally with lies (Żaryn, 2022).

Figure 4: https://emerging-europe.com/voices/russias-operation-against-poland-and-nato/

In Lithuania, *Russkaya Litva* (Russian Lithuania) spread a video of the Russian Foreign Minister describing how Ukraine was violating rights of Russian speakers, as well as aiming to gain support of the Russian populations in Lithuania and the other Baltic nations. There is also a large emphasis from Russian media on the narrative that Ukrainians are "taking over Lithuanian jobs" and benefitting from opportunities that Lithuanians cannot access, and they use this as a means to discourage Lithuanian support for Ukraine (Gajek, et al., 2022). As technology and social media become more available, Russian disinformation is spread around the world at a faster rate than ever before, specifically targeting countries that they see as a threat, including Poland, due to these countries' close relationship with Ukraine and Lithuania's Russian-speaking population.

As disinformation becomes a larger threat with developing and emerging technology and media, especially campaigns originating from Russian sources, it's important to recognize how disinformation is spread and who is being targeted or affected.

What are the Recommendations for Combatting Disinformation? How Can They Work?

To combat disinformation campaigns, a Rapid Response Team should be created as a way to execute Confidence Building Mechanisms to ensure the proper and efficient functioning of disinformation countermeasures, and improving regulations on media publication platforms.

Rapid Response Team (RRT)

RRTs are still a developing strategy, which gives NATO the unique opportunity to shape such resources in a time of extreme disinformation. Therefore, the RRT should be housed as a part of NATO, while simultaneously developing collaborative partnerships with outside entities, such as grassroot organizations and local NGOs. NATO's Partnerships and Cooperative Security Committee could be a key actor in implementing a Rapid Response Team to educate the public, as well as build trust.

Countering disinformation requires confidence building mechanisms, education, and a Rapid Response Team (RRT). NATO's Partnerships and Cooperative Security Committee (PCSC), which handles NATO relations with other international organizations, would be an area within NATO in which the RRT would work. This team would also work with international and local grassroots organizations (e.g.: EUvsDisinfo Lab and Reboot Foundation) in which the RRT will assign an ambassador or liaisons to work alongside these organizations to promote educational initiatives within schools and universities, as well as for the labor force and civil society (NATO, 2023).

NATO currently cooperates with other international allies, consulting and partnering with actors that have interoperability in various fields as a means to support NATO-led operations, improve stability, and strengthen security (NATO, 2022). By having the RRT as a part of NATO, it would enable a larger reach across the allied nations, strengthening the reputation of NATO as an irrefutable counteragency to disinformation. This would result in more support from governments, NGOs, and the general public. For example, the EU DisinfoLab in Belgium works in researching and sharing disinformation while organizing outreach activities, while the News Literacy Project in the United States works to expand disinformation literacy, and lastly the Reboot Foundation in France cultivates critical thinking capabilities for students and caregivers (EU DisinfoLab, 2023; The News Literacy Project, 2023; Reboot Foundation, 2023; Lans, 2021). Some nations, such as Poland, are assembling teams and education campaigns to raise

awareness and defenses against disinformation (Polish Press Agency, 2022). To maximize communication between the RRT and the allied entities, it's essential for NATO to develop a Disinformation Communications Team (DCT) to specialize in collaboration with allies and the RRT.

Well established international organizations could provide resources, including educators, to be a part of this RRT and send these forces to areas of increased prominence or risk of disinformation campaigns. Further, by partnering with local organizations within these tailored countries and communities, trust and confidence can be established between civilians and their governments, as it would demonstrate the loyalty of smaller nonprofits with the dedication to provide people with facts and prevent people from obtaining false information from deceitful sources. Liaisons from outside organizations would correspond with NATO's RRT liaisons, the DCT, to report to the RRT for investigation and debunking. Once this process is complete, the RRT DCT will report to NATO and inform their partner organization about specific disinformation strategies that are being developed, used, and spread across the globe. This collaboration is essential in slowing down and preventing the spread of disinformation because it develops clear communication pathways and builds confidence in these partnerships.

An example system that works similarly to NGOs and Grassroots would be the Bulgarian-Romanian Observatory of Digital Media (BROD), which could work with the RRT to provide "locally adapted multilingual tools" that analyze disinformation campaigns with fact-checks through media and disinformation research (Ontotext, 2023). NATO member states Bulgaria and Romania, supported by GLOBSEC and the EU, are currently regional hubs that combat and detect disinformation. The BROD project aims to organize tools and multinational experts to analyze disinformation campaigns. BROD is distributed to journalists, media literacy providers, and policy partners, along with the "biggest fact checker worldwide", Agency France-Presse (Development Aid, 2023). This project aligns with the idea to base the RRT within NATO because the RRT can act as a hub for organizations in allied states, like BROD. It will be useful to follow similar protocols to BROD, such as having NATO RRT liaisons similar to BROD's policy partners that collaborate together, using professional researchers and the most efficient fact-checking tools at the time.

For the benefit of all parties, another suggestion would be developing a 'disinformation database' website put forth by NATO in collaboration with allied organizations, to assemble

finalized disinformation campaign reports. A central disinformation database could operate similarly to the EUvsDisinfo site, but as a NATO-led network that can be accessible over the worldwide web to all parties with internet access (EUvsDisinfo, 2023). The core components of this online portal would be the professional, peer-reviewed publications readily accessible to the public via internet, as well as a self-reporting function for journalistic reporting, local media, and the general public.

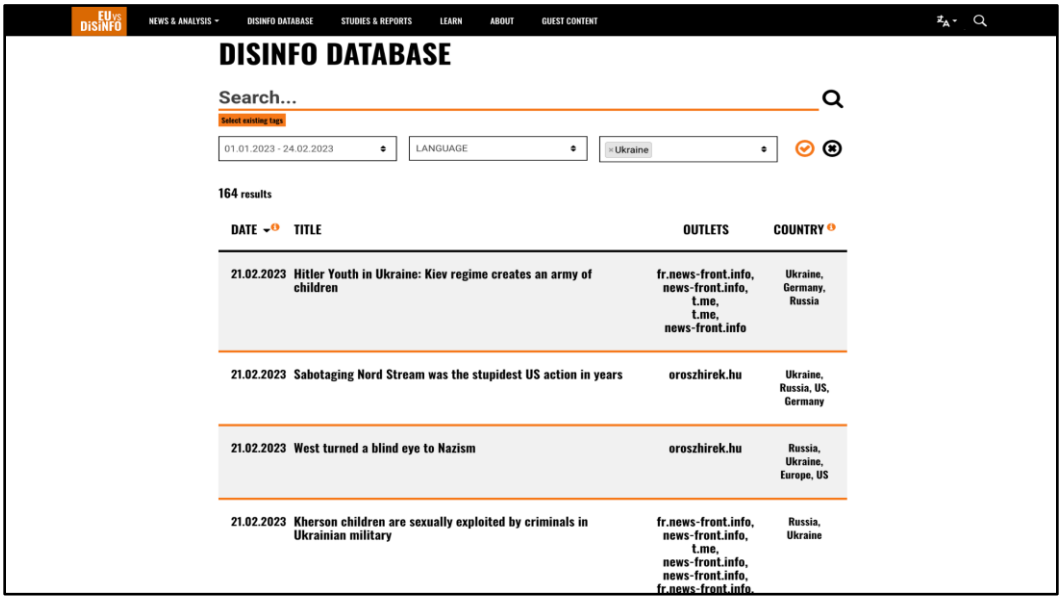

Figure 5: EUvsDisinfo's Disinformation Database; https://euvsdisinfo.eu/disinformation-cases/?text=&date=01.01.2023%20-%2024.02.2023&disinfo_countries%5B%5D=77547

Germany's Institute for Strategic Dialogue (ISD) is an organization that counters extremism through intergovernmental initiatives. Germany has created a response to internet-based attacks on information through the Online Civil Courage Initiative (OCCI). The OCCI is a non-governmental strategy partnered with the ISD and Facebook to "mount a Europe-wide proportional response to hate, violence, and terrorism online," (Institute for Strategic Dialogue, 2023). Although the OCCI is not directly targeting political disinformation, the online presence, resources, and research are practices that can be emulated by the RRT in their collaborations with NGOs, as well as how the RRT interacts online and provides advice for disinformation. Germany is already creating media-based strategies to combat disinformation, therefore this initiative could be not only an indicator that ISD would be a great organization to pair with the RRT, but also in cultivating the necessary skills to combat disinformation via civil groups and existing online presences, such as Facebook.

Confidence Building Mechanisms (CBMs)

CBMs are created by developing partnerships between RRTs and entities like grassroots organizations and NGOs, as they have already created confidence and rapport within their local communities (Stevens, 2022, 4:32). Since the Russia-Ukraine war began, Ukraine has been steadfast in collaborating to develop anti-disinformation measures, such as Vox Ukraine, EUvsDisinformation, and ProPublica. If NATO collaborates with existing organizations and allies actively countering disinformation, there will be a stronger baseline of trust amongst the local population to collaborate in applying countermeasures against disinformation (EU DisinfoLab, 2022). For example, the EUDisinfoLab hosts conferences and projects such as *Crossover* and *The Many Faces Fighting Disinformation*, a prime opportunity for developing partnerships between NATO's RRT and newly founded NGOs from a wide variety of nations.

Another CBM is the expansion of education to train people in questioning, recognizing, and reporting disinformation. Within the EU, two thirds of the citizens are exposed to disinformation weekly (Council of Europe, 2023). Given this exposure, the public has the greatest ability to be disinformation trackers, but only if they are properly trained to expand their understanding of disinformation and develop stronger critical thinking skills.

Expanding education varies depending on circumstances, including accessibility to information and risk levels. To counteract these discrepancies, it is suggested to increase awareness of producers and participants in disinformation campaigns and develop critical thinking skills to encourage openly questioning news. Education can be implemented across multiple demographics, with labor workers, children, and everyday citizens, benefitting from such tools that work to make these groups more cognizant of disinformation.

Wire services are useful tools for remaining alert and aware of disinformation. Wire services, such as Reuters, Associated Press, and Anadoul Agency, are news agencies that send out syndicated news copies to subscribers by wire or satellite transmissions (Merriam-Webster, 2023). The EU's EDMO currently works as a hub for fact-checkers, academics, and other relevant stakeholders to coordinate and respond to disinformation operations, developing transnational collaboration that supports training and accountability measures for media organizations (European Commission, 2023).

Many wire services are located in Western NATO states, but these are expensive for Ukraine and other Eastern European countries to access. Instead, they have cheaper access to wire services and news that are provided or dependent on Russian media, such as TASS (Tani, 2022; Russian News Agency, 2023). As such, the expansion of accessibility to diverse and reliable wire services for allied countries is recommended - particularly for allies in the East, who are most exposed to Russian-biased media.

Media Recommendations

Media recommendations fall in two primary categories: Social media monitoring and stricter criteria for journalism and news reporting.

The difficulty with most media recommendations is the concern regarding infringing on the freedom of speech, but this is why social media should be monitored properly to filter specific trending subjects such as elections and major conflicts.

Some options for moderating social media would include filters alongside "Disinformation Penalties." In 2017, Facebook announced their partnership with four independent fact-checking organizations, *Snopes, Politifact, ABC News, and FactCheck.org*, and all four members are part of the Poynter International Fact Checking Network (Roberts, 2017). These filters would not hinder speech, but rather monitor posts and articles while using banners to mark for disputed disinformation. With the COVID-19 pandemic, social media platforms including Twitter and Instagram have implemented these filters which tag keywords to flag misinformation on the virus and vaccine alike. Since 2015, as well as in response to the Ukraine conflict, a handful of keywords have been: Ukrainian Statehood, Russophobia, NATO, Nazi, Syrian War, Alexei Navalny, Disinformation, and many more (European Union, 2021; EUvsDisinfo, 2023). The largest issue with this partnership is that it only helps users to recognize disinformation when it passes through their feed, with no further action taken.

The Alliance for Securing Democracy's Hamilton 68 dashboard was established to help ordinary people and journalists detect Russian messaging themes and detect active disinformation campaigns. By monitoring the activity of 600 Twitter accounts that have clear connections to Russian influence, this dashboard focuses on providing insight on the workings of Russian propaganda and other online disinformation campaigns through three types of networks: those derived from openly pro-Russian users, those derived from users tweeting as part of disinformation campaign that is linked to Russian media, and a network of accounts that use bots

- or automated behavior - on behalf of accounts to reflect Russian messages (Berger, 2017). By exposing the public to common themes and disinformation tactics, consumers of information will become more resilient to disinformation, thus reducing Russia's international influence while deterring future campaigns, as countries that use disinformation will be less inclined to use these tactics as they become less effective (Berger & Rosenberger, 2017). By using programs such as the Hamilton 68 dashboard and creating more programs that track disinformation campaigns, more people around the world will be able to easily identify and combat disinformation in the future.

Nevertheless, there are a number of cases in which media platforms or profiles were held accountable through fines and account bans. In 2014, Latvia fined First Baltic Channel (PBK) three times for airing news that included fake and biased information broadcasted from Russian media, fining them again in 2015 (Sarlo, 2017). In 2021, Donald Trump was banned from Twitter and other platforms due to him spreading disinformation campaigns to overturn the election and incite violence (Twitter Inc., 2021).

This raises the concern in the realm of journalism and reporting credentials. The existing credentials for media publications need improvement to enact stricter criteria for what can be considered 'journalism.' Since disinformation should be considered a national security threat, it's important that expectations are high. After all, if anyone can quote a tweet in their report and call it 'journalism,' this poses a multitude of problems for what constitutes licensed journalism or 'official reports.'

When Could these Recommendations Be Implemented?

Ideally, the aforementioned recommendations surrounding disinformation would be applied immediately and regularly maintained, however, such practice is unrealistic. Each previously highlighted policy and recommendation plays an important role in combating disinformation campaigns and can be enforced at various times.

A critical policy recommendation is the application of CBMs. These mechanisms should be used immediately after being formed, with these policies having preventative measures toward future disinformation campaigns. These community-based groups are vital to fighting against disinformation due to the closeness with the public. Many grassroots and civil society organizations are close to those most vulnerable to disinformation and by working within such communities, these groups gain the ability to build both trust and credibility (Sienicka, 2022). By

building trust with the public through these civil society organizations, the work of recognizing disinformation and promoting digital resilience will become not only more effective, but also capable of reaching a wider audience.

