Southern China International MUN

Official Background Guide

Security Council: On measures to mitigate state-sponsored cyber-attacks in the Baltics

Agenda overseen by: Aiden Jung

1. Description of the Issue

1.1 History of the Issue

In an era growing more and more dependent on technology and with everyday lives becoming more reliant on social media, cyber-attacks have emerged as growing threats to national security, economic stability, and public trust—there has never been a tool more powerful than technology in the historical world of politics. As tensions in the Baltic region have grown, the utilization of technology has become more aggressive—especially through state-sponsored cyberattacks.

State-sponsored attacks first started being recognized in the late 20th century as nations started fearing the potential of digital tools for espionage and sabotage. Although early incidents were generally isolated and experimental, the rapid advancement of technology in the 1990s and early 2000s also created fertile ground for cyberattacks.

The history of state-sponsored cyberattacks in the Baltic Sea region has been shaped by a number of geopolitical tensions, especially those involving Russia and its neighboring countries. A notable incident was the 2007 cyberattack in Estonia that was largely attributed to Russian hackers. The attacks resulted after the Estonian government announced a decision to relocate the "Bronze Soldier Memorial", a Soviet-era monument—a decision that sparked significant protests from Russia [5][6]. The attacks, which lasted between April 27 and May 18, 2007, targeted a variety of Estonian government agencies, financial institutions, and media outlets through a series of Distributed Denial of Service (DDoS) attacks [7]. In response, Estonian banks implemented measures to temporarily cut off foreign traffic to mitigate the cyberattacks and protect local clients [5]. Russian origin was identified by analyzing the 1~2 million pre-infected bots across 175 jurisdictions with the identification of Russian language being present in the bots.

Similar cyber activities include the 2008 cyberattacks in Lithuania after the government outlawed the display of Soviet symbols, resulting in Russian hackers defacing the government through hammers-–and–-sickles and five-pointed stars—all soviet symbols—on webpages [8]. Additional examples include the 2008 DDoS cyberattack in Georgia [9] and the 2009 DDoS cyberattack in Kyrgyzstan [8].

1.2 Recent Developments

Through a more modern turn of events, state-sponsored cyberattacks have become a major strategy in warfare—especially visible through the Russia–Ukraine war. In 2015, a Russian attack on Ukraine's power grid resulted in a blackout for 250,00 Ukrainians [10]. In 2022, hackers connected to the Russian GRU hacking group launched a campaign that targeted the energy sector and logistics industries in Ukraine and Poland. Then again, in 2023, Russian hackers disrupted services for Kyivstar—Ukraine's largest mobile phone provider—which compromised not just civilian servers but also those connecting Ukrainian President Zelenskyy and then U.S. President Joe Biden [11].

However, the main concern regarding cyberattacks stems beyond warfare. It concerns the very livelihood of a nation's citizens. In 2020, it was reported that 40% of analyzed state-sponsored incidents involved attacks on both physical and digital components which included power plants and waste management systems [12].

Recently though, a brand new set of capabilities has gone on the rise: Artificial Intellegence. Shadow AI—unsanctioned AI models without proper governance have emerged as a significant threat to enterprises worldwide [13]. With the rise of AI, a brand new double-edged sword has risen to the surface, a tool that can be used both for more sophisticated cyberattacks as well as better threat detection and response times in combatting cyberattacks [14].

Key Terms

State-Sponsored Cyber Attacks – Cyber attacks carried out or supported by a nation-state
Distributed Denial of Service (DDoS) – An attack made to disrupt the normal traffic of a server by flooding it with internet traffic.
Critical Infrastructure – Assets, systems, facilities, and networks vital for the functioning of society.

Hybrid Warfare – The use of both conventional and unconventional acts of combat through the spreading of false information, or attacking important computer systems on top of traditional combat tactics.

Advanced Persistent Threat (ATP) – A prolonged and targeted cyber-attack where attackers gain unauthorized access to a for an extended period.

Cyber Espionage – The act of using technological means to gain access to confidential information.

Zero-Day Exploit – A cyberattack conducted by taking advantage of cybersecurity flaws unknown to the vendor.

2. Emphasis of the Discourse

It is important to start off with the note that nearly no nation is built up of exclusively right or left-wing policies and approaches, instead, countries make decisions based on a mixture of both sides—it is the formation and balance of this mixture that makes a nation lean left or right.

