The Case for an Icelandic Cyber Exploitation and Defense (ICED) Force for NATO Coalition Operations

Johan Sigholm
Dept. of Systems Science for Defence and Security
Swedish Defense University
Stockholm, Sweden
johan.sigholm@fhs.se

Bjarni Már Magnússon
Faculty of Law
Bifröst University
Bifröst, Iceland
bjarnim@bifrost.is

Magnús Skjöld
Faculty of Social Sciences
Bifröst University
Bifröst, Iceland
magnus@bifrost.is

Theodor Gislason
Syndis
Reykjavík, Iceland
teddi@syndis.is

Gregory Falco
Sibley School of Mechanical and Aerospace Engineering
Cornell University
Ithaca, USA
gfalco@cornell.edu

***Abstract*—Iceland's rapidly growing technology economy with significant dependence on digital communication, yields cybersecurity threats that pose a multifaceted challenge. We raise the question of how coalition operations, and the integration of international best practices for national cyber security, could effectively bolster the cyber defense capabilities of a NATO member state such as Iceland. A main contribution of this paper is the detailing on the role that NATO, with its profound experience in multi-domain joint operations and its established Cooperative Cyber Defence Centre of Excellence (CCDCOE), could significantly augment the cyber defenses of Iceland. This includes knowledge sharing, joint training exercises, rapid incident response collaborations, and shared cyber intelligence platforms. Drawing on experience from Nordic countries, fortified by NATO support and multi-sector collaboration, we conclude that the establishment of an Icelandic Cyber Exploitation and Defense (ICED) Force is necessary to strengthen Iceland's digital ramparts. An Icelandic Cyber Command will send a resounding message of deterrence, signaling Iceland's commitment and capability to thwart cyber threats with its coalition partners.**

***Index Terms*—Cyber Defense, NATO, Iceland, Nordics, Coalition Cyber Operations, CCDCOE**

I. Introduction

The digital age, characterized by its unprecedented interconnectivity and technological advancements, brings forth both unparalleled opportunities and profound vulnerabilities. In this matrix of evolving networks, states and institutions must fortify their defenses against growing cyber threats. Iceland, renowned for its pristine landscapes and geothermal marvels, has recently emerged as an epicenter of both technological innovation and associated cyber vulnerabilities. Iceland's ambitious dive into technology has seen significant growth in digital infrastructure such as data centers and high technology companies. This growth, catalyzed by the availability of affordable and abundant hydro-electric electricity, has attracted substantial international investments, particularly in the form of a booming data center industry. Coupled with significant investments in improved connectivity, illustrated by the recently (March 2023) launched IRIS 108 Tbps undersea cable system linking Iceland to Ireland and onwards to Europe and the US, Iceland is asserting its place as a premier hub for advanced yet cost-effective digital infrastructure. Nevertheless, this digital feat also has its downsides.

Given its vast data center infrastructure and focus on end-user privacy, Iceland has inadvertently become a de-facto staging ground for illicit cyber activities [1]. Notably, Chinese and Russian threat actors have exploited the nation's digital infrastructure for potentially malevolent purposes. These actors have firmly entrenched themselves, attempting to make notable land purchases, expanding diplomatic relations, and fostering increased investment in digital infrastructure in-country which has been a cause for international concern [2]. The strategic location of these target landholdings, coupled with considerable investment in information and communication technology infrastructure through nation-state connected entities such as Huawei, amplifies the potential threats manifold [3]. Such physical and digital presence of adversarial actors poses significant challenges to both Iceland's national security and the broader Euro-Atlantic community. For example, Iceland's Data Protection Authority alerted Icelanders to unnecessarily broad video surveillance activity around the Chinese embassy [4]. Iceland's exposed position in relation to existing cyber threats is especially worrisome in light of the country being ranked "at the bottom of the list" in terms of cybersecurity [5].