Although a major part of CBMs is establishing relationships through trusted institutions, the education of the public and those experiencing disinformation campaigns is also critical. Digital literacy is a must, especially within countries such as Ukraine, Poland, and the Baltic States who have experienced an increased number of disinformation attacks. By funding digital literacy, programs can be created that are tailored to different audiences, including children, journalists, labor workers, and the public. An organization that currently promotes digital literacy is TechSoup, an international nonprofit network stationed throughout Europe, that provides technical support and tools to other nonprofits (TechSoup, 2022). One way this group works to combat disinformation is through Hive Mind, a digital platform which gathers individuals ranging from activists to teachers and university students, all simultaneously working to improve digital and media literacy, including how to combat disinformation. Similar media literacy campaigns have been taken by Ukraine following the annexation of Crimea. Today, Ukraine has a strong civil society landscape with organizations responding to disinformation, monitoring and debunking activities and even producing research (OECD, 2022, p. 13). Although this policy of implementing confidence building mechanisms may appear daunting at first, once executed, such practices will actively work against disinformation and continuously benefit the general public and especially vulnerable nations.

Another policy recommendation is the introduction of a RRT by NATO. The enforcement of this policy should occur following a disinformation campaign against a member state of NATO. Currently, in a similar fashion to their media literacy efforts, Ukraine established the Centre on Countering Disinformation (CCD) which analyzes informational threats to Ukraine's national security (OECD, 2022, p. 14). The RRTs should be utilized following a disinformation operation, but must also work to introduce preventative measures that make disinformation campaigns less successful.

Although RRTs within NATO and the implementation and creation of CBMs are important, another beneficial new policy is the application of more media communications management. This supervision of media communications should become standard practice and can be accomplished by everyday actors, such as within Lithuania. The Baltic States are

extremely familiar with fake news, primarily Russian tactics of disinformation. A case of the public monitoring media communications is with Lithuania's 'Elves'. This large, informal internet community is made up of citizens who for almost a decade have worked against Russian disinformation in Lithuanian media, tackling issues ranging from COVID-19 to the war in Ukraine (Abend, 2022). As demonstrated by the 'Elves', it is possible for nations to work to combat misinformation through citizens volunteering to monitor media platforms. This is a necessary practice that must be implemented on an everyday basis regardless of if a widespread disinformation campaign has taken place or not.

Targeted disinformation efforts are not everyday occurrences, however, the highlighted policy recommendations must be executed and employed by states regularly to combat fake news, educate the public, and apply technologies to counter disinformation.

Where Would these Recommendations be Implemented?

Within NATO itself, these recommendations can be effectively used because each of the options has its own unique role and utility. In a NATO interview, Baiba Braže, NATO's Assistant Secretary General for Public Diplomacy, addressed the issue of combatting disinformation and how they respond to disinformation. Regarding their approach, Braže says, "…[it] involves understanding the information environment, engaging with audiences, communicating proactively and exposing major cases of disinformation." (Braže, 2021) This describes the key objective and core attributes of the RRT .

NATO has a large presence online, in which the official NATO Instagram account is verified, having over 1 million followers. By recognizing and spotlighting false information and sharing fact-checking reports, this online influence can feed directly into NATO's ability to help with the social media regulations previously recommended. Braže stated that, "NATO is committed to transparent and honest communication and to countering disinformation," which supports how NATO would be an excellent location for these newly founded confidence building mechanisms to take root (Braže, 2021). Not only would the RRT work with grassroots organizations, but by proxy, NATO would as well. This will help foster trust between all parties, and since NATO would be the most influential organization involved in the implementation of each of these recommendations, it makes sense to have them involved with each solution across varying capacities.

Many successful disinformation campaigns begin at the local level, which is why some recommendations are suitable for implementation in everyday life. For example, Instagram already has a fact-checking mechanism built into its interface, but the main issue is its entirely user-controlled. A BBC article by Shayan Sardarizadeh explains how the process allows, "…Instagram users to flag posts they think contain fake news to its fact-checking partners for verification," which essentially enables the general public themselves to combat disinformation (Sardarizadeh, 2019).

It is essential that populations working in CEI careers have access to multiple media platforms and resources. For the CEI workers living in rural communities, it's important to expand access to these resources, as they are particularly vulnerable to disinformation and it is difficult to facilitate outreach programs to these rural areas. One proposition is to extend disinformation initiatives to the CEI working communities, especially groups in vulnerable sectors, including coal and energy, through the spreading of disinformation education with incentives. Initiatives like this would require working with organizations such as the German Marshall Fund's Hamilton 2.0 Dashboard, which displays and reports on disinformation from accounts monitored over multiple mass media outlets, and the Carnegie Endowment for International Peace (CEIP), an organization that works alongside the EU and the Hague Program to create disinformation counter-initiatives ("Hamilton 2.0 Dashboard", 2023; Vériter, 2021). The partnership between the CEIP and the EU works in many areas to increase the digital proficiency of the public that helps them to critically evaluate disinformation. Sweden assigned their Committee on National Investment in Media and Information Literacy to work with the public to increase their resilience to counter disinformation and cyber hate (Vériter, 2021).

The EEAS Strategic Communication Division and its Task Forces (STRAT.2) currently exist with the objectives of "strengthen(ing) the EU's situational awareness" and improving the public's overall capacity to address - and counter - disinformation campaigns (European Union, 2021). STRAT.2 has partnered with Information Analysis teams and Task Forces to work on issues spanning across multiple regions, employing policies and strategies to further implement the European Democracy Action Plan. One particular development out of STRAT.2 was the creation of the Policy, Strategy, and Global Priority Issues Team (PSG), which currently helps coordinate the cooperation between the EU and international partners and managing the EU's Rapid Alert System (RAS) that fosters cooperation between EU Institutions and EU member

states in responding to threats. The EEAS's Stratcom closely cooperates with international partners including NATO, the G7 Rapid Response Mechanism (RRM) and three central Task Forces. The East Stratcom Task Force (ESTF) runs the EUvsDisinfo website, the Western Balkan Task Force (WBTF) works to expand traditional information channels through public campaigns and strategic partnerships, and the Task Force South (TFS) promotes EU action in MENA regions to develop anti-disinformation response campaigns (European Union, 2021).

If NATO collaborates further with the EEAS, there will be an abundance of resources to emulate, experiences that NATO can learn from, and potential partnerships that could help build confidence; the EEAS's PSG will be particularly helpful in outlining the capabilities and functions of the NATO RRT's Disinformation Communication Team (DCT) that was previously recommended (European Union, 2021).

Figure 6: The Division Structure of STRAT.2; https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication_en

These are especially important in the digital age, when diverse disinformation networks can lead to impacting more specialized communities, such as critical infrastructure workers. The study, *Disinformations threat to Canadian Critical Infrastructure* by Marianne Grenier mentions the 'risk society theory', in which modern industrial societies pose more risks than benefits. Risk society theory can be applied to the attacks on Ukraine's critical infrastructure, such as claims

that the U.S. was funding secret bioweapon facilities in Ukraine, which spread far enough to be broadcast on Fox News (Ling, 2022). The reality of this story is that these were scientific labs for studying medicine, but changing algorithms and platforms amplified the disinformation through facilitated biases and political trends. Due to this, online sharing platforms are included as a risk due to the relative ease of spreading false information to people working critical infrastructure jobs. The disinformation campaign on bioweapons was a result of the feedback loop between social media and other media outlets. Social media originated the conspiracy on bioweapons, while other media outlets continued to circulate the disinformation.

Many anti-disinformation resources can be distributed through 'disinformation awareness' seminars, which can be promoted via incentives and compensation. Although incentivizing such groups to spread awareness regarding disinformation is not a long-term solution, in the short-term it would motivate CEI employers to hold seminars, while incentivizing workers to participate in these disinformation forums. Workers who attend are paid overtime or compensated for their attendance. If the budget allows, each member of working age in a CEI worker's household could also qualify to receive compensation, through government funding, for attending these seminars. This would further spread these disinformation initiatives to rural communities, while also providing financial benefits to help CEI workers and their communities.

In relation to stopping disinformation, an aspect of the online realm worth noting is the presence of online websites such as EUvsDisinfo, which was established to "…better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns…" (EUvsDisinfo, 2015). This type of website is yet another resource available to the general public to learn about and discover sources of disinformation, and in becoming educated on how to spot false news as they read or hear it. Having these sorts of filtration and education systems available at the civilian level is incredibly important in the fight against disinformation campaigns. Since news spreads fast, from family to friends to community members, it is vital to recognize fake news and disinformation before it can spread.

Another important aspect for CBMs is accountability agreements between NATO countries and news wire services. One of the most popular and reliable wire services that countries like the U.S. have access to is the Associated Press (AP). However, this service is expensive to Eastern European nations. So many of NATO's poorer member states cannot afford

the costs to get news from AP and instead turn to alternative options like Reuters, a wire service that has an ongoing partnership with Tass, a Russian state-controlled media organization. An article from Politico discusses the issues with relying on Tass due to its unreliable nature, especially in light of the invasion of Ukraine, with author Max Tani writing that Tass was reported to have "…parroted Russia government claims that Ukrainians killed civilians in the Donbas region and dumped their bodies into mass graves…" (Tani, 2022).

Figure 7: Concerns over reliance on Russian TASS: https://www.politico.com/news/2022/03/20/reuters-staff-partnership-russian-wire-service-00018779

Stopping the spread of disinformation is impossible when the only news option for some countries is involved with sources known to be Pro-Kremlin. As such, all wire services and NATO should reach an agreement in which they are accountable for reporting on verifiable stories, to better protect nations where they do not have as many objective media outlets. Given the legal boundaries surrounding NATO and media organizations, accountability agreements would work to provide some level of liability for the spreading of false information.

In order to expand the accessibility of reliable information, a recommendation is to work alongside the EU to expand the number of wire service providers. Currently, Anadolu Agency in Turkey is the only substantial wire service located in Eastern Europe; the EU is working to transition further into the digital age, and part of this work could be the expansion of wire services due to the accessibility to technology that could help shield democracy from disinformation (European Commission, 2020). The proposed expansion of wire services could attempt to work with the EU's EDMO, a group already focusing their efforts on training people

to combat disinformation, or the East Stratcom Task Force (ESTF), a group that provides disinformation awareness platforms like EUvsDisinfo. These services have already started working to expand accessibility to disinformation counter-intelligence, which puts them in a unique position to help NATO broaden the availability of wire services.

Why Recommend these Disinformation Responses?

The impact that fake news and disinformation has on wars and government altercations are long withstanding, yet the Russian invasion of Ukraine heightened this influence dramatically. An interview from NPR highlights just how important it is to stop disinformation, with guest journalist Emily Dreyfuss explaining how, "…social science studies have shown that the more a person hears something or is exposed to something, the more true it sounds…in a disinformation ecosystem, it is really dangerous" (Garcia-Navarro, 2020). In the case of the Kremlin and their disinformation campaigns, their tactic is to spread as much disinformation so large populations hear it more frequently, either to misdirect, mislead, or overwhelm the receiver of disinformation (Stevens, 2022, 2:09). Regarding disinformation campaigns, it's important to consider where to implement recommendations so biased media sources cannot consistently flood people's social media feeds with false information. With the right tools and policies, the general public can remain well informed, defeat these campaigns, and maintain social stability.

Media platforms, articles published by journalists, and news outlets are the constituents of disinformation and are widely available to the general public, making them more susceptible to propaganda and disinformation. Preventing disinformation can be difficult due to the accessibility of reliable information. A RRT that works jointly with NGOs located within targeted countries, paired with a NATO communication team and a website with a central portal for peer reviewing information, all function as a system to prevent and act more efficiently on potential disinformation threats. The evaluation by RRT members acts as a filtering system without directly restricting resources and building an accessible space for those viewing the information provided.

It is vital for the RRT to have an internet presence. The RRT website acts as a safe format that reviews social media, blogs, and other forms of mass media platforms without directly affecting the democracy of media. For instance, Russia's Internet Research Agency's activity peaked on social media platforms such as Facebook and Instagram purposefully near key political dates such as presidential election days (Howard, 2023). A curated website that is a

repository for information tracked by the RRT forms a reliable hub of news media available to the general public. Providing media consultants with objective news, will ensure they are not affected by the lack of accessibility for trustworthy information. Russian independent media is under significant government pressure to limit coverage on sensitive topics and "prompting widespread self-censorship."(Corker, 2017). Reporters and journalists are easy targets for pro-Russian fueled propaganda, because they rely heavily on Russian news outlets as their sources for relaying information to media outlets.

To ensure the growth of trust, the NGOs and grassroots organizations located in each country are to connect the local citizens with a more familiar government institution. This results in an internal connection to an international issue. Built-in confidence mechanisms allow all parties involved in policy making and those affected by these policies to feel more confident in the organization's abilities.

The general public is not equipped with the skills to evaluate their sources of information to access media that is free of disinformation. Providing means for media literacy and a filter system for widespread media acts as a prevention method for spreading disinformation, in order to stop it before it becomes an international issue. Given the concerns from the general public on the infringement of rights, pushing for social media regulations is not easily enforceable. However, filtering systems and tracking more credible outlets for internet sources are theoretical foundations for the spread of accurate information. Social media is the most used origin of modern news and information. Over half the world's population uses social media for an average of 2.5 hours. Not only that, but 76% of U.S. citizens use social media to access news (Pew Research Center, 2021).

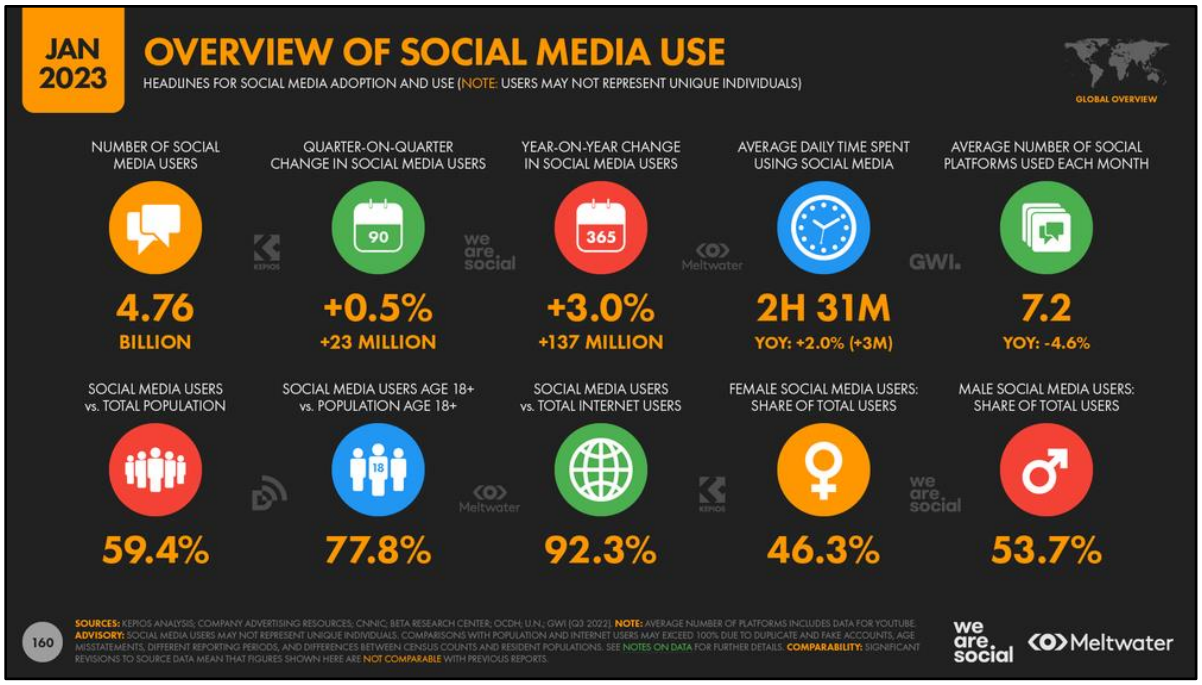

Figure 8: Overview of statistics on social media use; http://www.datareportal.com

Educational services on the risks of disinformation, and the vulnerabilities media poses to the general public, is another method to combat the spread of disinformation at its source. This includes vulnerabilities such as false information spread by Russian-speaking populations as seen in many of Russia's neighboring countries, or misinformation spread through common social media outlets where users have no previous knowledge that the information is false. Educating the general public, schools, teachers, and media consultants will set up a more reliable and trustworthy system of information sharing.