2.1 Right-Wing Approach

Emphasis on national sovereignty: Prioritizing national security and sovereignty over regional cooperation, right-winged parties tend to opt for stricter border controls on data, enhanced national defense mechanisms, and cyber retaliation capabilities to deter state-sponsored cyber-attacks.

Focus on national security: Generally seen as the more aggressive party, a right-winged government may be more willing to support offensive cyber capabilities to retaliate against or deter state-sponsored cyber-attacks [3].

Private sector leadership: Right-winged governments may advocate for private companies to take on the role of developing cyber defense solutions [4].

Risks: Given the clear and aggressive nature of the right-winged approach, it is unsurprising that there is the risk of heightening tensions and escalating conflicts with cyber-attackers.

2.2 Left-Wing Approach

Global cooperation: Left-wing parties tend to focus more on approaching the matter through global cooperation using intergovernmental organizations such as NATO, the EU, and the UN by passing new bills, resolutions, and treaties [4].

Focus on regulation and standards: Left-leaning policies show greater emphasis on government intervention in monitoring consumer data with the goal of enforcing cybersecurity standards across organizations [5].

Protection of civil liberties: The nature of the left-winged parties adds gravitas in ensuring the rights of citizens are not infringed upon during the monitorization.

Risks: Given the nature of the left-winged policies requiring a lot more external involvement, it brings additional security risks by the involvement of outside parties while also making it less time efficient as nations will have to reach consensus.

2.3 Stance of Intergovernmental Organizations

NATO: The stance of NATO has been very clear. They've focused on emphasizing the significance of addressing the hybrid threats in the Baltic Sea region, especially given the increased activities from Russia such as GPS jamming and sabotaging critical undersea infrastructure [5]. The alliance has also committed to enhancing its military presence in response to such threats, recognizing the Baltic Sea as a strategic area for collective defense. So far, NATO's efforts have included improving surveillance and situational awareness, as well as fostering cooperation through initiatives like the European Centre for Excellence for Countering Hybrid Threats [7] which promotes information sharing and training among member states to counteract hybrid threats effectively [6].

European Union (EU): The EU has spearheaded efforts to heighten cybersecurity across its member states through ENISA, the European Union Agency for Cybersecurity. Through the ENISA Cyber Security Act, the EU has drafted a number of cybersecurity policies and certification frameworks for products and services that have enhanced public trust in digital products and services [3]. Additionally, the EU has also established the Joint Cyber Unit (JCU) which has served to assist ENISA. Together, ENISA and the JCU have set physical platforms for certification offices in Brussels; established virtual platforms with tools for secure and rapid information-sharing; delivered the EU cybersecurity incident and crisis response plan based on national plans proposed in NIS2; produced EU cybersecurity reports using information and

intelligence regarding threats and incidents; established and mobilized EU Cybersecurity Rapid Reaction Teams; put an end to information sharing and operational cooperation agreements with private sector companies, both for users and providers of cybersecurity services; created enhanced detection capability tools, most notably SOCs; and set multi-annual plans to coordinate exercises and organize joint cybersecurity exercise and training [3].

United Nations (UN): The United Nations has undertaken a number of initiatives to take measures to address state-sponsored cyberattacks. However, it is yet to pass a resolution regarding state-sponsored cyberattacks in the Baltic Sea specifically. Resolutions addressing the general issue of cyber-based threats include resolution 2341, a resolution that included cyber defense as counter-terror measures; resolution 70/237, a resolution that placed partial responsibility for cyberattacks on member states; resolution 73/27, a resolution that adapted international law to apply to cyberspace; resolution 75/240, a resolution that mandated the protection of critical infrastructure from malware; resolution 76/19, a resolution that negotiated capacity-building, confidence-building measures, and regular dialogue on how international law applies to State cyber activity.

Baltic Sea Security Initiative (BSSI): The Baltic Sea Security Initiative (BSSI), consisting of nations such as Poland, Estonia, Latvia, Lithuania, Germany, and Denmark, is a collaborative effort aimed at enhancing cybersecurity and resilience in the Baltic Sea region.

2.4 Stance of Developed Countries

As the nations that tend to be at the forefront of cybersecurity, developed countries have created a number of regional policies and shaped global norms. Historically, developed countries were motivated by the need to protect their own critical infrastructure in order to maintain economic stability due to their vital roles in cyberspace; the want to assert strategic and technological dominance in the realm of cybersecurity has also been a big motivator that was only available for developed countries.