Iceland's geo-strategic significance is not solely based on its land or digital assets; it extends to the undersea and the skies [6]. The country hosts pivotal digital infrastructures of monumental importance to NATO and the broader Euro-Atlantic community. Crucial submarine cables that establish direct

communication channels between the US and Europe thread through Icelandic territories. Additionally, Iceland's satellite communication infrastructure, characterized by several indispensable ground stations, plays a vital role in ensuring seamless communication and surveillance for the transatlantic alliance. The security of these assets is paramount, not just for Iceland, but for the entire North Atlantic community. Recently, NATO has expressed concern about Chinese investment in Icelandic ground station infrastructure for what is claimed to be "Northern Lights research" [7]. Some scholars believe such ground infrastructure is part of a vast network of over-the-horizon-radar systems that China has strategically located around the globe, disguising them as dual-use scientific research stations [8], [9].

This paper is the product of discussions among Swedish, Icelandic and American experts in cybersecurity and national security law. It further incorporates insights from workshops held with members of the Icelandic National Security Council and high tech industry leadership across Iceland. In this paper, we raise the question: *How can Iceland constructively engage in cyber coalition operations while simultaneously improving its cyber national security by leveraging international collaborations and best practices?*

Given this intricate web of opportunities, threats, and global stakes, the establishment of a dedicated Cyber Exploitation and Defense Force (ICED) for Iceland emerges as an imperative. The intent is not just to defend Iceland's security but to ensure the resilience and security of broader transatlantic digital communication and defense systems. Collaborative endeavors, especially with defense giants like NATO, can harness shared intelligence, resources, and expertise, optimizing the defense against the backdrop of Iceland's unique challenges. As Iceland treads the path toward bolstering its cyber defenses, it need not venture alone. Several small states have embarked on similar journeys, having realized the indispensable need for formidable cyber defense mechanisms in light of rising digital threats. Two such nations, Sweden and Estonia, serve as valuable case studies for Iceland.

This paper aims to offer a comprehensive blueprint for Iceland, drawing from both its unique challenges and the lessons of fellow states. The subsequent sections will detail Iceland's digital assets, analyze the threats from adversarial actors, propose defense strategies inspired by Sweden and Estonia, and delve into potential collaborations, especially with NATO. To conclude, Iceland's intricate digital scenario calls for a well-rounded, collaborative approach. Drawing from the experiences of other nations and harnessing the strength of global alliances will be pivotal to ensure Iceland's digital future remains secure and thriving. This paper will traverse the multifaceted landscape of Iceland's digital challenges, drawing from global benchmarks and offering comprehensive strategies. Ensuing chapters will detail the intricacies of Iceland's digital and geo-strategic assets, dissect the emerging threats from foreign actors, and advocate for robust defense mechanisms, emphasizing the role of NATO and collaborative international endeavors. Iceland's position in the global digital chessboard is both advantageous and vulnerable. Navigating this delicate balance will determine its future resilience, security, and prominence in the digital domain.

We commence our exploration with an overview of the cyber threat landscape, emphasizing the unique vulnerabilities Iceland faces due to its geopolitical positioning and its recently gained position as a leading center for digital infrastructure in the Euro-Atlantic region. Drawing inspiration from international benchmarks, as well as successful defense strategies adopted and operationalized by comparable nations, we propose a framework for the inception, growth, and operation of an Icelandic Cyber Exploitation and Defense (ICED) Force to bolster the nations defenses against a broad range of cyber threats. Special emphasis is given to the pivotal role of human capital, highlighting strategies for the recruitment, training, and retention of top-tier cyber talent.

II. Iceland's Military Posture

Iceland is a country that has actively eschewed a military since becoming a republic and fully independent from Denmark on June 17, 1944. Despite this stance, it was a founding member of NATO and has been an active member since NATO's inception in 1949. In 1951, the United States and Iceland signed a bilateral defense agreement in which the United States committed to defending Iceland's interests on behalf of NATO in return for basing rights in Keflavik, Iceland. In 2006, the United States agreed to continue providing for Iceland's defense, while also making provisions for decommissioning the permanent base in Keflavik. Despite not having a military, Iceland maintains an active Coast Guard and domestic police force, both under the guise of being law enforcement agencies. The Icelandic Coast Guard patrols its waters and performs search and rescue operations. In addition it is responsible for operational defence tasks in Iceland including but not limited to operation of NATO – Keflavik Air Base, Security Zones, Iceland Air Defence Systems, its remote radar and communication sites. It also provides host nation support for all Allied visiting forces operating in Iceland [10].