Conclusion

Countering disinformation as modern society faces it today is only possible with multistep processes such as the Rapid Response Team, Confidence Building Mechanisms, and Tighter Media Regulations. Organizing such a system will not be without challenges. Reliable contracts would have to be implemented in order to work between NATO and the local NGOs in the allied countries. There would have to be a training process and resources for the setup of an RRT website that is fully secured. The CBMs would need to be implemented effectively, starting with education days in schools, businesses, and communities. In order to be efficient, discussions with wire services are recommended with outlines on how such amenities can be more affordable and accessible to as many countries as possible, primarily those in the East. Monitoring social media and filtering news presents the greatest challenge due to an obvious potential influence on

free speech and press in multiple countries. It is important to note that the right to free speech and press should not be impeded through this recommendation; instead, these rights will be protected by filtering out false information. While implementing these recommendations will certainly prove difficult, it is necessary in order to better protect countries from the widespread impacts of disinformation. Hybrid warfare will only continue to become a more strategic and complex form of international conflicts. Let Russia's invasion of Ukraine be an example for NATO allied countries to build defenses that will combat disinformation and other forms of hybrid warfare in the future. After all, perseverance in the face of adversity is the hallmark of overcoming hardship and deceptive influence.

Final Recommendations for Combating Disinformation within NATO and allied States

Disinformation is becoming increasingly problematic for undermining democracy, international and national security, and trust in government functions and capabilities individually and as a collective. As an international alliance of states, the continued use of disinformation undermines NATO's abilities to function by targeting public opinion, critical infrastructure, and creating various issues for NATO states and its allies, such as the example with Ukraine.

Eliminating disinformation altogether is impossible due to its continuous adaptation to emerging technology, particularly within the context of hybrid warfare where the campaigns target a nation's critical infrastructure; this development has expanded the influence of disinformation on the public's opinion, which consistently causes harm to communities by undermining the stability of state sovereignty and national security.

Russia has utilized disinformation campaigns against their adversaries as early as the 1950s when the Soviet KGB started implementing them against the United States; after the conflict in Ukraine began, the use of disinformation as a method of hybrid warfare increased dramatically (Bittman, 1985, p. 1-2). On February 21st, 2023, the EUvsDisinfo database cataloged and disproved a total of six different disinformation campaigns that targeted Ukraine, Germany, United States, and the West as a collective (DISINFO Database, 2023).

Education on this subject is a significant factor in countering disinformation because disinformation explicitly targets the public - especially people without the skills to identify disinformation. In July 2022, EU Parliament released statistics in which 64% of respondents

were ‘somewhat or very confident’ they could identify disinformation, while only 28% of respondents had admitted to possible exposure to disinformation - respondents from Netherlands reported at 12% and Bulgaria reported at 55% (European Parliament Press Releases, 2022).

Half of EU citizens between the ages of 15-30 admitted to needing “critical thinking and information skills to help them combat fake news and extremism,” showing an awareness amongst the public of this educational gap; this gap in disinformation awareness can be partially attributed to a lack in educational outreach on the subject, as well as limited accessibility to reliable news and delays in implementing countermeasures (Council of Europe, 2023). This delay in responding to disinformation as a security threat since its first application in the 1950s has allowed Russia to continuously deploy disinformation campaigns against allies such as Lithuania, Italy, and Poland, amongst other affiliates (Kuzminski in Lohmann, 2022, p. 163; Elmore in Lohmann, 2022, p. 215; Padigepati in Lohmann, 2022, p. 249).

Some recommendations can be implemented as standalone processes. However, all recommendations require a rapid implementation due to the damage that delayed reactions have already had on national security and confidence in government functions - especially if countermeasures are further postponed.

Section 3: Cyber Attacks

Executive Summary

Lastly, as the world rapidly modernizes and technology advances, so do the means in which states participate in hybrid warfare. The hybrid warfare setting, wherein states are able to attack other states through conventional kinetic means and also within the cyber realm, has become more commonplace in conflicts between states. This multifaceted strategy will continue to shape the way we view warfare and the way in which nations partake in it as well. Building up to the beginning of the invasion of Ukraine that first took place in February of 2022, NATO members and states sympathetic towards Ukraine, have been threatened with malicious cyber attacks. A year later, these attacks have only increased since the beginning of the invasion, which has many repercussions for states and their critical infrastructure. Organizations in healthcare, maritime, transportation, government, and communications sectors are key targets for cyber attacks in the current climate. In many sectors, cyber security has been lacking or even nonexistent and data pipeline vulnerabilities, a lack of cyber attack reporting, and hacktivism are some notable issues that have arisen in NATO countries.

The proposed recommendations outlined attempt to mitigate a few key issues explored in multiple recent case studies since the beginning of the war. This includes education and work certifications for companies involved in critical infrastructure, mandates of concern to Cyber Early Warning Systems (CEWS), and malicious cyber intrusion reporting of concern to critical infrastructure. These recommendations, again, attempt to target the issues of a lack of basic cyber security, preparing companies for these malicious cyber intrusions, and under-reporting of malicious cyber intrusions between companies—especially those involved in critical infrastructure— and governments.

The proposals could be further developed by NATO groups or NATO and EU partner groups such as the Hybrid CoE to then be proposed to NATO for unanimous decision making. NATO could collaborate with the EU to develop a viable application for states to further implementation. Such policies could coincide with the ongoing revisions and proposals for EU cyber security, including the EU Cyber Resilience Act and organizations such as ENISA. Cooperation to increase cyber security would be beneficial, as cyber attacks and cyber security are a paramount concern to EU and NATO member states due to the ongoing Ukrainian conflict. Promoting an ever-stronger union and cooperation between NATO and the EU during the current looming crisis could bring a more secure community when facing the current threat from Russia.

Hybrid Threat: How are Cyber-Attacks Affecting NATO's Critical Infrastructure and Why Does it Matter?

In the context of the Russian-Ukrainian War, vulnerabilities of critical infrastructure industries security have been increasing. Since the beginning of the war, we have seen Russia's aggression through malicious cyber attacks on critical infrastructure, not only towards Ukraine but also towards NATO member states, which is a threat that is projected to grow as the war continues (NATO, 2022). These malicious attacks exert enormous pressure on NATO states and present a danger to societal functions and people's lives. Since the war in Ukraine, the EU has been facing an energy crisis that is not only affected by Russian dependency but also threatened by Russia's cyber aggression. It is not only a concern for the EU and its constituents but also a concern of the people (European Commission Eurobarometer, 2022). However, other sectors of critical infrastructure are also a major concern. The prevailing discourse of concern to affected critical infrastructure has mainly been dominated by the issue of energy, with incidents like

NotPetya and the Colonial Pipeline propelling energy security concerns (Lohmann et al., 2022). However, other sectors, particularly maritime, healthcare, communication, transportation, and government operations, all of which are vital to the operation of society and a state, are also deeply vulnerable and often overlooked.

Maritime Sector

One of the main concerns in cybersecurity is the global maritime infrastructure. Today, this significant sector relies on digitalization, operational integration, and automation. Most shipbuilding companies are looking to innovate. Thus, they produce ships with various capabilities, such as advanced remote control, communication, and connectivity. However, this brought new challenges, including cyber attacks that target digital services. Consequently, the lack of a proper cybersecurity framework leads to disruptions in operations, financial and environmental damages. In the last decade, there have been several cybercrime cases reported in the maritime industry in NATO states. Yet, many of them remain unknown because shipbuilding companies are reluctant to share these cases to protect their reputation in the world market.

The operational technology (OT) systems in most modern ships are vulnerable and do not have the proper security measures because these essential systems are thought to be less crucial to ships' performance (Akpan, 2022). These vulnerabilities are found in the Automatic Identification System (AIS), Global Positioning System (GPS), Global Navigation Satellite System (GNSS), Industrial Control Systems (ICS), and IT Network Systems (Akpan, 2022). One of the main concerns is that many of these systems lack authentication, encryption, and verification of personal information; some IT systems run on computers with no security updates. In addition, AIS data are available to the public via the Vessel Finder Limited and Maritime Traffic websites (Akpan, 2022). Through these vulnerabilities, hackers can send false signals to disable various systems.

Case Studies: France, Greece, and the United States

There have been numerous attacks in the last decade. In March 2020, the port of Marseilles in southern France was affected by the "Mespinoza/Pysa" ransomware. As a result, the maritime infrastructure was impacted by this attack because of its correlation with information systems (Nicaise, 2022). In 2021, several Greek shipping companies were targeted by a ransomware attack that spread via the methods of an IT consulting firm (“Cyberattack Hits Multiple Greek Shipping Firms,” 2021). In this regard, the United States is no exception. In

2019, malware disrupted the onboard computer system of a ship bound for the Port of New York (Winder, 2019). This proved a vulnerability in a system that is utilized to update electronic charts, manage cargo data, and communicate with shore-side structures.

These cases display that the NATO shipping infrastructure is under significant threat from cyberattacks. These attacks can exert pressure on supply chains. Therefore, shipbuilding companies must prioritize not only the efficiency of their crafts but also focus their attention on cybersecurity.

Healthcare Sector

The healthcare infrastructure systems are currently receiving attention in the midst of the pandemic and the Russian-Ukrainian War. Attacks in this sector have taken place within Europe and the United States' healthcare infrastructure through ransomware. Within the year of 2022, it calculated a total of 127 major incidents impacting the sectors of medical manufacturing and development, and patient care services throughout 32 nations, which are heavily centered in the United States and Europe (CyberPeace Institute, 2022). These have become frequent in the United States in particular. In 2022, CommonSpirit Health, one of the largest health systems in the United States, experienced an attack on patient's personal data and medical records that impacted patient care within the affected hospitals (Miller, 2022).

What these incidents portray is how cyber attacks can impact a nation's safety through the supply chain or connections within systems, and these "attacks can occur at any point of the supply chain" (HIPAA Journal, 2021). Pertaining to NATO, addressing cyber attacks on the health sector of the alliance are crucial in considering the number of incidents, and the impact a more intentional attack could have on a state's infrastructure and wellbeing of its people.

Case Study: Ransomware Attack in a Hospital in Düsseldorf, Germany

A particular case that highlights these concerns occurred in September of 2020. A ransomware attack encrypting data and requesting payment targeted a hospital in Düsseldorf, Germany (Ralston, 2020). The direct and most alarming effect was an ambulance being diverted to a different location than planned, and a patient dying due to delayed medical assistance. The additional aftermath that occurred was a disruption in the hospital's digital infrastructure in communication with doctors and services, causing cancellations of numerous operations and cutting down on the number of patients treated (Ralston, 2020).

The attack is suspected to have been misdirected and was intended for Heinrich Heine University, which is linked directly with the hospital (Ralston, 2020). Even with this possibility, the vulnerabilities that existed within hospital systems and the interconnection between systems and lack of transparency between actors are of concern. This is particularly important because the suspects have links to Russian groups. This emphasizes the need for international cooperation and transparency between organizations being crucial in order to address this (ENISA, 2022).

Communications Sector

The critical infrastructure sector of communications has been dramatically affected by the current Russo-Ukrainian War, with effects spreading across NATO and even the globe. In particular, cyber attacks have been increasingly used to dismantle different facets of the crucial communication sector. The communication sector is vital to our modern societies, and when access is lost, the effects are long-lasting and widespread. This idea is further propagated by the U.S. Cybersecurity and Infrastructure Sector Agency (CISA), which outlines that the communications sector underlies “the operations of all businesses, public safety organizations, and government” (“Critical Infrastructure Sectors”, 2020).

Case Study: Viasat Satellite Hack

In February 2022, Russia invaded Ukraine. Moreover, many cyber attacks occurred concurrently with the invasion. One of the facets of hybrid warfare by Russia in the recent invasion of Ukraine was the cyber attack on a major satellite, which is owned by the U.S. company Viasat. The attack was a disastrous wiper malware named AcidRain which was implanted in customers' residential modems and quickly infiltrated their main control system, erasing everything on the satellite’s system (O'Neill, 2022). Furthermore, when customers tried to reboot their systems at home, they found that the malware had permanently disabled their modems (O'Neill, 2022). The satellite company Viasat estimated that “tens of thousands of people "lost access to their internet and phone services immediately following the attack” (Burgess, 2022). Even months later, “thousands still remain offline in Europe" (Burgess, 2022). Moreover, the attack affected Ukraine’s military communications on the same day of the Russian invasion. Ukraine’s national cyber security agency, which is a part of the State Special Communications Service of Ukraine, commented on the attack just after it had occurred, stating that “it was a really huge loss in communications in the very beginning of war” (Burgess, 2022). This attack teaches an important lesson in cyber security, that the complex systems of the

internet of things and flows of data are important to defend. As in the Viasat hack, attackers infiltrated the system through modems in people's homes, rather than hacking directly into the main system itself. This shows the importance of protecting all points across data pipelines, as attacks and infiltration can occur at any point in the complex flow of data. As the Viasat attack demonstrated, there are numerous ways to disrupt NATO communications, and if communications are disrupted, the consequences can be far-reaching.

