Reviewing NATO's cyber defence strategy

Committee: NATO

Student Officer: Harry Kelly

Forum: North Atlantic Treaty Organization

Issue: Reviewing NATO's cyber defence strategy

Name: Harry Kelly

Position: Head Chair of NATO

Introduction

The North Atlantic Treaty Organization (NATO) is an international political and military alliance between thirty (30) countries across North America and Europe. Established in 1949, NATO's primary focus is to "*guarantee the freedom and security of its members through political and military means.*"

Its founding members consist of Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, United Kingdom, and the United States. That said, it is important to note that being a member of NATO does not equate to being a member of the European Union (EU); these two groups have similar interests and values, overlapping members, and close interconnectedness, however are two separate entities.

Cybersecurity has become an increasingly important part of modern life. As technology develops, it is becoming easier for criminals to access sensitive information, steal identities, and cause financial damage. By implementing effective cybersecurity measures, businesses, organisations, institutions and individuals can protect themselves from cyber threats and minimise the risk of data breaches, financial losses, and other malicious activities. Cybersecurity also helps protect against data loss, which can be devastating to a business or individual. This is critical to keeping online information safe, secure, and private, and is essential to protecting businesses, governments, and individuals from cyber threats.

Cyber defence is a key component of cybersecurity within an institution/organisation. In a continuously developing and dynamic digital world, the protection of databases, communication infrastructure and information systems is arguably as, if not more important than the physical, non digital equivalents. This would incorporate measures - such as authentication or intrusion detection systems that combat

varying levels or cyber attacks, whether it be espionage, sabotage, economic disruption, etc. Furthermore, cyber defence can help reduce the risk of data loss due to malicious attacks. It can also reduce the risk of data being stolen or corrupted due to unauthorised access. In addition, cyber defence can help organisations comply with industry regulations and standards such as the Payment Card Industry Data Security Standard (PCI DSS). It can also help organisations meet the requirements of data privacy laws.

Definition of Key Terms

Armed attack

An armed attack is an offensive military action or encounter between two or more hostile forces in which at least one side uses weapons or force to cause or threaten injury, death, or destruction.

Cyber defence

Cyber defence is the practice of defending computer networks, systems, and data from malicious cyber attacks. It includes the implementation of security measures such as firewalls, antivirus software, and intrusion detection systems to protect networks from unauthorised access and malicious activities. It also includes strategies for responding to and recovering from cyber attacks.

Cybersecurity

Cybersecurity is the practice of protecting networks, systems, and programs from digital attacks. These attacks are usually aimed at assessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes. Cybersecurity technologies are used to detect and prevent cyberattacks, protect against unauthorised access to networks and data, and defend against malicious code.

Cyberspace

Cyberspace is an interconnected network of computers, computer networks, and the information and communication systems that connect them. It exists in an abstract, virtual space that can be accessed and navigated through the use of computers and other digital technology.

Cyber terrorism

Cyber terrorism is the use of computer networks to cause disruption or fear in order to achieve a political or ideological goal. It typically includes the use of malicious software, such as viruses or worms, to damage or disable computer systems and networks, or the threat of such actions. It may also include attacks on websites, networks, or other online infrastructure, as well as attacks on physical infrastructure such as power grids or dams.

Cyber threat

Cyber threats are any type of malicious attack or security breach that targets an organisation's digital assets and/or computer systems. These threats can come in many forms, including phishing scams, malware, viruses, ransomware, and other forms of malicious software. Cyber threats are a growing concern for businesses and individuals alike, as they can lead to data breaches, financial losses, and other serious damages.

Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) is a type of cyber attack that involves sending a large number of requests to a server or network in order to overwhelm it and cause it to crash or become inaccessible. DDoS attacks can be launched from multiple locations and devices and are typically difficult to detect and mitigate.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The standard was created by the Payment Card Industry Security Standards Council and is managed by the major payment brands such as Visa, MasterCard, American Express, Discover, and JCB. PCI DSS requires companies to maintain an information security management system and adhere to its 12 main requirements, which include:

1. Maintain a secure network

2. Protect cardholder data

3. Maintain a vulnerability management program

General Overview

NATO's Cyber Defence Strategy

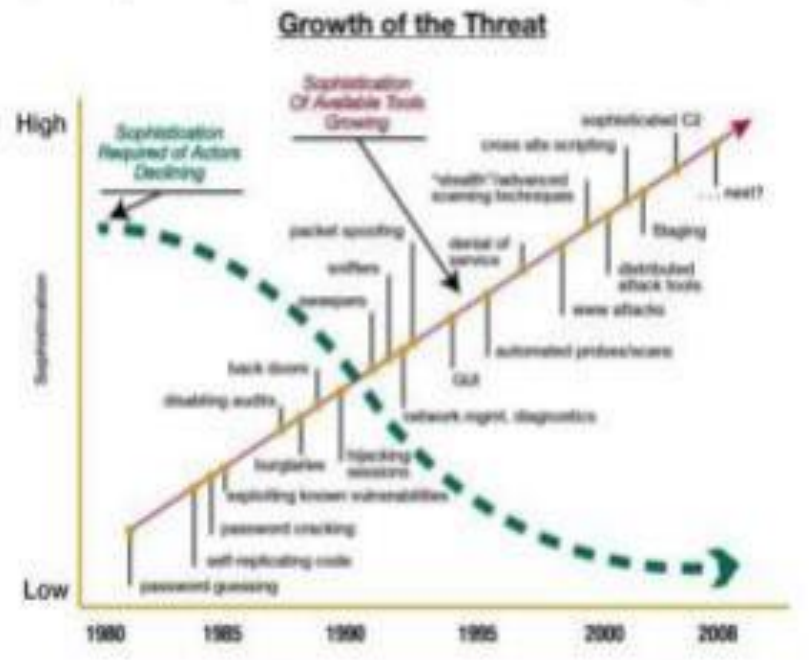
The NATO Alliance has seen a rise in complex, damaging, and coercive cyber threats to the security. The North Atlantic Treaty Organization continually adjusts to the changing cyber threat environment, in order to carry out the key missions of the Alliance: collective defence; crisis management; and cooperative security. For such a digitally powerful group, it is imperative that NATO is ready to defend its operations and networks from the increasingly sophisticated cyberthreats it encounters (**Fig. 1**).

The NATO Summit in Wales (2014) resulted in the adoption of an improved strategy and plan of action that were supported by Allies in order to keep up with the quickly evolving threat picture and maintain strong cybersecurity measures. (**https://www.nato.int/cps/en/natohq/ topics_78170.htm**). The 2014 policy confirmed the application of international law in cyberspace, outlined the further development of NATO and Allies' capabilities, and strengthened NATO's cooperation with industry. It also established that cyber defence is a component of the Alliance's primary task of collective defence. The new comprehensive

Cyber Defence Policy,

which supports NATO's three main objectives, as well as its overall deterrence and defence posture, was approved by allies at the 2021 NATO Summit in Brussels. The defensive nature of NATO's mission was reinforced, and allies agreed to use their complete arsenal of tools to thwart, defend against, and fight the full range of cyber threats at all times. Responses m u s t b e c r g c i

Fig. 1: *The speed and sophistication of cyber attacks have been increasing over time.*



North Atlantic Treaty Organization (2016). NATO Review - NATO: changing gear on cyber defence. [online] NATO Review. Available at: https://www.nato.int/docu/review/articles/2016/06/06/nato-changing-gear-on-cyber-defence/index.html [Accessed 28 Dec. 2022].

ng and include all of the political, diplomatic, and military options in the NATO toolkit.

Allies also acknowledged that, under some conditions, the impact of considerable harmful cumulative cyber activity may be regarded as an armed attack. Because of the nature of cyberspace, a comprehensive strategy involving cooperation at the political, military, and technical levels is required; activities at all three levels were advanced by the 2021 policy and its related action plan.