Due to the domestic political discourse, that has often tended to interpret Iceland's lack of military capabilities as a 'pacifist' stance, Icelandic authorities have outwardly expressed discomfort with offensive military operations [11]. However, the nature of warfare has changed. In June 2023 pro-Russian hacking group NoName057 launched cyber attacks targeting the Icelandic Parliament's websites and Icelandic cyber infrastructure, potentially in response to Iceland hosting the Council of Europe Summit [12]. The Computer Emergency Response Team of Iceland (CERT-IS), housed in the Electronic Communications Office of Iceland, has struggled to defend against such threats previously [13]. This is unsurprising given Iceland's purely defensive and reactive stance to cyber incidents. Other countries have taken a more proactive approach to defending their country from offensive cyber operations by defending forward in the digital domain. For example, the United States has adopted a cyber strategy of persistent engagement and defending forward, which has yielded success [14], [15].

Table I
SUPPORT TO ICED FORCES PROVIDED BY NATO

Cyber Defense Support	Description
Assessment and Gap Analysis	Conduct thorough assessments of Iceland's current cyber infrastructure, identifying vulnerabilities and areas for improvement.
Joint Training Exercises	Organize and lead joint training exercises, simulating real-world cyberattack scenarios to test and enhance response mechanisms.
Shared Intelligence and Resources	Offer real-time threat intelligence, sharing information about emerging threats, and providing resources to counteract them. FMN provides a secure platform for sharing threat intelligence, vulnerabilities, and best practices among member nations.
Infrastructure Fortification	Assist in strengthening the nation's critical digital infrastructure, from submarine cables to data centers, ensuring they remain resilient against sophisticated attacks. As part of the FMN initiative, Iceland can tap into a suite of advanced cyber defense tools, software, and technology solutions that are being used across NATO member nations.
Communication and Information Systems	FMN enables a rapid instantiation of mission networks, enhancing interoperability and serving as a foundation for efficient communications.

Given that the UN Charter does not explicitly consider all cyber operations an act of force, we argue that Iceland can preserve its proclaimed pacifist ethos, while conducting offensive cyber operations for purposes of national security through the creation of ICED. As subsequently described, Iceland has the in-country skills to adopt such a cyber operations strategy and it would serve to benefit engagement for future NATO coalition operations.

III. ICELAND'S CURRENT CYBERSECURITY LANDSCAPE

Iceland's national security and defense strategy rests on the foundation of the country's collaboration with NATO, an active collaboration with other Nordic countries, and its defence agreement with the United States. In understanding the nuances of Iceland's cybersecurity needs, it's pivotal to first comprehend the nation's existing capabilities. This highlights the current cyber defense infrastructure of Iceland, spanning the civilian commercial sector, public sector initiatives, and the nation's long-term cybersecurity strategy for 2022–2037.

Civilian Commercial Sector—The Icelandic civilian commercial sector has witnessed a surge in cybersecurity startups and enterprises over the past decade. Drawing from the nation's strong IT talent pool and innovative research institutions, the Icelandic commercial sector offers a wide array of services including penetration testing, threat intelligence, and cybersecurity consultancy. Many of these firms have pioneered unique cybersecurity solutions tailored to the needs of the Icelandic market, such as the fishing and aluminium smelting industries, while some have gained traction in global markets.

Collaborative Ventures—Some Icelandic cybersecurity firms have forged partnerships with international counterparts, benefiting from shared technologies, methodologies, and market access. Among the most prominent is Syndis, Iceland's leading information security company, with operations in both US and continental Europe. Especially noteworthy is the offensive capabilities Syndis has demonstrated publicly by working with top-tier US based companies such as Dropbox [16]. Syndis has over the years trained many of Iceland's top cybersecurity experts that have demonstrated competitiveness at a global level, for example by qualifying for the Defcon CTF finals, placing second among the nordics in CTF competitions, and placing 17th in the European Cyber Security Challenge where the USA placed 15th.