Government Operations

From the beginning of the Russian-Ukrainian war, Russia has deployed cyber warfare tactics through government and private actors to achieve its military and political goals. A recent report by Microsoft Digital Defense shows that 90 percent of Russia's cyber attacks detected over the past year targeted NATO member countries, primarily in the IT, think tanks, nongovernmental organizations, and government sectors, suggesting a strategy of pursuing multiple means of initial access to these targets (Microsoft, 2022). Another report from Trustwave claims that known threat organizations from the Russian Federation Security Service (FSB), the Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff of the Armed Forces (GRU) are responsible for the majority of attacks on Ukraine's critical industrial infrastructure and data networks (Nichols, 2022). Through these government supported cyber attacks, there are three categories: disrupting the normal operation of critical infrastructure, installing destructive malware on essential networks (including phishing, denial of service, taking advantage of software vulnerabilities), and focusing on intelligence collection and espionage activities by secretly installing spyware on endpoint systems. As the war drags on far longer than the Kremlin anticipated, Russian hackers now focus on the spyware. (Lewis, 2022).

Case study - Spear Fishing and Malicious Attachments or Links

Russian state and Russian affiliated organizations, such as Gamaredon (targets Ukrainian government, military, law enforcement), APT29 (targets IT, government, think tanks, higher education), FancyBear (targets Government, defense, think tanks, higher education), EnergeticBear (targets Energy, aviation, critical manufacturing, defense industrial base), Callisto Group (targets Intelligence/Defense personnel, think tanks), and Sandworm (targets Critical infrastructure, operational technology) used phishing activities to access the accounts and networks of organizations inside and outside Ukraine (Microsoft, 2022). Many activities use

compromised or spoofed accounts at targeted organizations or within the same industry with compelling themes to lure victims.

APT29 used compromised diplomatic accounts to send phishing emails to foreign ministry employees around the world. FancyBear created spoof accounts based on publicly searched names of account holders within US think tanks and sent phishing information to access the accounts of these think tanks. Additionally, Callisto Group used bait related to coverage of the Ukraine conflict for phishing to gain initial account access to the Nordic countries' international affairs think tanks (Microsoft, 2022).

Transportation Sector

Many sectors involved in critical infrastructure are vulnerable to malicious cyber-attacks, even more-so during the current Russo-Ukraine conflict. The Ukrainian transportation sector has been highlighted in early cyber security strategies as a particularly vulnerable sector in critical infrastructure (Cyber Security Strategy of Ukraine, 2016). Since the beginning of the Ukraine war, we have seen Russian based hacktivist cyber attacks targeting major airports across the US (Rosen, 2022). This sparked concern and compelled the US to enact new cyber security laws. The new laws included the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (CISA, 2022), State and Local Government Cybersecurity Act of 2021 (The White House, 2022), and Federal Rotational Cyber Workforce Program Act of 2021 (The White House, 2022). These bills aimed to address the lack of transparency and collaboration between the government and the private sector in critical infrastructure, as well as the lack of skilled cybersecurity employees within the private sector and government workforce. The new laws, and the Distributed Denial of Service (DDoS) attacks on US airport websites, highlight a severe issue in the US, which is also a widespread problem in NATO. Cooperation and knowledge of attacks between governments and companies poses a severe security issue. The disconnect in knowledge of cyber attacks between governments and private firms poses a severe cybersecurity risk in critical infrastructures. The increase in cyber warfare used not only by governments but also by politically state aligned hacktivist groups also pose a threat. The transportation sector cannot be overlooked, and the protection of its functionality is vital not only in peacetime but also during this tumultuous period with an ever-growing cyber threat imposed by malicious groups and states.

Case Study: DDoS Attacks on US Airport Websites

In October 2022, 14 airports experienced DDoS attacks that resulted in issues with airline websites (Rosen, 2022). This brought large concern and confusion to airlines and aviation safety commissions, and US Senator Jacky Rosen issued a letter to the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Transportation (DOT) for additional information in response to the troubling cyber attacks (Rosen, 2022). These attacks have been attributed to the pro-Russian hacktivist group Killnet. The coordinated attacks on US aviation depict an issue with the cyber security of critical infrastructures, which is expected to increase in a growing hybrid warfare setting.

Intrusions into major airports pose large threats to airlines and aviation transportation as a whole. The DDoS attacks were not recorded to have interfered with airline operations. However, the intrusions were nevertheless of concern as they could have escalated into a more serious threat. These cyber attacks are not new. Russia had been preparing for years before they declared war on Ukraine, testing the limits early on with cyber attacks before and during the war.

The letter from Senator Rosen to the DOT and CISA, which requested additional information regarding the knowledge and response to the cyber attacks, points to the glaring issue of secrecy surrounding cyber security incidents and the lack of cooperation. This is also evident as there has been no documented response from CISA in an article detailing the DDoS attack from Security Week (AFP, 2022). Events like this can be circumvented if necessary measures are taken to establish coordination and communication, like in the case with attacks on US financial structures (Lawder, 2022). When companies become vulnerable to cyber attacks, the implications on their public image and investability compels firms to obscure the truth. (Newman, 2018). This is a prevalent issue, and in the US, legislation was passed for the Strengthening American Cybersecurity Act of 2022, which specifically targets issues of concern to transparency and disclosures pertaining to malicious cyber attacks (Congress, 2022). While steps are being made to amend this ongoing issue , it is clear that neglect and evasion of such issues place firms, especially those involved in critical infrastructure, at risk if they are unable to honestly and cohesively work together in solving cyber security issues.

The rhetoric that is generated by attacks and political activism, or “hacktivism”, is yet another tool in this hybrid war setting. Killnet is a group that has been vocal about its pro-Russian stance, and they have made public statements directly against NATO members and other

states that are leaning towards Ukraine (Roussi, 2022). Although the group's techniques are not considered extremely sophisticated (Roussi, 2022), their public presence and support garnered the hacktivists' presence of concern.

Case Study of NATO Cyber Attack Response

Nations go to war as a mechanism to exert influence on an opponent and create political conditions in their favor. It is relatively easy to define an act of war in physical space. For instance, a Tomahawk Land Attack Missile (TLAM) fired from a naval ship at a target in Syria is an easily identifiable signal of the United States attempting to influence Syrian behavior (Mattis, 2018). Warfare executed via physical means such as artillery, infantry, aerial bombardment and naval blockades has internationally recognized rules, such as the Geneva Conventions, in place to aid in the governing of conflict. However, the development and rapid proliferation of a variety of technological innovations over the past twenty years has fundamentally changed the "character of war" in ways that international law and policy have yet to define. Space-based surveillance platforms, cyber attacks, and the increasingly complex information environment have enabled both state and non-state actors to exert direct influence on rivals that in years past would have required kinetic military action (Dunford, 2018). Moreover, many of these capabilities enable nations to engage in attacks in ways that are difficult-to-impossible to assign attribution, providing political and military decision makers a great degree of flexibility and deniability. Nowhere is this new threat more prevalent than in the cyber domain, where both nations and non-state actors are engaged every day in actions and activities that can have devastating results.

Over the last decade, cyber attacks have become more and more frequent, particularly in Eastern Europe and throughout the North Atlantic Treaty Organization (NATO) states. This paper examines the likely threat vectors for those attacks as well as introduces potential policies that can aid in buffering NATO from continued attack. As these threats become more commonplace, implementing shared standards for security and education, addressing data pipeline vulnerabilities, and increasing transparency across the alliance will be critical to ensuring that each nation is capable of contributing to the collective defense.

Who is Launching the Cyber-Attacks?

NATO members and their allies have been a primary target of one of their main adversaries in East Europe—Russia (Lohmann et al., 2022, p. 77). Since the beginning of the

invasion of Ukraine, NATO's critical infrastructure (CI), such as its energy, maritime, healthcare, communication, government, and transportation sectors, has suffered a significant strike from the opponent. This revealed consequential vulnerabilities that NATO must not ignore. Cyberspace is an area that favors the aggressor more than the defender, as David Cattler, NATO assistant secretary general for Intelligence and Security, noted (Miller, 2022). There is a constant correlation in the lack of cyber security that leads to open exposure for attacks by looking at the case studies presented earlier in the research. This includes the necessity to address the issues within the data pipelines, the absence of transparency, and neglecting systems that could operate more efficiently. The interconnection between OT systems has grown and continues to advance. Therefore, mature cyber security techniques must go hand in hand with developing technologies. Otherwise, a wide variety of industries that are vital for the function of the NATO states and people's lives will continue to be under the control of cyber threats of the Eastern adversary who seeks to attack the CI. NATO must remember that the character of cyber space requires an extensive perspective “through unity of effort at the political, military, and technical levels" (Cyber Defence, 2022).

NATO must cooperate closely with all its allies, and every member state should work alongside the private sector—big companies and corporations, which are crucial players in cyberspace. Both small and medium enterprises (SMEs) can provide innovative answers and explanations in cyber space, addressing data pipeline issues by implementing early warning systems. The NATO Industry Cyber Partnership (NICP), created by Alliance leaders at the 2014 Wales Summit, facilitates quick response to cyber threats by encouraging timely information sharing between SMEs and NATO partners. Therefore, NICP members must incentivize businesses within NATO borders and its allies to implement early warning systems, "enhancing everyone's resilience and capabilities to safeguard information" (NATO Industry Cyber Partnership). NATO would need to propose new policies to the EU so that new strategies on cyber early warning systems can be implemented by the EU parliament on a state level. In addition, companies would also be involved with and affected by these policies if they were passed by the EU parliament, as these mandates would apply to those involved in critical infrastructure.

Moreover, NATO should continue to increase its cyber defense capacity through the education and certification of workers in the critical infrastructure industry as "cyber defense is

as much about people as it is about technology" (Cyber Defence, 2022). In the case of education, the NATO Cooperative Cyber Defense Centre of Excellence (CCD CoE) in Tallinn, Estonia, a NATO-accredited research and training facility, along with the NATO Communications and Information (NCI) Academy in Portugal, could increase collaboration with other education facilities in NATO member states and its allies (Cyber Defence, 2022). The European Security and Defense College (ESDC) is another example. Thus, they should be responsible for providing cyber defense training standards and certification (for the certification of workers in the private and governmental sectors) alongside the organizations mentioned above, thus improving cyber security in critical infrastructure (European Commission, 2022). In addition, it is recommended that the European Union Agency for Cyber Security (ENISA) constantly provide a framework of cybersecurity certification schemes and update specific guidelines (EU Cybersecurity Certification, 2023). Consequently, ENISA would bring these recommendations to the EU Commission and the EU member states, so that new strategies on education and certification of workers can be further implemented by the EU parliament on a state level. Then, government officials would partner with businesses to implement these changes (NATO's Response to Hybrid Threats, 2022).

The partnership between the NATO member states, the European Union (EU), the United Nations (UN), the Organization for Co-operation in Europe (OSCE), and other international organizations is essential in combating cyber warfare. This collaboration is similar to a chain of interconnected links joined together for one purpose; international organizations cannot operate unilaterally in this cyber war. By working together, international organizations can pool their resources and invest in cyber security.

What Policy or Resource Should Be Introduced?

The overlapping themes include the essential need to address the vulnerabilities within the data pipelines, the lack of transparency and overlooking of systems that could work more efficiently, and the rise in hybrid warfare of political activism or "hacktivism". This highlights the lack of investment and focus on securing a state's critical infrastructure with the rise of hybrid warfare and low levels of accountability(Hollis, 2021). So how can this be addressed, and what can be implemented to achieve security? What are the necessary actions that NATO should take? In Sarah Lohmann's book and report, *What Ukraine Taught NATO About Hybrid Warfare*, three norms are mentioned regarding the direction NATO should take. The three norms are

NATO "states should restrain from directing malicious cyber activity at another states critical infrastructure," states should “take responsibility for keeping their cyberspace jurisdictions in order," and thirdly, there should be an international organization “to monitor and report on the violation of the above norms" (Lohmann et al., 2022, p. 22-23).

With suggested norms and the common themes found in the case studies, there are three policy and technology recommendations that were concluded as crucial. First, is the push for the promotion of cyber security education. This idea would be actualized by requiring education on cyber security as well as basic training and certifications for businesses dealing with critical infrastructures. Recently, the European Security and Defence College (ESDC) offered a Cyber Diplomacy Advanced course to address the latest developments on cyber security and ways to implement measures to improve resilience (European Security and Defense College, 2023). As the research progressed, it was understood that there are regulations of this sort currently in place or being proposed by NATO and its allies. The European Union alone proposed the Cyber Resilience Act, which is to promote independent testing, inspection, and certification sectors, in addition to setting reinforced cyber security protocols expected to help companies and manufacturers (Feingold, 2022). This act, currently being negotiated, has the potential to create a unified front with the EU via ENISA and in connection with NATO that focuses on certifications that improve and prepare the workforce. In observing that action has been taken, the report wants to build off of these policies and urge the continuation of implementing this as a norm for allied states to incorporate in the private sector.

Secondly, there needs to be promotion of company standards of concern to data pipeline vulnerabilities by implementing exercises and Cyber Early Warning Systems (CEWS). States need to work with companies that provide services within critical infrastructures to create company norms like cyber security exercises and implement CEWS in order to check efficiency and identify areas for improvement (Christoforatos et al., 2022). Regarding the health sector, multiple partners in the EU participated in testing and simulating a crisis to address vulnerabilities, which proved useful in understanding where the system is lacking before an incident occurred (Christoforatos et al., 2022). Another example can be found within the NATO Cooperative Cyber Defence Centre of Excellence. The Red team vs. Blue team exercise is conducted annually by member nations, where a variety of scenarios are created for the teams to assess how effectively they are working in “reporting incidents, executing strategic decisions and

solving forensic, and legal and media challenges" ("Locked Shields", 2022). As such, implementing workspace exercises conducted by a designated team would provide a sandbox for NATO to be better prepared in responding to potential attacks.

In any scope of policy, unequal application of laws and requirements is present and a major obstacle in this discussion. However, focusing solely on early warning systems would be a significant step toward industries mitigating the impacts of cyber attacks in the data pipeline. ENISA's Programming Document of 2023-2025 outlines measures and a course of plan which the EU should take to increase the level of cybersecurity among its members. This includes the Network Code on Cybersecurity, stipulating rules that are sector specific on risk assessments and requirements. Additionally, it explains implementation of early warning systems to be a measure to address the new security threats with the current war in Ukraine ("Enisa Single Programming Document", 2023, 18). The promotion and implementation of this plan, or one that is similar, in NATO states would address pipeline concerns. As a background, the CEWS work to send alerts and notifications on attacks that include malware or denial of service that interferes with the flow of operations and remove or tamper with information on critical infrastructure systems. This is particular to IoT systems, but on a larger scale. With these systems in place, one would be notified of incident notifications, network abuse events, and vulnerability and open ports alerts, preventing long term impacts ("Early Warning", 2021).