The main differences across the approach to cybersecurity among developed nations can be seen when comparing the U.S. with EU member states. The U.S. has historically favored offensive cyber capabilities whereas European nations tended to prefer setting regulations and global frameworks. This contrast stems from the different values of the developed sides. The U.S. views cybersecurity as a national security issue, focusing on protecting critical infrastructure from state-sponsored attacks. However, Europe has made it clear on their emphasis on protecting user

privacy and data rights. This focus on user privacy has been reflected through regulations such as the General Data Protection Regulation (GDPR).

2.5 Stance of Developing Countries

As nations that often lack the resources to build robust cybersecurity infrastructure, developing countries face many challenges in cyber threats due to their often outdated technology and limited expertise. As a result, these regions have seen a 32% increase in cyberattacks on financial institutions over the past year. As such, they have become increasingly dependent on the support of developed nations to swiften innovations in cybersecurity.

Historically, developing nations around the Baltic Sea region such as Estonia, Latvia, and Lithuania have been subject to a number of cyberattacks. One of the most well-documented was the 2007 cyberattack on Estonia, where after Estonia's decision to relocate the Bronze Solider—a Soviet-era ware memorial—Estonia became the victim of cyberattacks predominantly involving DDoS techniques. Although Russia has denied all involvement in the attack, the Estonian government traced the attacks to Russian language sources and suggested Russian state sponsorship. As a result of the attack, Estonia experienced significant disruption to online services which went as far as to impact banking operations and government communications. Since then, Estonia has strengthened its cybersecurity capabilities through enhancing collaboration with NATO and EU partners—mostly composed of developed nations.

3. Possible Solutions

3.1 In Favor of Developed Countries

As nations that want to assert global dominance in the realm of cybersecurity technology, developed nations would most favor solutions that expand their control over the global landscape of cyber-infrastructure. With most of the developed nations relating to the issue having a form of connection with the EU or NATO, developed countries gain the biggest advantage by enhancing cooperation in cyber security defense.

Thus, a solution in favor of developed countries would include setting robust regulatory frameworks and standards across industries while training developing countries with widespread adoption and education on these new sets of regulatory frameworks.

3.2 In Favor of Developing Countries

As developing countries face more complex and layered challenges in improving their cybersecurity due to a combination of technological reliance, lack of awareness, limited resources, vulnerable infrastructure, and less sophisticated regulations, developing nations would need a solution that puts a lesser financial burden on them while still reaping the benefits of a sophisticated cyberinfrastructure [15].

The solutions to cyberattacks are quite universal—both developed and developing countries want greater layers of cyber defenses—developing countries can become a vulnerability for developed countries and developed countries have the technology and resources to support the growth of cyber-defense systems in developing countries [15].

4. Keep in Mind the Following

When researching about this topic keep in mind your country's involvement in this topic (have they been a victim or an aggressor), what geographical, political, or cultural stance regarding recent political campaigns they have recently followed, and how reliant or developed is the nation's technological capabilities. Below are a few questions to help guide your research:

1. *Country's Involvement*
    a. *Has your country been a victim of state-sponsored cyber-attacks? If so, what sectors were affected, and how has the country responded?*
    b. *Has your country been accused of sponsoring cyber-attacks? If so, what has the official response or justification been from your country?*
2. *Cyber-Defense Related Policies*
    a. *What national cybersecurity laws or frameworks does your country have in place?*
    b. *Have there been any recent initiatives or investments to strengthen your country's cybersecurity defenses?*
3. *Country's Stance on Baltic Cyberattacks*
    a. *How does your country perceive the role of the Baltics to be in terms of the stability of global cybersecurity?*
    b. *What historical or political relationships influence your country's stance on related nations?*
    c. *Is your country part of any major cybersecurity alliances, such as those relating to the NATO or EU frameworks?*
4. *Cyber-Infrastructure and Capabilities*

a. *How sophisticated is your nation's cybersecurity and defense sector?*
b. *Does your country have the economic capability to independently address cybersecurity challenges?*
c. *Is your country a leader in either developing or exporting cybersecurity technologies?*
d. *How well-educated is your country's public in user data protection and cybercrimes?*

5. Evaluation

The issue regarding state-sponsored cyberattacks in the Baltic Sea is a modern issue and something that has become an even greater threat with the rise of AI and society's dependence on social media. Achieving consensus on the matter will be difficult as cyber warfare will continue to become mainstream and increasingly important in the wars to follow. Thus, do not limit yourself to these solutions, as nations will ultimately break the very same rules they set. Instead, delegates are encouraged to solve the issue from its very roots—tensions that ultimately result in wars. In order to do so, it is essential that you delve into the convoluted roots of this issue and get a grasp of the entire picture. This will not be an easy task, but through careful cogitation, I am confident you will be able to unravel this intricate issue.