Defend Iceland—Syndis was recently awarded a 2,5 million Euro grant under the Digital Europe plan for the project Defend Iceland, a nationwide bug bounty platform aimed at including every Icelandic organisation and company in scope. Iceland is an ideal testing ground for a project of such a large scale with short communication lines between government and industry. In addition the nation's digital infrastructure and services reflect a microcosm of other nation states due to several factors, including population size, high level of digital literacy, and geographical isolation. Defend Iceland is supported by key stakeholders, indicating a strong shift in the cybersecurity culture and readiness to employ innovative and cost-effective ways to improve cyber resilience that eventually could be transposed globally.

Education and Training—Recognizing the importance of cybersecurity awareness, several enterprises have established training centers, offering courses ranging from cybersecurity clinics for students to help small businesses to advanced threat mitigation classes [17]. In 2023, Iceland was awarded a grant from the European Digital Innovation Hubs Network to create The Center for Digital Innovation to focus on cybersecurity. This grant will foster collaboration across the university ecosystem, startup companies and established industry with founding partners including companies Origo and Syndis, Auðna Tæknitorg (the Icelandic Technology Transfer Office,) the University of Iceland, the University of Reykjavík and Rannís.

Public Sector—To promptly address and mitigate cyber threats and incidents, the Icelandic government established the Computer Emergency Response Team (CERT-IS) in 2013, as organisational unit under the Electronic Communications Office of Iceland (ECOI). As the national authority on cyber incident response, CERT-IS collaborates closely with other governmental bodies, the private sector, and international counterparts. Its remit is multifaceted, encompassing threat intelligence sharing, coordinating national responses to significant cyber incidents, and advising both public and private entities on best practices for cyber resilience. The Icelandic government has also invested in modernizing the

public sector's digital infrastructure through such initiatives as Digital Iceland, launched in 2018, ensuring that it is built on contemporary technological frameworks that inherently prioritize security, thus reducing potential vulnerabilities.

The Icelandic National Cybersecurity Strategy—In November 2021, the Icelandic government published a comprehensive National Cybersecurity Strategy for the years 2022–2037, outlining the nation's vision and action plan for the next fifteen years. This strategy, a testament to Iceland's commitment to cyber resilience, emphasizes several key areas:

- **Infrastructure Protection**: Recognizing the importance of safeguarding critical infrastructure, from energy grids to communication networks, the strategy lays out measures for their continual assessment and fortification.
- **Public-Private Partnerships**: A significant portion of the strategy is dedicated to fostering partnerships between the government and the commercial sector, ensuring that both domains benefit from mutual expertise.
- **Research and Innovation**: The strategy earmarks substantial resources for research and innovation, aiming to keep Iceland at the forefront of cybersecurity technologies and methodologies.
- **International Collaboration**: Given the transnational nature of cyber threats, the strategy underscores the importance of international cooperation, particularly with bodies like NATO and the EU, to bolster Iceland's cyber defenses.
- **Capacity Building**: Aiming to build a nation well-equipped to handle cyber challenges, the strategy outlines plans for comprehensive training, curriculum integration, and the establishment of cybersecurity institutions.

IV. The Role of NATO for ICED

NATO can play a pivotal role in enhancing Iceland's cyber defenses. One of the most effective ways is through the deployment of multi-national Cyber Protection Teams (CPTs) to Iceland, leveraging the NATO Federated Mission Networking (FMN) framework for enhance interoperability and information-sharing. Such teams, comprised of experts from various member states, bring a wealth of knowledge, experience, and resources to the table.

Table 1 describes the main support provided by NATO CPTs by working closely with a future ICED Force, and other Icelandic agencies and institutions.

Further, as of March 2023 Iceland became a formal member of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The annual Locked Shields exercise, organized by the NATO CCDCOE in Estonia, is the world's largest and most advanced international live-fire cyber defense exercise. 2023 was the first year Iceland participated in this event, where Iceland and Sweden partnered to take first place of the 38 countries participating, demonstrating its cyber defense prowess [18]. By participating in and even organizing such drills, Iceland can ensure its defense personnel remain at the cutting edge of cyber defense strategies.