Lastly, the recommendations encourage transparency within industries via federal policies or incentives in NATO states to strengthen malicious cyber intrusion reporting. This would mean fostering EU NATO cooperation to strengthen reporting pertaining to critical infrastructure between states, companies, and stakeholders. An example of this could be seen in the United States' Securities and Exchange Commission (SEC) federal policies that push companies to contact investors and partners of incidents that occur, and regular disclosures of cyber security risks present in their systems (Taylor, 2022). Although there could be pushback from companies, this is an alternative that should be tested. Focusing back on the EU and NATO cooperation, the previously mentioned expansion of the EU Cyber Resilience Act to include cyber intrusion reporting with the preexisting proposals regarding cyber security requirements for products with digital elements is a route that should be taken in NATO member states. ENISA in addition is promoting the Digital Operational Resilience Act (DORA) to the European Parliament. This would require that firms meet a basic cyber security requirement while more

specifically focusing on requirements for information and intelligence sharing that will come into effect in 2025 (“Enisa Single Programming Document", 2023, 17; “The Digital Operational Resilience Act”, 2023). The expansion and implementation of federal and international policies are currently in motion. With this in mind, this report recommends the push of similar policies in place.

Due to NATO’s scope of influence and how it interacts with the European Union, North American states, and individual states, NATO needs to build on previous frameworks, and influence policy. Direct funding in this sector for the national state level can implement these policies, but incentives for industries in the private sector that service in critical infrastructure functions could be useful to smoothly transition to higher transparency. “Incentives leave discretionary space for actors to decide themselves”, and whether it be economic or historic incentives, which is the incentive through experience, it could lead industries to take action without heavy regulation being placed (Wessels et al., 2021). It is important to highlight the economic advantages of information sharing in the private sector and apply similar and improved models such as the Information Exchanges, recommended by ENISA, to achieve this (ENISA, 2010). This refers to Information Sharing Analysis Centers (ISACs) that create a space as non-profit organizations to connect the public and private sectors to share information and incidents. Creating the space to share information in a regulated form, it would allow companies in the private sector to not be hesitant and not fear information being leaked.

With these norms and proposed recommendations, acknowledging the necessity of viewing cyber security threats as one views threats by weapons of mass destruction is important. While there is oversight for weapons of mass destruction, oversight is limited for hybrid warfare tactics that cause the same impact (Terra, 2021). In mentioning this, it’s to suggest that there are also other responses, such as sanctions, instead of hack backs, and enforcement or build off of current state and NATO committees (Terra, 2021). This includes growing initiatives similar to the European Union’s Joint Cyber Unit, NATO’s Comprehensive Cyber Defence Policy, and Battlefield Evidence Policy in which there are teams to collect information and assess cyber security situations (“Brussels Summit Communique”, 2021).

Where Could this New Policy or Technology or Resource be Used?

To promote cyber security education, the government should cooperate with education centers to establish basic training programs on cyber security to strengthen the new generation’s

awareness of cyber security. At present, NATO is strengthening its education and training capabilities to improve its cyber defense capacity. There are four institutions and centers that are known to provide relevant education and training for personnel from allied countries. These include the following organizations: the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia offers recognised expertise and experience; the NATO Communications and Information (NCI) Academy in Oeiras, Portugal provide training for NATO communications and information systems operations and maintenance; the NATO School in Oberammergau, Germany provides cyber defense-related education and training to support alliance operations; the NATO Defense College in Rome, Italy fosters strategic thinking on cyber defense issue (Cyber Defence, 2022). NATO should build more relevant institutions, especially in the eastern member states, for young generations.

To address data pipeline vulnerabilities for future security, countries need to cooperate with private companies that provide critical infrastructure services. The private sector is a key participant in cyberspace, and the technological innovation and expertise of the private sector are crucial for NATO and its allies to effectively respond to cyber threats. Although in recent years, as cyber security has become more and more important, governments, private companies, and research institutions have improved their ability to identify attacks at a higher degree and private and state analysts have established databases and feature patterns for known intruders. At the technical level, the truly harmful network attacks are also becoming increasingly complex (Davis, 2019). Therefore, it is important to deepen the information exchange between private enterprises and the government. It is now known that through the NATO Industry Cyber Partnership (NICP), NATO and its allies are working to strengthen their relations with industry and academia. This partnership includes NATO entities, national Computer Emergency Response Teams (CERTs) and Allies' industry representatives (Cyber Defence, 2022). Currently, only 23 companies have joined the partnership (NCI Agency, 2019), NATO needs to work with more industry leaders and policymakers to develop new strategies to protect data pipelines from new cyber security challenges.

To enhance transparency within industrial national policies in NATO states, member states should further strengthen cooperation and exchanges since the transparency of cyber security and defense measures is also a deterrent signal. Right now, NATO has the NATO Computer Incident Response Capability (NCIRC) which protects NATO's own networks by

providing centralized and round-the-clock cyber defense support, and it will have a Cyberspace Operations Centre (CyOC) to provide situational awareness and coordinate operational activity. The NATO Communications and Information Agency through its NCIRC Technical is responsible for the provision of technical cyber security services throughout NATO. Also, in February 2017, allied defense ministers approved an updated Cyber Defence Action Plan and a roadmap for implementing cyber space as a domain of operations. This increased the allies' ability to work together, develop capabilities, and share information. (Cyber Defence, 2022).

When Should New Policy or Technology Be Used, and Under What Circumstances?

For the policies proposed, the timing is different in each case. Policies should be implemented immediately to start the process and reap the benefits and effects as quickly as possible. Since many of these proposals are preventative measures rather than solutions for post-attack, preventive measures need to be implemented quickly in order to bridge the growing gap between critical infrastructure's cyber vulnerability and emerging technologies. Ukraine, for instance, had taken steps to start fostering cyber education (CRDF Global), along with the preemptive National Cybersecurity Initiative in 2016 (Cyber Security Strategy of Ukraine, 2016). With concern for these proposals, the pressing issue is the timelines that could be bogged down through processes, especially when these policies and implementation of plans are vital in the current climate.

Currently, the European Agency for Cyber Security (ENISA) has plans undergoing development related to certification of cybersecurity for the private sector in the form of certifications for ICT products, services, or processes (ENISA, 2023). These obligations not only apply to products but also the manufacturers, importers, and entities that distribute them (ENISA, 2023). The current target for ENISA is to have 75% of EU nations signed on and begin developing certification processes by the end of 2023 (ENISA, 2023). Regarding the outlined proposals stated previously, if following a similar format under the guidance of ENISA, as these proposals began development in 2021 and were officially announced in 2022, a two year minimum would be realistic for the development of further certification goals pertaining not only to ICT products but also certification processes for employees.

Of concern to policies for the promotion of cyber security in the EU, the timeline for these recommendations would require years. The EU has already begun developing plans to mitigate cyber attack risks. In an article detailing a recently proposed cybersecurity legislation

from WeForum, “the legislation was first put forth by European Commission President Ursula von der Leyen in November 2021. If the act is approved by the European Parliament and the European Council, EU countries will have two years to adapt the new rules” (Feingold, 2022). This proposal has not yet been passed by the end of 2022. Again, EU policies take a long time to be implemented and approved, with even the most pressing policies taking up to three years. Moreover, as EU policies underway coincide with the cybersecurity issues that the proposed recommendations attempt to address, proposals of concern to cyber intrusion reporting would have to be expedited if combined with the policies drafted and proposed in the ongoing EU Policy on Cyber Defense (European Commission, 2022). Moreover, regarding the suggested expansion of the Cyber Resilience Act, expediting a framework for the presentation of this proposal would also need to be implemented by June 2023. EU ministers plan to meet regarding progress on the file (Bird & Bird, 2023), as well as the Presidency’s plans to advance as far as possible with negotiations before the end of their term within these next six months (2023, Dr2 Consultants). It would be necessary if implemented quickly to be included in the framework currently underway.

Implementing new policies, expanding pre-existing ones, and creating standards for cybersecurity require much time, planning, and cooperation. These processes could take up to years, as it relies on individual states and multi-body organizations such as the EU and NATO to approve, process, and implement. The certification policies proposed that would be established by ENISA would also need time to create these propositions that are eventually brought to the EU. This holds true for CEWS standards and cooperative efforts for malicious cyber intrusion reporting. Even with an expedited process occurring during the current Ukraine conflict of concern to cyber security, many policies will still take a long time and need to be given realistically two to three years to be fully implemented and see effective change in preventative measures.

Why Should this Policy or Technology Be Used? What Opportunities Does it Provide? What Vulnerabilities Does it Have, or Challenges Does it Pose to International Security?

Critical infrastructure is essential to our modern, democratic processes (“Critical Infrastructure Sectors.”, 2020). When incapacitated, there are devastating consequences. Furthermore, with the exponential increase in cyber attacks, it is essential to promote cyber security. As we have seen recently, cyber attacks have the potential to disable entire

organizations and major systems, and in turn, if we can bring down these threats, safer, more productive, and more efficient societies will emerge.

Greater cyber security education is one basic way that NATO can better build up its defense against cyber attacks on critical infrastructure. As outlined above, one way that NATO could promote greater cyber security awareness would be through the promotion of the current ENISA (The EU's Agency for Cybersecurity) certification program. The reason why the promotion of cyber security certification, through the EU, makes the most sense is due to the fact that NATO does not have the mandate to implement domestic policies, while the EU does. This means that by working through the EU, one can mandate change rather than suggest it, which will ensure the ratification of all EU nations. Moreover, if all EU nations are aligned, it will be easier for NATO to persuade the final few member states to follow suit. ENISA is doing the most groundbreaking work, as ENISA is currently working on creating an EU-wide cyber security certification called the "EU Cybersecurity certificate" alongside the European Commission ("EU Cybersecurity Certification", 2023). This is by far the most comprehensive and effective way to promote a higher standard of overall security and also better cyber awareness for NATO states, as the framework and process are already underway. This process is also very complex, requiring many resources to organize and maintain it, which is another reason why it makes the most sense for NATO to promote it rather than try to recreate something itself. In the future, if the EU Cybersecurity certificate gets passed through the EU parliament, NATO could then extend the structure to the other few countries that are a part of NATO but not the EU (such as the U.S.). The implementation of a cyber security standard would aim to create systems that are interoperable within each other and can be much more easily fixed due to their homogeneity. Cyber security will also be more easily managed by an overseeing body if all systems are held to the same standard, as opposed to now, where each and every company has different cyber security practices in place. This program would also ensure that more people are educated and up to date on important cyber security matters. Currently, studies by The Journal of Information Security show that there is a very low level of internet safety awareness (Amankwa, 2021). This is very dangerous, as many cyber attacks start small and grow, often going undetected as people are generally unaware of what basic things to look for. Accordingly, with the ENISA Cybersecurity certificate, there are educational courses for workers that will be a requirement for each organization to complete (European Commission, 2022, Page 17). This

certification would also ensure that moving forward, some of the biggest vulnerabilities within NATO's critical infrastructure cyber space, have been addressed, creating much safer systems. One of the ENISA targets is by the end of 2023 to have 75% of EU nations signed on and starting to develop the certification processes (*Enisa Single Programming*, 2023, Page 57). However, one difficulty with the ENISA certification process is that it is still under development, and will take a few years to actually be fully functional. Furthermore, it may be more difficult to get some countries to agree than others, which will create setbacks in the process. With this being said, there are many reasons for NATO to promote ENISA's certification process, which is already underway.

Thus far, this report has made it clear that cyber attacks have been and will continue to be on the rise. Furthermore, there have been many cases of major cyber crimes starting from IoT devices due to their lack of security, making data pipelines very vulnerable. Due to this, it is essential that companies have at least a basic implementation of cyber security exercises such as Cyber Early Warning Systems (CEWS). Currently, most IOT devices are made with cost efficiency over security. Furthermore, IoT devices connect and exchange data with other servers, linking them to larger, more important entities (Cassandra and McFadin, 2015). This needs to be changed so that moving forward there will be fewer of these attacks on NATO countries. One way for NATO to effectively address this problem is to promote the Network Code, which is currently under development by ENISA. The Network Code is a planned cybersecurity standard that will set specific rules for cybersecurity within the critical infrastructure sector. The Network Code has specific cyber security exercises outlined for firms, such as Cyber Early Warning Systems. This will ensure that all firms covered by the Network Code will be resilient against cyber attacks ("Enisa Single Programming Document", 2023, Page 18). A complete and complex process has already been outlined by ENISA, which makes more sense for NATO to promote it rather than trying to recreate something with a similar goal.

The final recommendation given is to foster EU-NATO cooperation to strengthen malicious cyber intrusion reporting pertaining to critical infrastructure. Transparency within critical infrastructure industries is vital because it allows people to work together and pool resources toward a combined effort. Rather than each individual organization trying to solve a problem themselves, they can reach out to others and learn from their mistakes (Singer and Friedman, 2014). A prime example of when transparency could have aided in solving cyber

security issues occurred in the Maritime Sector, where many control systems were infected with the same malware called "Mespinoza/Pysa". This malware was used across multiple countries, and if collaboration and transparency were in effect, the devastating effects could have been mitigated. Another case that was mentioned previously, the cyber attack on U.S. airports, could have also been handled much more effectively if all cases were reported, as a similar attack had occurred a few days prior but went unreported (Lawder, 2022). Thus, we recommend that by encouraging malicious cyber intrusion reporting, NATO can better protect its critical infrastructure.

Conclusion

Overall, all of these recommendations allow for long-term improvement across the Alliance by doing the hard work of setting up a better base of cyber security. The threats posed by actors such as Russia, and increasingly China, in cyberspace will only continue to grow more complex, with potentially greater impacts. Over the past twenty years, both of these nations have made significant investments in their cyber-based capabilities while NATO has lagged behind. By focusing on the protection of critical infrastructure through education, early warning capabilities, data pipeline protections, and increased transparency across the Alliance, NATO can harness the strength of collective defense against these threats.

Policy Recommendations

Recommendations for Combating Malign Influence and Economic Coercion

The results of the dual case studies indicate that the NATO alliance possesses a compelling security interest in countering Chinese supply chain dominance and soft power malign influence operations. First, this paper recommends that to counter Chinese dominance in the REE industry NATO states could implement a three part plan to identify, mitigate, and eliminate reliance on Chinese REE exports as soon as possible, with the year 2027 serving as a deadline, and to pursue partnerships with Norway and Sweden to diversify REE sources. Second, this paper advises that to reduce Chinese malign influence and espionage in NATO academic institutions and governments the alliance could strengthen regulations to monitor and restrict UFWD/CAIFC activities in affected states.