6. Bibliography

1. "European Union Agency for Cybersecurity | European Union." *European Union*, 2023, european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en. Accessed 13 Dec. 2024.
2. Jazeera, Al. "Estonia Repels Cyberattacks Claimed by Russian Hackers." *Al Jazeera*, 18 Aug. 2022, www.aljazeera.com/news/2022/8/18/estonia-says-it-repelled-cyber-attacks-claimed-by-russian-group. Accessed 29 Dec. 2024.
3. "Joint Cyber Unit." *Shaping Europe's Digital Future*, 26 Dec. 2024, digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit. Accessed 13 Dec. 2024.
4. NATO. "NATO to Enhance Military Presence in the Baltic Sea." *NATO*, 2024, www.nato.int/cps/en/natohq/news_231800.htm. Accessed 13 Dec. 2024.
5. "What to Expect from the NATO Summit for Baltic Sea Security." *Wilson Center*, 13 Dec. 2024, www.wilsoncenter.org/article/what-expect-nato-summit-baltic-sea-security. Accessed 13 Dec. 2024.

6. “Analysis of 2007 Cyber Attacks against Estonia: Information Warfare.” *Docslib*, 2017, docslib.org/doc/1138705/analysis-of-2007-cyber-attacks-against-estonia-information-warfare. Accessed 29 Dec. 2024.
7. *2007 Cyber Attacks on Estonia*, stratcomcoe.org/publications/download/cyber_attacks_estonia.pdf. Accessed 29 Dec. 2024.
8. Windrem, Robert. “Timeline: Ten Years of Russian Cyber Attacks on Other Nations.” *NBC News*, 18 Dec. 2016, www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111. Accessed 29 Dec. 2024.
9. “Russia Cyber Threat Overview and Advisories: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia. Accessed 30 Dec. 2024.
10. Euronews. “Estonia Hit by ‘Most Extensive’ Cyberattack since 2007 amid Tensions with Russia over Ukraine War.” *Yahoo News*, 18 Aug. 2022, uk.news.yahoo.com/estonia-hit-most-extensive-cyberattack-111107644.html?guccounter=1&guce_referrer=aHR0cHM6Ly9zdG9ybS5nZW5pZS5zdGFuZm9yZC5lZHUv&guce_referrer_sig=AQAAAB9DkIjQCRdd4Kkjoxd5Em3qzUVKb6Ym89HpEc2OKbBT46m-1PQcPhGuDG6pLXRceq3gMN9aU6wVGf74qBj1Fbyy3Aj9tHNZfUh7FlUqIhHf8lk4Y5xQkji4dDr1YEF9U93iuYvYkwfNEnAIKTon6cRL_29ACz6WgnL9J8Kt_OLZ. Accessed 29 Dec. 2024.
11. “Significant Cyber Incidents | Strategic Technologies Program | CSIS.” *Csis.org*, 2025, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 29 Dec. 2024.
12. Euronews. “Estonia Hit by ‘Most Extensive’ Cyberattack since 2007 amid Tensions with Russia over Ukraine War.” *Yahoo News*, 18 Aug. 2022, uk.news.yahoo.com/estonia-hit-most-extensive-cyberattack-111107644.html. Accessed 29 Dec. 2024.
13. “5 Cybersecurity Trends for 2025: Preparing for a Year of Elevated Risk and Accountability | Bitsight.” *Bitsight*, 2025, www.bitsight.com/blog/5-cybersecurity-trends-2025-preparing-year-elevated-risk-and-accountability. Accessed 29 Dec. 2024.
14. Poremba, Sue. “Cybersecurity Trends: IBM’s Predictions for 2025.” *Security Intelligence*, 9 Dec. 2024, securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2025/. Accessed 29 Dec. 2024.
15. Tuhu Nugraha. “Strengthening Cyber Defences in Developing Countries: Offensive and Adversarial AI Threats.” *Modern Diplomacy*, 15 July 2024,

moderndiplomacy.eu/2024/07/15/strengthening-cyber-defences-in-developing-countries-offensive-and-adversarial-ai-threats/. Accessed 29 Dec. 2024.