V. Case: Sweden

Sweden's National Strategy for Information and Cyber Security, set forth by the Swedish Government in 2017, acts as the guiding principle for all cyber-related activities in the country. It identifies threats, vulnerabilities, and outlines clear goals. Such a strategic foundation ensures that various departments and agencies operate in tandem and toward a common objective. Sweden's approach underscores the importance of multi-agency collaboration. The Swedish Armed Forces, Swedish Security Service (Säpo), and the Swedish Civil Contingencies Agency (MSB) work in concert to safeguard the nation's cyber realm. This synergy allows for pooling resources, intelligence, and capabilities, ensuring a unified response to threats. Established in 2022, the Swedish National Cyber Security Centre (NCSC) is tasked by the Swedish government to reinforce the nation's capability to prevent, detect, and manage cyberattacks. The center coordinates stakeholder efforts in the area, and publishes advice regarding active cyber threats, vulnerabilities, and risks. Recognizing that a significant chunk of cyber infrastructure is owned and operated by the private sector, Sweden has been proactive in fostering public-private partnerships. The Forums for Cyber Security Information Sharing, an initiative by MSB, serves as a platform for dialogue and cooperation between state agencies and private stakeholders within several separate business verticals. For Iceland, this can be an invaluable lesson in integrating the strengths of the civilian commercial sector with national defense imperatives.

Sweden's emphasis on educating the public about cyber risks cannot be understated. One of the most publicized campaigns during the last few years was the brochure "If Crisis or War Comes" from 2018—distributed by mail to all Swedish households—detailing how Swedes can become better prepared for the consequences of serious accidents, military conflict, or cyber attacks. Through various such campaigns, the Swedish public is continously made aware of potential threats and best practices for digital hygiene. Iceland, given its interconnected digital infrastructure, would do well to emulate this aspect, ensuring its populace remains a strength, not a vulnerability. Despite its tradition of neutrality, Sweden actively collaborates with international entities, including EU, NATO, and other nations on cyber-related issues. The sharing of threat intelligence, best practices, and participation in joint drills strengthens Sweden's cyber posture. Sweden's National Defence Radio Establishment (FRA) actively monitors cyberspace, ensuring that emerging threats are identified and countered proactively. The dynamic nature of cyber threats necessitates an adaptive defense mechanism, where exploitation of an aggressor's cyber weaknesses may sometimes be the best approach to defense. Companies like Ericsson, based out of Sweden, play pivotal roles in the global digital infrastructure. The expertise and insights from such entities are integrated into Sweden's national defense strategies. Iceland, with its burgeoning digital infrastructure sector, can similarly leverage insights from its commercial entities for national defense.