This paper recommends these following policies:

- Establish economic security sub-committee within NATO's Economics and Security Committee to perform comprehensive review of REE supply-chains and consult allied governments on supply-chain diversification and risk mitigation
- Promote the development of alternative supply chains, in collaboration with the European Raw Materials Alliance, by increasing mutual trade and investment in REEs between allied states and non-NATO partners.
- Encourage allied states to establish or enlarge REE strategic reserves
- Formally designate UFWD and CCP-linked institutions as foreign agents, allowing for greater legal and regulatory scrutiny and increased transparency requirements regarding operations in allied nations
- Establish a committee to audit material from CSSAs/UFWD groups present within academic institutions or else audit material through another government body
- State DOE/MOE would conduct screening and background checks to ensure exchange students do not have ties to the Chinese military industrial complex
- NATO states must employ stricter anti-corruption and anti-influence mechanisms by establishing an autonomous agency to counter CAIFC influence operations,
    - The agency will enforce laws on foreign financial transactions and lobbying, imposing a lifetime ban on presidents and vice presidents with a decreasing time period for lower-level officials.
    - The agency will monitor current and former civil service officials to ensure transparency in engagement, disclosure of funding, and editorial conflicts of interest related to CAIFC

Recommendations for Combating Disinformation

Disinformation is becoming increasingly problematic for undermining democracy, international and national security, and trust in government functions and capabilities individually and as a collective. As an international alliance of states, the continued use of disinformation undermines NATO's abilities to function by targeting public opinion, critical infrastructure, and creating various issues for NATO states and its allies, such as the example with Ukraine.

The primary recommendations that would benefit NATO states and create positive policy toward disinformation is through the implementation of:

- Rapid Response Team (RRT): Housing the RRT as part of NATO would allow for collaborative partnerships with outside entities like grassroots and NGOs, while also providing existing resources and avenues to work with existing NATO digital partnerships. The RRT would act as a hub that benefits all collaborating parties by providing a central 'disinformation database'; a Disinformation Communications Team (DCT) specializing in collaborating with NATO's partners would optimize communication, both in initiating the database to assemble finalized reports and in educating the public on disinformation literacy via initiatives and outreach.
- Confidence Building Mechanisms (CBM): These can be built into the RRT through partnering with grassroots and NGOs, as well as nations that actively develop disinformation countermeasures, such as Ukraine. Confidence can be built through expanding education to CEI worker and student communities, helping them to question, recognize, and report disinformation, both in an effort to build the public's skills and increase awareness on the scope of what disinformation is capable of. Agreements that ensure the trustworthiness of wire services to be more verifiable will ultimately help to make information more reliable and affordable to allied countries.
- Media Recommendations: Applying filters to monitor social media on trending subjects using algorithms and registered keywords will benefit the recognition and investigations into disinformation campaigns; additionally, applying disinformation penalties - primarily fines and bans - for deliberate sharing of disinformation will build accountability, leading to more reliable news outlets. Journalism and news reporting criteria need drastic improvement to enact stricter measures for what can be claimed as 'journalism.'

Recommendations for Countering Cyber Attacks

We have witnessed that countries such as Russia, have gained access to significant cyber areas. Due to the rising threat of cyber security (especially during the Russo-Ukrainian war conflict), NATO must implement new tactics, rules, and regulations to provide proper security for its member states and critical infrastructure. Therefore, NATO alliances need to raise more attention on attack vectors within critical infrastructure sectors to truly mitigate NATO's security.

Due to these current issues, we recommend that NATO focus on and invest in long-term prevention mechanisms due to NATO member states' lack of standardization of general cyber

security in critical infrastructure. Prevention would be promoted through cyber security education, security exercises, early warning systems, new regulations for companies, and implementing cyber security mechanisms into emerging tech.

- **NATO and EU promotion of basic cyber security** education in the critical infrastructure industry through work certification.
    - Firms operating in critical infrastructure sectors would require certifications issued by states and given standardized rules set by the EU in collaboration with NATO.
    - Implementation at the national level and standardized across NATO (State by state but education "plan" could be standardized by NATO). NATO and EU are recommended to both have policies due to higher implementation if implemented through the EU and the inclusion of non-EU countries.
    - ENISA can establish the standards and objectives, the EU parliament would vote on these proposals and NATO and EU collaborate to implement policies
- **Promotion of company standards** of concern to data pipeline vulnerabilities by implementing exercises and Cyber Early Warning Systems (CEWS).
    - Implemented by the EU parliament, the application of Cyber Early Warning Systems in IoT systems and exercises to check for cyber vulnerabilities would be implemented in critical infrastructure.
    - Currently, ENISA is promoting the Network Code, which is a planned cybersecurity standard that will set specific rules for cybersecurity within the critical infrastructure sector. The Network Code has specific cyber security exercises outlined for firms, such as CEWS. This will ensure that all firms under the Network Code will be resilient against cyber attacks ("Enisa Single Programming Document", 2023, Page 18).
- **Foster EU-NATO cooperation** to strengthen malicious cyber intrusion reporting pertaining to critical infrastructure between states, companies, and stakeholders.
    - Incentives for companies to communicate cyber intrusions and encourage information sharing through previous and improved models of Information Exchanges.

- Expansion of the EU Cyber Resilience Act to include cyber intrusion reporting with the preexisting proposals regarding cyber security requirements for products with digital elements, as it has not been passed yet.
- Following the recent policies set by the Securities and Exchange Commission (SEC), that push companies to contact investors and partners of incidents, and regular disclosures of cyber security risks, EU could also implement regulations similar to the US.

Looking Forward: NATO in an Age of Hybrid Warfare

For final concluding thoughts, in its over seven decades of operations, NATO has successfully deterred territorial aggression, conducted peace enforcement, and combatted transnational terrorist threats, all the while fulfilling its collective security mandate as the most successful military alliance in history. Yet, as new threats proliferate and the international security environment deteriorates, NATO will have to address pressing new defense needs which extend beyond the scope of conventional warfare.

This report examines several emergent hybrid warfare threats in the domains of economic coercion, malign influence, disinformation, and cyber warfare. Each of these distinct threats possesses the ability to undermine allied security, and taken in the context of the ongoing Russo-Ukrainian War and the China-Russia partnership, present a comprehensive strategic challenge to NATO. Cyberwarfare threatens the integrity of allied critical infrastructure, and disinformation undermines the sociopolitical stability upon which effective collective security depends. Economic coercion degrades the allied industrial base and jeopardizes defense readiness, and malign influence compromises social and policymaking processes from within. Although the NATO allies do not currently face the threat of overt conventional warfare, hybrid threats nevertheless endanger vital allied security interests.

The 2022 invasion of Ukraine has aggravated Russian cyberwarfare and disinformation threats against the NATO alliance. As Ukraine's principal provider of military aid, NATO has had to contend with Russia's hybrid efforts to compromise allied critical infrastructure and social cohesion. NATO must inoculate itself against cyber and disinformation threats by implementing robust cybersecurity measures into critical infrastructure and constructing credible and effective infrastructure to combat disinformation narratives. And as the alliance seeks to continue its support for Ukraine in its defense against Russia's illegal war of aggression, NATO must be

prepared to bolster allied resilience in the face of continued, and perhaps greater, cyber and information threats in the near future.

With the solidification of the China-Russia partnership “without limits”, NATO must also defend against economic and malign influence threats emanating from China. Current allied exposure to Chinese coercion in rare earth element markets constitute a glaring vulnerability in NATO’s defense industrial base, and covert Chinese influence operations present intelligence threats and undermine policymaking capacities. In this context, the alliance must secure its supply chains and exercise its institutions of covert influence, and in the process build capacity to credibly resist China. And in anticipation of rising US-China tensions in the Taiwan Strait and potentially greater Chinese involvement in the Russo-Ukraine War, NATO must prepare itself to confront China as a strategic competitor capable of threatening allied security interests.

Going forward, NATO may find its greatest challenges not on the battlefield, but in combating aggression which falls beneath the threshold of kinetic conflict. Although NATO possesses deep competencies in conventional warfare, new and emergent security exigencies necessitate policy innovation and institutional flexibility. In this regard, and for the purpose of maintaining collective security, NATO must now accustom itself to conflict in an age of hybrid warfare.

Bibliography

Malign Influence & Economic Coercion

Allen-Ebrahimian, B. (2018, February 14). *Chinese government gave money to Georgetown Chinese student group.* Foreign Policy. https://foreignpolicy.com/2018/02/14/exclusive-chinese-government-gave-money-to-georgetown-chinese-student-group-washington-china-communist-party-influence/

Al Jazeera (2022, July 26) *What is Nord Stream 1 and why is it crucial to Europe?* https://www.aljazeera.com/news/2022/7/26/explainer-nord-stream-1-gas-pipeline-russia-germany-europe

Associated Press, (2022, November 11th) *German lawmakers OK delay in switching off nuclear plants*, Berlin https://apnews.com/article/europe-business-germany-olaf-scholz-climate-and-environment-d05757365632c8437a5672878a9eccca

Biesecker, M., Dupuy, B., & El Deeb, S. (2022, October 3). *Russia Smuggling Ukrainian Grain to Help Pay for Putin's War*. PBS. https://www.pbs.org/wgbh/frontline/article/russia-smuggling-ukraine-grain-putin-war/

Bowe, A. (2018, August 14). *China's Overseas United Front Work Background and Implications for the United States.* US-China Economic and Security Review Commission Staff Research Report. https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf

Bowman, E. L. (2019, April 11). *Do Confucius Institutes threaten academic freedom?* Share America. https://share.america.gov/do-confucius-institutes-threaten-academic-freedom/.

Bowman, E. L. (2019, June 18). *Why is China suppressing speech at schools in other countries?* Share America. https://share.america.gov/why-is-china-suppressing-speech-in-u-s-schools/.

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

CAIFC Site. (n.d.). *About the China Association for International Friendly Contact (CAIFC)*. *About the China Association for International Friendly Contact (CAIFC) - About CAIFC-*. CAIFC. https://www.caifc.org.cn/index.php?m=content&c=index&a=show&catid=23&id=563

Cerulus, L. (2022, Dec 14). *Germany is (still) a Huawei hotspot in Europe.* Politico. https://www.politico.eu/article/germany-is-still-a-huawei-hotspot-in-europe-5g-telecoms-network/

Cristiani, Dario, et al. (2021). The Security Implications of Chinese Infrastructure in Europe. *The German Marshall Fund,* 35-44. https://www.gmfus.org/sites/default/files/2022-01/Cristiani%20et%20al%20-%20report%20%281%29%20Updated.pdf

Chan, K., & Wiseman, P. (2022, June 18). *Explainer: How did Russia-ukraine war trigger a food crisis?* AP NEWS. https://apnews.com/article/russia-ukraine-covid-politics-health-middle-east-58bb99da6bf9fc6af5a5a645022bc4d7

Dorfman, Z. (2018, July 27). *How silicon valley became a den of spies.* Politico. https://www.politico.com/magazine/story/2018/07/27/silicon-valley-spies-china-russia-219071/.

Fedasiuk, R. (2020, September 16). *Putting money in the Party's mouth: How China mobilizes funding for united front work.* Jamestown. https://jamestown.org/program/putting-money-in-the-partys-mouth-how-china-mobilizes-funding-for-united-front-work/.

Garnaut, J. (2023, January 30). *How China interferes in Australia*. Foreign Affairs. https://www.foreignaffairs.com/articles/china/2018-03-09/how-china-interferes-australia

Gershaneck, K. K. (2020). *Political Warfare*. MCU. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-11-no-1/Political-Warfare/

Go, J. (2022, September 17). *Beijing-linked influence campaign takes aim at Western investors.* FDI Intelligence. https://www.fdiintelligence.com/content/feature/beijinglinked-influence-campaign-takes-

Aim-at-western-investors-81245

Grasso, V. B., & Congressional Research Service. (2013). *Rare earth elements in national defense: Background, oversight issues, and options for Congress*. Congressional Research Service. https://apps.dtic.mil/sti/citations/ADA590410

Grossman, Derek. (2021, November 10). *Taiwan Is Safe Until at Least 2027, but with One Big Caveat.* The Rand Blog. https://www.rand.org/blog/2021/11/taiwan-is-safe-until-at-least-2027-but-with-one-big.htM1

Hart, B. (2020, July 17). *Does China pose a threat to global rare earth supply chains?* China Power. https://chinapower.csis.org/china-rare-earths/

Hartman, L. (2020, August 27). *Confucius Institutes advance Chinese propaganda on campuses.* Share America. https://share.america.gov/confucius-institutes-advance-chinese-propaganda/.

Hill, Jenny. (2023, Jan 19). *Germany says it is no longer reliant on Russian energy.* BBC. https://www.bbc.com/news/business-64312400

Hund, K., La Porta, D., Fabregas, T. P., Laing, T., & Drexhage, J. (2020). *Minerals for Climate Action: The Mineral Intensity of the Clean Energy Transition*. World Bank Group. https://pubdocs.worldbank.org/en/961711588875536384/Minerals-for-Climate-Action-Th
e-Mineral-Intensity-of-the-Clean-Energy-Transition.pdf

International Energy Agency. (2022, October 31). *European Raw Materials Alliance*. Iea.org. https://www.iea.org/policies/14268-european-raw-materials-alliance

Jakobsen, S. E., & Amundsen, B. (2022, November 29). *Norway could make Europe less dependent on critical minerals from China*. ScienceNorway. https://sciencenorway.no/finance-finans-mineralogy/norway-could-make-europe-less-dependent-on-critical-minerals-from-china/2108785

Kucukgocmen, A., & Spicer, J. (2022, November 24). *Ukraine grain exports sputter after an extension deal with Russia*. Reuters. https://www.reuters.com/markets/commodities/ukraine-grain-exports-sputter-after-extension-deal-with-russia-2022-11-24/

Lloyd-Damnjanovic, A and Bowe, A. (2020, October 7). *Overseas Chinese Students and Scholars in China's Drive for Innovation.* US-China Economic and Security Review Commission Staff Research Report. https://www.uscc.gov/sites/default/files/2020-10/Overseas_Chinese_Students_and_Scholars_in_Chinas_Drive_for_Innovation.pdf

Lord, E. M., & The Senate Committee on Armed Services. (2020). *Supply chain integrity*. Armed Services Senate. https://www.armed-services.senate.gov/hearings/20-09-16-supply-chain-integrity

Luard, T. (2005, July 22). *Asia-Pacific | China's Spies Come out from the Cold.* BBC. http://news.bbc.co.uk/2/hi/asia-pacific/4704691.stm.