16. *Seventy-Sixth Session Agenda Item 95 Developments in the Field of Information and Telecommunications in the Context of International Security Resolution Adopted by the General Assembly on 6 December 2021 Developments in the Field of Information and Telecommunications in the Context of International Security, and Advancing Responsible State Behaviour in the Use of Information and Communications Technologies*. documents.un.org/doc/undoc/gen/n21/377/48/pdf/n2137748.pdf.
17. *A/RES/75/240 - General Assembly - the United Nations*, documents.un.org/doc/undoc/gen/n21/000/25/pdf/n2100025.pdf. Accessed 29 Dec. 2024.
18. *Resolution Adopted by the General Assembly on 5 December 2018*. 2018, documents.un.org/doc/undoc/gen/n18/418/04/pdf/n1841804.pdf.
19. IBM. "Critical Infrastructure." *Ibm.com*, 5 July 2023, www.ibm.com/think/topics/critical-infrastructure. Accessed 29 Dec. 2024.
20. "NATO Review - Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." *NATO Review*, 30 Nov. 2021, www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html. Accessed 29 Dec. 2024.
21. Cambridge Dictionary. "Hybrid Warfare." *@CambridgeWords*, 29 Dec. 2024, dictionary.cambridge.org/dictionary/english/hybrid-warfare. Accessed 29 Dec. 2024.
22. "What Is an Advanced Persistent Threat (APT)? | CrowdStrike." *Crowdstrike.com*, 2024, www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/. Accessed 29 Dec. 2024.
23. Falch, Morten, et al. "Cybersecurity Strategies for SMEs in the Nordic Baltic Region." *Journal of Cyber Security and Mobility*, Jan. 2023, https://doi.org/10.13052/jcsm2245-1439.1161. Accessed 3 Mar. 2023.
24. "Cybersecurity Policies | ENISA." *Europa.eu*, 2016, www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies. Accessed 29 Dec. 2024.
25. "NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems." *Shaping Europe's Digital Future*, 15 Dec. 2024, digital-strategy.ec.europa.eu/en/policies/nis2-directive. Accessed 29 Dec. 2024.
26. "European Parliament Plenary Debate: Need to Detect and to Counter Sabotage by the Russian Shadow Fleet, Damaging Critical Undersea Infrastructure in the Baltic Sea." *European Commission - European Commission*, 2025, ec.europa.eu/commission/presscorner/detail/en/speech_25_312. Accessed 29 Dec. 2024.
27. "Digital Breakthroughs Must Serve Betterment of People, Planet, Speakers Tell Security Council during Day-Long Debate on Evolving Cyberspace Threats | Meetings Coverage

and Press Releases." *Un.org*, 20 June 2024, press.un.org/en/2024/sc15738.doc.htm. Accessed 29 Dec. 2024.

28. "Document Viewer." *Un.org*, 2025, docs.un.org/en/S/RES/2341(2017). Accessed 29 Dec. 2024.
29. *CTED TRENDS REPORT PHYSICAL PROTECTION of CRITICAL INFRASTRUCTURE against TERRORIST ATTACKS*. 2017, www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted-trends-report-march-2017-final.pdf. Accessed 29 Dec. 2024.
30. General, Distr. *Security Council*. 2001, p. 2322, documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf.
31. *A/RES/70/237 General Assembly*. documents.un.org/doc/undoc/gen/n15/457/57/pdf/n1545757.pdf.
32. R-NE-2, Don. "H.R.2922 - 118th Congress (2023-2024): Baltic Security Initiative Act." *Congress.gov*, 2023, www.congress.gov/bill/118th-congress/house-bill/2922#:~:text=The%20goals%20of%20this%20initiative,systems%20and%20integrated%20air%20and. Accessed 29 Dec. 2024.
33. "Zero-Day Vulnerability - Definition | Trend Micro (US)." *Trendmicro.com*, 2025, www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability. Accessed 29 Dec. 2024.