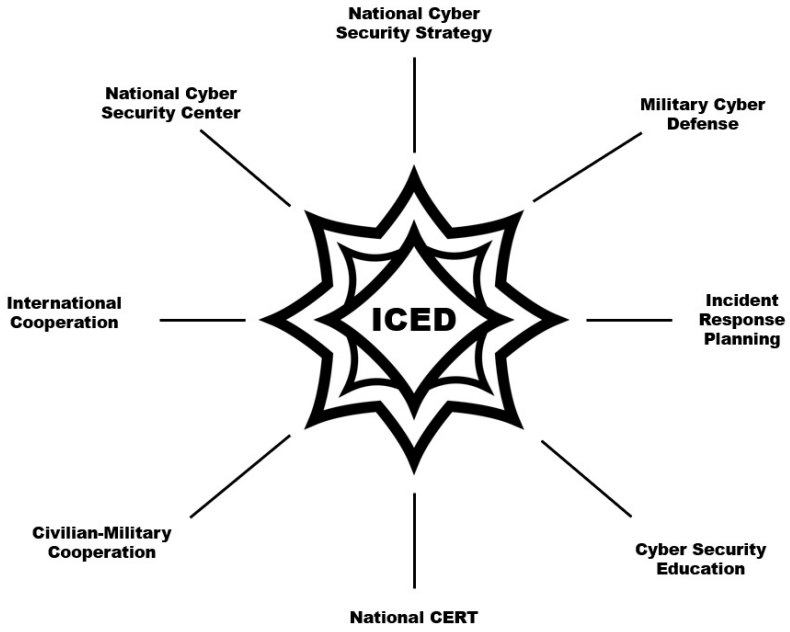

Figure 1. Capability Components of ICED Forces

VI. Case: Estonia

Estonia's experience with cyber defense stands as a beacon for nations grappling with the challenges of an interconnected digital age. The 2007 cyber-attacks on Estonia, which crippled its financial, media, and governmental online platforms, acted as a wake-up call. Since then, Estonia has transformed itself into a global leader in the realm of cyber defense. Its journey offers invaluable lessons for nations like Iceland, eager to fortify their digital frontiers.

Following the 2007 attacks, Estonia promptly revisited its national cybersecurity policies. The result was the National Cyber Security Strategy, which placed cyber defense at the forefront of national defense priorities. It demonstrates the need for a responsive policy framework that evolves with threats. Estonia's response after the 2007 attack wasn't just defensive; it involved a deep introspection and post-incident analysis, leading to revamped strategies and infrastructure. This adaptive mindset, where failures become steppingstones to robust solutions, is essential for any nation, including Iceland. One of Estonia's most significant achievements is its transformation into a digital society, with e-governance at its heart. e-Estonia ensures that governmental services are accessible online, reflecting a deep trust in its cyber defense capabilities. This trust arises from rigorous security measures, a model Iceland could emulate to bolster public faith in digital platforms. Estonia realized early on that cybersecurity was not just a national concern but a global one. As a result, Estonia has been a strong advocate for international cooperation, leading to the establishment of the NATO CCDCOE in its capital, Tallinn. By fostering international collaboration, Iceland can tap into a global reservoir of knowledge and expertise.

Like Sweden, Estonia acknowledges the crucial role the private sector plays in cybersecurity. Their close cooperation with tech companies, ISPs, and banks ensures that the national cyber defense framework is holistic and resilient. Estonia's Cyber Defence Unit, a part of its voluntary Defence League, exemplifies civilian engagement in national cyber defense. Citizens with IT skills offer their expertise to fortify the nation's cyber infrastructure, creating a robust line of defense that complements professional military and governmental efforts.

VII. Building Blocks of Iceland's Future Cyber Defense Capability

To fortify Iceland against the ever-evolving spectrum of cyber threats, a comprehensive and multi-faceted approach to defense is imperative. This section delves into the eight cornerstone components vital for building a robust and resilient cyber defense framework for Iceland.

- **National Cyber Security Strategy**: A clear, well-defined national cyber security strategy serves as the roadmap for Iceland's cybersecurity initiatives. It defines the nation's cyber priorities, threats, vulnerabilities, and outlines measures for preparedness, response, and recovery. Although the current strategy from 2021 lays down a cohesive foundation, it must continuously be revised to stay in line with technological trends and geopolitical development.
- **Military Cyber Defense**: A potent military cyber defense capability is as vital as conventional armed forces. Since the war in Ukraine started, the number of cyberattacks targeting Nordic countries has grown significantly, where Iceland has become a de-facto staging ground for illicit cyber activities. This involves the creation of specialized

units trained in cyber operations, tools for threat detection and response, and ongoing warfare simulations to prepare for potential cyber attacks targeting national defense assets.