Myles, D. (2023, February 23). *Sweden ignites northern Europe's rare earth cluster*. FdiIntelligence. https://www.fdiintelligence.com/content/feature/sweden-ignites-northern-europes-rare-earth-cluster-82020

Nakano, J. (2022). *The geopolitics of critical minerals supply chains*. Center for Strategic and International Studies. https://www.csis.org/analysis/geopolitics-critical-minerals-supply-chains

Needham, Kirsty. (2022, March 15). *Australia unveils $360 mln in critical minerals funding to offset China dominance.* Reuters. https://www.reuters.com/business/australia-unveils-360-mln-critical-minerals-funding-offset-china-dominance-2022-03-16/

Norge Mining. (2023, February 7). *ERMA supports Norge Mining in securing finances* Businesswire.com. https://www.businesswire.com/news/home/20230206005592/en/ERMA-supports-Norge-

Mining-in-securing-finances-for-responsible-sourcing-of-crucial-minerals-in-Norway-to-secure-EU%E2%80%99s-autonomy-on-Critical-Raw-Materials

Paddison, L. (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

Schweizer, P. (2022, January 28). Chinese elite have paid some $31 million to Hunter and the Bidens. New York Post. Retrieved February 15, 2023, from https://nypost.com/2022/01/27/chinese-elite-have-paid-some-31m-to-hunter-and-the-bidens

Sevastopulo, D., Mitchell, T., & Yu, S. (2021, February 16). *China targets rare earth export curbs to hobble US defence industry.* Financial Times. https://www.ft.com/content/d3ed83f4-19bc-4d16-b510-415749c032c1

Solomon, E., & Bennhold, K. *Shadowy Arm of a German State Helped Russia Finish Nord Stream. 2* New York Times. https://www.nytimes.com/2022/12/02/world/europe/germany-russia-nord-stream-pipeline.html

State Department. (2020, December 18). *China's Coercive Tactics Abroad.* State Gov. https://2017-2021.state.gov/chinas-coercive-tactics-abroad/index.html.

Thomson R. (2023, January 13). *Sweden's LKAB finds Europe's biggest deposit of rare earth metals*. Reuters. https://www.reuters.com/markets/commodities/swedens-lkab-finds-europes-biggest-deposit-rare-earth-metals-2023-01-12/

United States Department of Defense. (2018). *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*. Media Defense. https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

Wehrmann, Benjamin. (2022, Nov 22). *Heating costs to rise by 1,000 euros for German homeowners even after deducting state support.* Cleanenergywire.org.

https://www.cleanenergywire.org/news/heating-costs-rise-1000-euros-german-homeowners-even-after-deducting-state-support

Wong, E., & Swanson, A. (2023, January 2). *How Russia's War on Ukraine Is Worsening Global Starvation*. The New York Times. https://www.nytimes.com/2023/01/02/us/politics/russia-ukraine-food-crisis.html

Yao, X. (2022, September 7). *China is moving rapidly up the rare earth value chain.* Brink News. https://www.brinknews.com/china-is-moving-rapidly-up-the-rare-earth-value-chain/

Cyber Security

AFP. (2022, October 10). *US Airport Websites Hit by Suspected Pro-Russian Cyberattacks.* SecurityWeek. https://www.securityweek.com/us-airport-websites-hit-suspected-pro-russian-cyberattacks/.

Agency, N. C. I. (n.d.). *NATO Industry Cyber Partnership*. NCI Agency | NATO Industry Cyber Partnership. https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022, March 7). *Cybersecurity Challenges in the Maritime Sector*. MDPI. https://www.mdpi.com/2673-8732/2/1/9

Amankwa, E. (2021, September 9). *Relevance of cybersecurity education at pedagogy levels in schools*. Journal of Information Security. https://www.scirp.org/journal/paperinformation.aspx?paperid=111804#:~:text=To%20ensure%20cybersecurity%20awareness%20and,to%20protect%20themselves%20from%20cybercrimes.

Bilal, A. (2021, November 30). *Hybrid warfare – new threats, complexity, and 'trust' as the antidote.* NATO Review. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Brussels Summit Communique. (2021, June 14). North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

Burgess, M. (2022, March 23). *A mysterious satellite hack has victims far beyond Ukraine*. Wired. https://www.wired.com/story/viasat-internet-hack-ukraine-russia/

Christoforatos, N., Lella, I., Rekleitis, E., Van Heurck, C., Zacharis, A. (2022, December). *CYBER EUROPE 2022: AFTER ACTION REPORT:Findings from a PAN-EUROPEAN cyber crisis Exercise*. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report.

Critical Infrastructure Sectors. Cybersecurity and Infrastructure Security Agency CISA. (2020, October 21). https://www.cisa.gov/critical-infrastructure-sectors

Cyber Europe 2022: After action report. (2022, December 13). ENISA. http://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

Cyber Awareness Challenge 2023. (2023). *DoD Cyber Exchange Public*. https://public.cyber.mil/training/cyber-awareness-challenge/.

Cyber Defence. (2022, March 23). NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

Cyber Incident Reporting for Critical Infrastructure Act of 2022. (2022, March). Cybersecurity and Infrastructure Securty Agency. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

Cyber Security Strategy of Ukraine (2016). https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf.

Cyber Incident Tracer #HEALTH. (2022, September 29). CyberPeace Institute. https://cit.cyberpeaceinstitute.org/explore.

Cyberattack Hits Multiple Greek Shipping Firms. (2021, November 3). The Maritime Executive. https://maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms

Cyber Defence. NATO. (2022, March 23). https://www.nato.int/cps/en/natohq/topics_78170.htm.

Davis, S. (2019, August 13). NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence. NATO PARLIAMENTARY ASSEMBLY. https://www.nato-pa.int/download-file?filename=sites/default/files/2019-

09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf

David Lawder. (2022, November 1). *U.S. Treasury Thwarted Attack by Russian Hacker Group Last Month-Official.* Reuters. https://www.reuters.com/world/us-treasury-targeted-by-russian-hacker-group-last-month-official-2022-11-01/.

Dunford, J. F. (2018, April 12). *From the chairman: The character of war and strategic landscape have changed*. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1491632/from-the-chairman-the-character-of-war-and-strategic-landscape-have-changed/

Early Warning. (2021, May 11). National Cyber Security Centre. https://www.ncsc.gov.uk/information/early-warning-service#section_3.

Emmott, R. (2018, October 16). NATO Cyber Command to be fully operational in 2023. Reuters. https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9

ENISA. (2010, September 8). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security.* https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing.

ENISA Single Programming Document 2023-2025. (2023, January). *file:///C:/Users/penel/Documents/School/enisa_programming_document_2023_2025.pdf*

Enisa Single Programming Document 2023-2025. ENISA. https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-report-2023-2025.

European Commission. (2022, November 10). Joint Communication to the European Parliament and the Council. European Commission. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

European Cyber Resilience Act: Can new requirements strengthen your organization's cybersecurity resilience? (2023, February). Dr2 Consultants. https://dr2consultants.eu/european-cyber-resilience-act/#:~:text=On%2015%20September%202022%2C%20the,been%20taking%20action%20against%20cybercrime.

EU Cybersecurity Certification. ENISA. https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq

EU's response to the energy challenges. (2022 Dec). European Union-Eurobarometer. https://europa.eu/eurobarometer/surveys/detail/2912

EU Cybersecurity Certification. ENISA. https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq

European Commission. (2022, November 10). *Joint Communication to the European Parliament and the Council*. European Commission. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

Feingold, S. (2022, September 28). *New European Union cybersecurity proposal takes aim at cybercrime.* World Economic Forum. https://www.weforum.org/agenda/2022/09/new-european-union-cybersecurity-proposal-takes-aim-at-cybercrimes/#:~:text=The%20EU's%20Cyber%20Resilience%20Act,to%20surpass%20%E2%82%AC10%20trillion.

Heads of State and Government NATO Summit. (2022, June 29). NATO 2022 Strategic Concept. https://www.nato.int/strategic-concept/.

Hollis, D. (2021, June 14). *A brief primer on International Law and Cyberspace*. Carnegie Endowment For International Peace. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763.

HVAC Vendor Allegedly Hacked: Access Gained to Hospital Systems. (2021, August 23). HIPAA Journal.https://www.hipaajournal.com/hvac-vendor-allegedly-hacked-access-gained-to-hospital-systems/.

Is the EU Healthcare Sector Cyber Healthy? The Conclusions of Cyber Europe 2022. (2022, December 13). ENISA. https://www.enisa.europa.eu/news/is-the-eu-healthcare-sector-cyber-healthy-the-conclusions-of-cyber-europe-2022

Microsoft. (2022). Microsoft Digital Defense Report 2022. Microsoft Security. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Joint Communication to the European Parliament and the Council. (2022,Oct 11). European Commission. *https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq*

Lewis, J. A. (2022, June 16). Cyber War and Ukraine. CSIS. https://www.csis.org/analysis/cyber-war-and-ukraine#:~:text=Russia%20sought%20to%20disrupt%20services,by%20Russia%20in%20these%20attacks.

Locked Shields. (2022). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/exercises/locked-shields/.

Lohmann, S. J. et al. (2022). *What Ukraine Taught NATO about Hybrid Warfare*. US Army War College USAWC Press.

Mattis, J. N. (2018, April 13). *Briefing by Secretary Mattis on US Strikes in Syria*. United States Department of Defense. https://www.defense.gov/News/Transcripts/Transcript/Article/1493658/briefing-by-secretary-mattis-on-us-strikes-in-syria/-of-cyber-europe-2022.

Miller, M. (2022, March 12). *NATO prepares for Cyber War*. POLITICO. https://www.politico.com/news/2022/12/03/nato-future-cyber-war-00072060

Miller, M. (2022, December 28). *The Mounting Death Toll of Hospital Cyberattacks*. POLITICO. https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638.

NATO Secretary General warns of growing cyber threat. (2022, Nov 10). NATO. https://www.nato.int/cps/en/natohq/news_208889.htm?selectedLocale=en

NATO's response to hybrid threats. (2022, June 21). NATO https://www.nato.int/cps/en/natohq/topics_156338.htm

NCI Agency. (2019, October 17). Three NATO Industry Cyber Partnership Agreements signed at Nias'19. NATO COMMUNICATIONS AND INFORMATION AGENCY. https://www.ncia.nato.int/about-us/newsroom/three-nato-industry-cyber-partnership-agreements-signed-at-nias19-.html

Newman, Craig. (2018, March 5). *When to Report a Cyberattack? For Campanies, That's Still a Dilemma.* The New York Times. https://www.wsj.com/articles/fears-of-cybersecurity-attacks-may-increase-disclosure-requirements-for-businesses-11647444384

Nicaise, V. (2022, September 1). *Port Cyberattack: Hackers & Maritime Cybersecurity*. Stormshield. https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/.

Nichols, S. (2022, August 18). Russian cyber attacks on Ukraine driven by Government Groups: TechTarget. Security. https://www.techtarget.com/searchsecurity/news/252523950/Russian-cyber-attacks-on-Ukraine-driven-by-government-groups

O'Neill, P. H. (2022, May 11). *Russia hacked an American satellite company one hour before the Ukraine invasion*. MIT Technology Review. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/#:~:text=The%20attack%2C%20on%20February%2024,effectively%20destroyed%20in%20this%20way

Patrick McFadin, A. C. (2015, August 7). *Internet of things: Where does the data go?* Wired. https://www.wired.com/insights/2015/03/internet-things-data-go/

Press corner. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_5374

Press Release: Bill Signed: S. 1097, S. 2520, S. 3823. (2022, June 21). The White House https://www.whitehouse.gov/briefing-room/legislation/2022/06/21/press-release-bill-signed-s-1097-s-2520-and-s-3823/#:~:text=2520%2C%20the%20%E2%80%9CState%20and%20Local,Representative%20Neguse%20for%20their%20leadership

Ralston, W. (2020, November 11). *The Untold Story of a Cyberattack, a Hospital and a Dying Woman*. WIRED. https://www.wired.co.uk/article/ransomware-hospital-death-germany.

Rosen, Jacky. (2022, October 17). *The Honorable Pete Buttigieg the Honorable Jen Easterly*. https://www.rosen.senate.gov/wp-content/uploads/2022/10/Letter-to-DOT-and-CISA-on-Russian-Cyberattacks-on-Airports-10.17.2022.pdf.

Rosen, Jacky. (2022, October 18). *After Recent Russian Cyberattacks Target U.S. Airports, Rosen Sends Letter to Biden Administration Requesting Additional Information.* Jacky Rosen. https://www.rosen.senate.gov/2022/10/18/after-recent-russian-cyberattacks-target-u-s-airports-rosen-sends-letter-to-biden-administration-requesting-additional-information/.

Roussi, Antoaneta. (2022, September 11). *Meet Killnet, Russia's Hacking Patriots Plaguing Europe.* POLITICO. https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/.

Singer, P. W., &; Friedman, A. (2014). *Cybersecurity and cyberwar what everyone needs to know*. Oxford University Press. https://ebookcentral-proquest-com.offcampus.lib.washington.edu/lib/washington/reader.ction?docID=1538365

Strengthening American Cybersecurity Act of 2022. (2022, March 1). Congress. https://www.congress.gov/bill/117th-congress/senate-bill/3600/text

Strengthening cybersecurity in Ukraine by building capacities at local universities. CRDF Global. https://www.crdfglobal.org/news/strengthening-cybersecurity-ukraine-building-capacities-local-universities/

Swedish Presidency of the Council of the European Union. (2023, Feb 16). Lexology. https://www.lexology.com/library/detail.aspx?g=cd0b45d1-8b42-4e9a-b954-d8633137f0d5

Taylor, H. (2022, November 8). *Coming Clean: Why Cybersecurity Transparency Is A Strength, Not A Weakness*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/11/08/coming-clean-why-cybersecurity-transparency-is-a-strength-not-a-weakness/?sh=360692f1be24.

Terra, J. (2021, August 4). *NATO Cannot Cede The New Art Of Modern Warfare To Russia And China*. Reporting Democracy. https://balkaninsight.com/2021/08/04/nato-cannot-cede-the-new-art-of-modern-warfare-to-russia-and-china/.

The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554. (2023). The Digital Operational Resilience Act. https://www.digital-operational-resilience-act.com/.

Uberti, David. (2022, March 17). *Fearing More Cyberattacks, Congress Requires Key Businesses to Report Digital Breaches*. The Wall Street Journal https://www.wsj.com/articles/fears-of-cybersecurity-attacks-may-increase-disclosure-requirements-for-businesses-11647444384

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., van Ruijven, T. (2021, October). *Understanding incentives for cybersecurity investments: Development and application of a typology*. Digital Business, *1*(2). https://doi.org/https://doi.org/10.1016/j.digbus.2021.100014.