- **National Cyber Security Center (NCSC)**: Drawing inspiration from Sweden's National Cyber Security Center, Iceland should consider establishing its own NCSC. This body would act as the epicenter for cyber threat intelligence, risk assessments, and providing best practices to sectors across the nation, enhancing the country's overall cybersecurity posture.
- **Active National CERT**: The Icelandic Computer Emergency Response Team (CERT-IS) acts as the frontline defense, offering immediate response to cyber incidents and facilitating their mitigation. An active national CERT, working in tandem with the NCSC, would provide the necessary technical expertise and coordination for incident management at a national level.
- **International Cooperation**: In the realm of cybersecurity, no nation stands alone. Given the borderless nature of cyber threats, international cooperation—-both military and civilian—-is paramount. Engaging in alliances, sharing threat intelligence, and participating in multinational cyber exercises can significantly boost Iceland's readiness and response capabilities.
- **Incident Response Planning**: Having a clear-cut incident response plan ensures timely and efficient action during a cyber crisis. This involves categorizing potential threats, designating roles and responsibilities, and setting communication protocols for a swift response to mitigate the impact of cyber incidents.
- **Civilian-Military Cooperation**: Cyber security is not just a security issue. It is also a requirement to fully harness the power of innovation. A harmonized approach between civilian entities and military units is thus crucial. Civilian infrastructure often becomes the target in cyber conflicts. To future-proof all of society there needs to be awareness, expertise, and regulations regarding cyber security. Seamless cooperation, sharing resources and intelligence between these two sectors can amplify the nation's defense mechanisms.
- **Cyber Security Education**: The cornerstone of a resilient cyber defense is an informed populace. Integrating cybersecurity education into school curricula and conducting public awareness campaigns can empower individuals to safeguard their digital realms. A well-informed society can act as the first line of defense, reducing vulnerabilities and enhancing national cyber resilience.

VIII. Discussion

The digital era has ushered in not only unprecedented opportunities but also multifaceted challenges, as exemplified by nations like Estonia and Sweden. Iceland, in its strategic location and with its growing digital infrastructure, finds itself at a unique juncture, necessitating robust defenses against cyber threats. Establishing an Icelandic Cyber Exploitation and Defense Force, fully integrated with partner resources in multinational operations, appears to be an attractive approach to address to meet the plethora of cyber threats that the country is faced with.

Drawing from the lessons of Sweden and Estonia, a cohesive national strategy becomes imperative. This strategy should outline Iceland's objectives, threats, stakeholder roles, and long-term goals in the cyber domain. It will provide a directional compass for the ICED Force, ensuring alignment with national priorities. The complexity of modern cyber threats requires a multi-layered defensive approach. This means integrating capabilities across sectors, from monitoring submarine cables and satellite communication ground stations to safeguarding national data centers. The ICED Force should be equipped to detect, defend, and deter threats across these layers. Given its NATO affiliations and the lessons from Estonia's active collaboration on global platforms, Iceland should prioritize international cooperation. NATO's Federated Mission Networking, which enables joint operations, data sharing, and improved situational awareness, can be a pivotal tool for the ICED Force. Much like Sweden's approach, Iceland needs to recognize the invaluable expertise lying within its private sector. A synergetic relationship between the ICED Force and companies, especially those operating critical infrastructure, can enhance threat detection and response times. Estonia's Cyber Defence Unit demonstrates the strength of civilian engagement. A similar voluntary defense league in Iceland, perhaps an eventual spin-off from Defend Iceland, drawing from the nation's pool of IT professionals and enthusiasts, can significantly augment the ICED Force's capabilities. Continuous training, simulations, and international cyber drills should be integral to the ICED Force. Such initiatives ensure that the ICED Force remain updated on evolving threats and best practices, honing their skills in real-time scenarios. Beyond mere defense, the ICED Force should be adept at rapid incident response, minimizing potential damage. Furthermore, post-incident analysis and feedback loops, much like Estonia's approach post-2007, will ensure that the force continuously refines its strategies and tools.

Lastly, as Iceland has established itself as a focal point for digital communication services in the Northern Atlantic, it's paramount for the country to prioritize societal cyber hygiene. Iceland's strategic position between North America and Europe magnifies its importance, especially given Russia and China's acquisition of both physical and cyber assets within its borders. These acquisitions present potential vulnerabilities, possibly allowing covert surveillance or sabotage of key digital connections between Europe and the U.S. Strengthening governance over foreign investments, coupled with enhanced threat detection and diplomatic engagements, is crucial for safeguarding national interests. Iceland must simultaneously fully integrate its cyber defenses with alliance members to ensure its digital domain remains secure and sovereign.