Winder, D. (2019, July 10). *U.S. Coast Guard Issues Alert After Ship Heading Into Port of New York Hit by Cyberattack*. Forbes. https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=4813597541aa

Disinformation

Abend, L. (2022, March 6). *Meet the Lithuanian 'Elves' Fighting Russian Disinformation*. Time. https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine/

About. (2022, April 12). EUvsDisinfo. https://euvsdisinfo.eu/about/

Anadolu Agency Turkish Inc. (n.d.). Anadolu Agency. https://www.aa.com.tr/en/

Associated Press. (2021, March 17). *Polish state websites hacked and used to spread false info*. AP NEWS. https://apnews.com/article/europe-poland-eastern-europe-lithuania-nuclear-waste-424dd97778b3d2046bc1cb61a175f270

Berger, J.M.. (2017, August 7). *The Methodology of the Hamilton 68 Dashboard.* Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/the-methodology-of-the-hamilton-68-dashboard/

Berger, J.M. & Rosenberger, L. (2017, 2 August). *Hamilton 68: A New Tool to Track Russian Disinformation on Twitter.* Alliance for Securing Democracy.

https://securingdemocracy.gmfus.org/hamilton-68-a-new-tool-to-track-russian-disinformation-on-twitter/

Bittman, L., & Godson, R. (1985). *The KGB and Soviet Disinformation: an Insider's View*. Pergamon-Brassey's.

Bloomberg News. (2022, February 24). *Transcript: Vladimir Putin's Televised Address on Ukraine*. Bloomberg. https://www.bloomberg.com/news/articles/2022-02-24/full-transcript-vladimir-putin-s-televised-address-to-russia-on-ukraine-feb-24#xj4y7vzkg

BROD Establishes a Regional EDMO Hub to Combat Disinformation in Bulgaria and Romania. Ontotext. (2023, February 20). https://www.ontotext.com/company/news/brod-establishes-a-regional-edmo-hub-to-combat-disinformation-in-bulgaria-and-romania/

Corker, B. (2017). (rep.). *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*. Washington, DC: U.S. Government Publishing Office.

Council of Europe. (n.d.). *Dealing with propaganda, misinformation and fake news - democratic schools for all - publi.coe.int*. Democratic Schools for All. https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/dealing-with-propaganda-misinformation-and-fake-news

De Witte, M. (2022, April 13). *What to Know about Disinformation and How to Address It.* Stanford News. Stanford University. https://news.stanford.edu/2022/04/13/know-disinformation-address/.

Developmentaid. DevelopmentAid. (n.d.). https://www.developmentaid.org/

Disinformation and Russia's war of aggression against Ukraine. (2022, November 3). OECD. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

DISINFO Database. (n.d.). EUvsDisinfo. https://euvsdisinfo.eu/disinformation-cases/?text=&date=21.02.2023+-+22.02.2023

Disinfo: US May Give Western Ukraine to Poland If Warsaw Pays Kyiv's Debt to the US. (2023, 23 January). EUvsDisinfo. https://euvsdisinfo.eu/report/us-may-give-western-ukraine-to-poland-if-warsaw-pays-kyivs-debt-to-the-us.

Estonia. (7 Dec. 2019). EU DisinfoLab. https://www.disinfo.eu/resources/estonia-2/.

European Commission. (2023, January 11). *European Digital Media Observatory (EDMO)*. European Commission. https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory

European Parliament Press Releases. (2022, July 12). *EU citizens trust traditional media most, new Eurobarometer survey finds*. European Parliament. https://www.europarl.europa.eu/news/en/press-room/20220704IPR34401/eu-citizens-trust-traditional-media-most-new-eurobarometer-survey-finds

European Union. (2021, October 12). *Tackling disinformation: Information on the work of the EEAS Strategic Communication division and its task forces (SG.STRAT.2)*. European Union External Action. https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication_en

Farley, R. (2022, March 31). Fact Check. https://www.factcheck.org/2022/03/the-facts-on-de-nazifying-ukraine/

Gajek, M., Kowalczyk, M., & Krīgere, M. (2022, November 4). *Different countries, similar messages. How Kremlin's propaganda spreads in Baltics and Poland—LRT Investigation*. LRT. https://www.lrt.lt/en/news-in-english/19/1813845/different-countries-similar-messages-how-kremlin-s-propaganda-spreads-in-baltics-and-poland-lrt-investigation

Garcia-Navarro, L. (2020, December 13). *How disinformation spreads, and why it's so hard to combat*. NPR. https://www.npr.org/2020/12/13/945989935/how-disinformation-spreads-and-why-its-so-hard-to-combat

Grenier, M. (2022, March 6) *Fake News, Real Violence: Disinformation's Threat to Canadian Critical ...* https://canis-network.ca/wp-content/uploads/2022/06/Marianne-Grenier-Disinformation-and-Critical-Infrastructure-CANIS.pdf.

Haines, J. R. (2015, February). *Russia's Use of Disinformation in the Ukraine Conflict*. Foreign Policy Research Institute. https://www.fpri.org/article/2015/02/russias-use-of-disinformation-in-the-ukraine-conflict/

Hamilton 2.0 Dashboard. (n.d.). Alliance For Securing Democracy. https://securingdemocracy.gmfus.org/hamilton-dashboard/

HENSOLDT Analytics. (2022, October 3). *Russian Propaganda Narratives about Ukraine: Russian Sacrifices, Western Lies, and Heavy Censorship of the Russian Media*. HENSOLDT Analytics. https://www.hensoldt-analytics.com/2022/09/16/russian-propaganda-about-ukraine/

Home. (2023, February 10). EU DisinfoLab. https://www.disinfo.eu/

Howard, P. N., Ganesh, B., & Liotsiou, D. (n.d.). *The IRA, Social Media and Political Polarization in the United States, 2012-2018*. Computational Propaganda Research Project. https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf

How the People's Republic of China Amplifies Russian Disinformation. (2022). U.S. Department of State. https://www.state.gov/briefings-foreign-press-centers/how-the-prc-amplifies-russian-disinformation

Institute for Strategic Dialogue. (2023, February 10). *Home Page*. ISD Global. https://www.isdglobal.org/

Jamalzadeh, S., Barker, K., González, A. D., & Radhakrishnan, S. (2022, July 26). *Protecting infrastructure performance from disinformation attacks*. Nature News. https://www.nature.com/articles/s41598-022-16832-w

Kohler, K. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture: Policy and*

Organizations. ETH Zürich.

Kremlin Disinformation Bulletin - United States Department of State. (2022, Aug 31) U.S. Department of State. U.S. Department of State https://www.state.gov/disarming-disinformation/kremlin-disinformation-bulletin/.

Kuvaldin, S. (2022, July 12). *Why Russia Keeps Insisting That Poland Is Preparing to Partition Ukraine*. Carnegie Endowment for International Peace. https://carnegieendowment.org/politika/88585

Lans, S. van der. (2021, February 26). *18 organizations leading the fight against fake news*. The Trusted Web. https://thetrustedweb.org/organizations-leading-the-fight-against-fake-news/

Lighting fire to emotions with lies. (2023, February 9).EUvsDisinfo. https://euvsdisinfo.eu/lighting-fire-to-emotions-with-lies/

Ling, J. (2022, March 18). *How 'Ukrainian bioweapons labs' myth went from QAnon fringe to Fox News*. The Guardian. https://www.theguardian.com/media/2022/mar/18/ukrainian-bioweapons-labs-qanon-fox-news

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

McLaughlin, J. (11 May 2022). *How One of Russia's Neighbors Is Dealing with Putin's Propaganda.* NPR. NPR, https://www.npr.org/2022/05/11/1096856581/how-one-of-russias-neighbors-is-dealing-with-putins-propaganda.

Mick, C. (2022, June 15). *Ukraine and Poland: Why the countries fell out in the past, and are now closely allied*. The Conversation. https://theconversation.com/ukraine-and-poland-why-the-countries-fell-out-in-the-past-and-are-now-closely-allied-184906

Moore, J. (1997). *Deception and Deterrence in "Wars of National Liberation," State-Sponsored Terrorism and Other Forms of Secret Warfare*. Carolina Academic Press.

NATO. (2022, March 28). *Partnerships and Cooperative Security Committee*. North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/topics_79430.htm

NATO. (2022, December 6). *Partnerships: Projecting stability through cooperation*. North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/topics_84336.htm

NATO. (2021, May 27). *How does NATO respond to disinformation?* North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/news_184036.htm#:~:text=NATO%20is%20committed%20to%20transparent%20and%20honest%20communication,communicating%20proactively%20and%20exposing%20major%20cases%20of%20disinformation

The News Literacy Project. (2023, February 7). News Literacy Project. https://newslit.org/

Nuclear power generation share by country 2021. (2023, January 16). Statista. https://www.statista.com/statistics/270367/share-of-nuclear-power-in-the-power-supply-of-selected-countries/#:~:text=Nuclear%20share%20of%20domestic%20electricity%20generation%202021%2C%20by%20select%20country&text=France%20has%20the%20greatest%20share,of%20France's%20total%20electricity%20production.

Paul, C. & Matthews, M. (2016). *The Russian 'Firehose of Falsehood' Propaganda Model Why It Might Work and Options to Counter It.* Rand. https://www.rand.org/pubs/perspectives/PE198.html.

Poland to counter disinformation threats. Polish Press Agency. (2022, September 23). THEfirstNEWS. https://www.thefirstnews.com/article/poland-to-counter-disinformation-threats-33276

Social Media Fact Sheet. (2021, April 7). Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/fact-sheet/social-media/

Reboot Foundation: Improving Critical Thinking in the 21st Century. (2023, February 6). REBOOT FOUNDATION | Elevating Critical Thinking. https://reboot-foundation.org/

Roussi, A. (2022, August 18). *Estonia Fends off 'Extensive' Cyberattack Following Soviet Monument Removal*. Politico. https://www.politico.eu/article/estonia-extensive-cyber-attack-following-soviet-war-monument-removal/#:~:text=Russian%20patriotic%20hackers%20hit%20Estonia's,cancel%20tourist%20visas%20for%20Russians.

Russia's war against Ukraine "affects people even far away from the battlefield". (2022, October 21). EUvsDisinfo. https://euvsdisinfo.eu/russias-war-against-ukraine-affects-people-even-far-away-from-the-battlefield/

from Europe. (2019, July 16). Congress.Gov. https://www.congress.gov/event/116th-congress/house-event/LC64157/text?s=1&r=1.

Tass Russian News Agency. (n.d.). Russian News Agency. TASS. https://tass.com/

Russian so-called 'peace proposals' are empty PR stunts. EUvsDisinfo. (2023, January 18). https://euvsdisinfo.eu/russian-so-called-peace-proposals-are-empty-pr-stunts/

Sardarizadeh, S. (2019, September 14). *Instagram fact-check: Can a new flagging tool stop fake news?* BBC News. https://www.bbc.com/news/blogs-trending-49449005

Sarlo, A. W. (2017, July 6). *Fighting disinformation in the Baltic States*. Foreign Policy Research Institute. https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/

Sarlo, A. Wiktorek. (2017, July 6). "Fighting Disinformation in the Baltic States." *Foreign Policy Research Institute*. https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/.

Sienicka, A., & Makowska, M. (2022, June 16). *Strategies for Addressing Disinformation in Eastern and Central Europe*. Medium. https://techsoup.medium.com/strategies-for-addressing-disinformation-in-eastern-and-central-europe-f94c9ef9c290

Sienicka, A. (2022, June 28). *Strategies for Addressing Disinformation in Eastern and Central Europe.* The TechSoup Global Network. https://techsoup.medium.com/strategies-for-addressing-disinformation-in-eastern-and-central-europe-f94c9ef9c290

Shaping Europe's digital future. European Commission. (2020, February 19). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en

Shifting the focus, engineering paranoia, manufacturing fake threats. EUvsDisinfo. (2023, February 3). https://euvsdisinfo.eu/shifting-the-focus-engineering-paranoia-manufacturing-fake-threats/

Smith, B., & Browne, C. A. (2021). *Tools and weapons: The promise and the peril of the Digital age*. Penguin Books.

Smith, B. (2022, February 28). *Digital Technology and the war in Ukraine*. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

Stevens, S. J. (Trans.). (2022, September 20). *How to Counter Disinformation: Communication Strategies, Best Practices, and Pitfalls to Avoid*. Union of Concerned Scientists. https://www.ucsusa.org/resources/how-counter-disinformation

Still at war: Russia's disinformation targeting Ukraine. EUvsDisinfo. (2022, November 30). https://euvsdisinfo.eu/still-at-war-russias-disinformation-targeting-ukraine/

Suliman, A. (2022, January 24). *Sweden Sets up Psychological Defense Agency to Fight Fake News, Foreign Interference.* The Washington Post. WP Company. https://www.washingtonpost.com/world/2022/01/06/sweden-fake-news-psychological-defence-agency/.

Sweden Defends Its Elections against Disinformation, 2016 – 2018 | Innovations for Successful

Societies. (2020). The Trustees of Princeton University, https://successfulsocieties.princeton.edu/publications/sweden-defends-its-elections-against-disinformation-2016-%E2%80%93-2018.

Tani, M. (2022, March 20). *Reuters staff raise alarms over partnership with Russian-owned wire service*. Politico. https://www.politico.com/news/2022/03/20/reuters-staff-partnership-russian-wire-service-00018779

Terracino, B., Craig M. (2022, November 2). *Disinformation and Russia's War of Aggression against Ukraine.* OECD. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/.

Thomson Reuters. (n.d.). *Breaking International News & Views*. Reuters. https://www.reuters.com/

Tucker, J., et al. (2018). *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature.* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3144139.

Twelve myths about Russia's war in Ukraine Exposed. (2023, February 20). EUvsDisinfo

https://euvsdisinfo.eu/twelve-myths-about-russias-war-in-ukraine-exposed/

Twigg, K., and Kerry A. (2021, March 12). *The Disinformation Tactics Used by China.* BBC News. https://www.bbc.com/news/56364952.

Twitter Inc. (2021, January 8). *Permanent suspension of @realDonaldTrump*. Twitter. https://blog.twitter.com/en_us/topics/company/2020/suspension

United States, Congress, Foreign Relations, Womack, T. (2018). *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security: A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations, United States Senate, One Hundred Fifteenth Congress, Second Session, January 10, 2018*, US Government Publishing Office. 115th Congress, 2nd session, report.

Ukraine War Resource Hub. (2022, June 16). EU DisinfoLab. https://www.disinfo.eu/ukraine-hub/

Véritér, S. (2021, December 12). *European Democracy and Counter-Disinformation: Toward a New Paradigm?* Carnegie Europe. https://carnegieeurope.eu/2021/12/14/european-democracy-and-counter-disinformation-toward-new-paradigm-pub-85931

Wire service. 2023. In *Merriam-Webster.com*. https://www.merriam-webster.com/dictionary/wire%20service

Zabjek, A. (2023, January 22). *Deny, Deflect, Distract': How Russia Spreads Disinformation about the War in Ukraine*. CBC News. https://www.cbc.ca/news/politics/disinformation-ukraine-stop-fake-org-1.6721522.

Żaryn, S. (2022, December 16). *Russia's operation against Poland and NATO.* Emerging Europe. https://emerging-europe.com/voices/russias-operation-against-poland-and-nato/