IX. Conclusion

Iceland has exceptional in-country expertise in the cyber domain, which, if appropriately organized, could yield significant contributions to NATO cyber coalition operations. Iceland's currently fragmented approach to cyber national security does not serve its domestic interests or its allies. Organizing and coalescing Iceland's cyber resources into an Icelandic Cyber Exploitation and Defense (ICED) Force will allow Iceland to remain true to its civilian-focused strategic ambitions, while engaging in a robust defend forward and persistent engagement cyber strategy. As evidenced by Iceland's joint win with Sweden at Locked Shields in 2023, engaging in robust cyber coalition operations has great potential. The ICED Force blueprint outlined in this paper proposes a path toward fostering robust coalition engagement that will benefit both Iceland and its NATO allies.

Author's Note

Insights gathered from the Icelandic National Security Council and workshops with Icelandic industry stakeholders were conducted while co-author Dr. Gregory Falco served as a Fulbright Iceland-National Science Foundation Scholar in Cybersecurity and Critical Infrastructure in Reykjavik, Iceland.

References

[1] F. House, "Freedom on the net 2022," 2022.
[2] T. Dams, L. van Schaik, and A. Stoetman, "Presence before power," *Clingendael Netherlands Institute of International Relations*, 2020.
[3] C. Osborne, "Does china's route to infrastructure control run through iceland's data centers," 2019.
[4] J. Distill, "Chinese embassy in iceland may be breaking privacy laws," *The Reykjavik Grapevine*, 2020.
[5] A. Ómarsdóttir, "Iceland is at the bottom of the list in terms of cyber security," *Ríkisútvarpið*, 2023. [Online]. Available: https://www.ruv.is/frettir/innlent/2023-03-12-island-nedarlega-a-bladi-i-netoryggismalum
[6] N. Boschetti, N. Gordon, J. Sigholm, and G. Falco, "Commercial space risk framework assessing the satellite ground station security landscape for nato in the arctic and high north," in *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 2022, pp. 679–686.
[7] I. F. Vilhjálmsson, "Nato hefur lýst áhyggjum af rannsóknarmiðstöð kína um norðurljósin," *Heimildin*, 2023. [Online]. Available: https://heimildin.is/grein/17192/nato-hefur-lyst-yfir-ahyggjum-vegna-rannsoknarmidstodvar-kina-um-nordurljosin/
[8] N. Boschetti, I. Nikas, S. Sharma, and G. Falco, "A global ionosphere situational awareness architecture for over the horizon radar operations," *IEEE Aerospace Conference*, 2024.
[9] "Undercover infrastructure dual-use arctic satellite ground stations, author=Falco, Gregory and Nicolo Boschetti and Ioannis Nikas, journal=CIGI, year=2024,."
[10] I. C. Guard, "Security and defence," *lhg.is, year=2023*.
[11] S. Lyall, "Disquiet in iceland that its peacekeepers dress for war," *New York Times, Reykjavík Journal*, 2004.
[12] C. Szumski, "Heightened cyber attacks threat before council of europe summit in reykjavik," *EURACTIV.com*, 2023.
[13] C. Szumski, "Cyberattacks target icelandic official websites, tech companies," *EURACTIV.com*, 2023.
[14] J. Hsu and G. Falco, "Space booby traps: Hacking back and assured cyber deterrence in space," in *2023 IEEE International Conference on Assured Autonomy (ICAA)*. IEEE, 2023, pp. 115–118.
[15] M. Smeets, "Us cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection," *Intelligence and National Security*, vol. 35, no. 3, pp. 444–453, 2020.
[16] Dropbox, "Offensive testing to make dropbox (and the world) a safer place," *Dropbox*, 2018. [Online]. Available: https://dropbox.tech/security/offensive-testing-to-make-dropbox-and-the-world-a-safer-place
[17] M. MCGRATH, "Cybersecurity in the icelandic multiverse," in *Ethnographic Praxis in Industry Conference Proceedings*, vol. 2022, no. 1. Wiley Online Library, 2022, pp. 317–335.
[18] Ministry for Foreign Affairs, "Joint iceland-sweden team wins nato's largest cyber defence exercise," *government.is*, 2023.