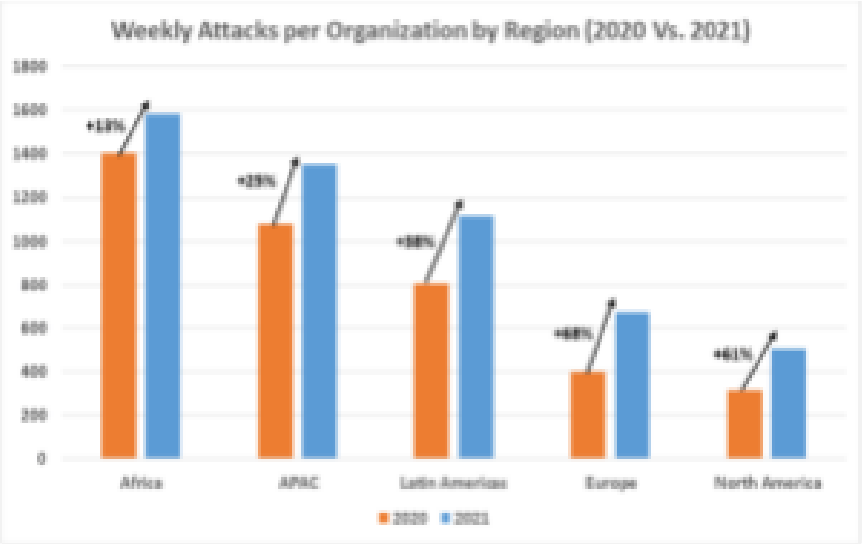
Simply put, there are two main facets to NATO's responsibility in cyber defence. As agreed by allies at the NATO Summit in Wales in 2014, protecting its own networks is the first concern. Given the Alliance's extensive presence across several locations and operating facilities, this is a difficult task. In carrying out this aspect of its cyber defence responsibilities, NATO is responsible for making sure that the communication and information systems the Alliance depends on for its operations and missions are secure against attacks coming from the internet.

Cyber Threats

The number of governments that view cyber capabilities as legitimate and essential components of their arsenal of strategic tools alongside diplomacy, economic strength, and military force has increased significantly. This raises questions about whether a full-fledged cyberwar between governments will be seen very soon. Additionally, there is sporadic interest in the use of cyber capabilities by non-state parties, albeit there is little proof of this at the moment (https:// www.nato.int/docu/review/articles/2016/06/08/nato changing-gear-on-cyber-defence/index.html).

One of the biggest obstacles to NATO recognizing its own role in cyber defence is the variety of ways that cyber capabilities might be deployed. When analysing NATO's position on the cyber arena, two primary forms of attack are especially pertinent. First, whether at the strategic or operational level, cyber-enabled espionage has the potential to violate the security of information and information systems, possibly disclosing critical information to enemies.

Figure 2: *Weekly Cyber Attacks per Organization by Region*



Check Point (2022). Check Point Research: Cyber Attacks Increased 50% Year-over-Year. [online] Check Point Software. Available at: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ [Accessed 29 Dec. 2022].

Second, cyber-enabled sabotage can have significant physical effects (**https://www.nato.int/docu/review/articles/2016/06/08/nato-changing-gear-on cyber-defence/index.html**), particularly when energy or transportation networks are attacked, or when data is modified to throw the target off guard and impair command and control decision-making.

Additionally, extortion or fraud for financial gain, or as a first step in the aforementioned attacks, can be used to target NATO workers at all levels and in all departments, and moreover, the complexity of operational security in cyberspace is further exacerbated by the prevalence of social media and the Internet on mobile devices.

Reviewing NATO's Cyber Defence Strategy

Regular reviews and revisions are made to the Strategic Concept. These often come in the form of international summits, followed by a reform to the current system in place and/or accompanied by (annual) reports, such as that of 2017 or 2021 (**https://www.nato.int/cps/en/ natohq/79511.htm**). It has been modified approximately every decade (https://www.nato.int/ strategic-concept/) since the end of the Cold War to reflect changes in the world's security environment and to make sure the Alliance is ready for the future.

NATO's Lisbon Summit in 2010 saw the adoption of the prior strategic concept. The revised Strategic Concept outlines the Alliance's new security reality, restates NATO's core principles, and outlines NATO's primary goal of ensuring the Allies' collective defence (https://www.nato.int/ strategic-concept/).

Each Ally has a personal obligation to maintain and enhance both individual and collective ability to counter cyberattacks in compliance with NATO's Article 3. The NATO Defence Planning Process
(NDPP) addresses this individual duty at the NATO level (**https://www.nato pa.int/download-file? filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev. %201%20fin%20%20- %20NATO%20IN%20THE%20CYBER%20AGE.pdf**).

Each ally establishes national planning targets under the NDPP, and the other allied nations periodically assess each ally's compliance with its mandates and goals. In 2013, the initial Cyber Defense Capability Targets were established. They included goals for cyber defence governance, NATO network response capabilities, and education and training initiatives (https://www.nato-pa.int/ download-file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev. %201%20fin%20%20- %20NATO%20IN%20THE%20CYBER%20AGE.pdf).

The 2016 Warsaw Summit saw Allies agree that it was now a top priority to strengthen the cybersecurity measures of national networks and infrastructure. They, therefore, opted into a Cyber Defence Pledge to improve capabilities development as an addition to the regular

NDPP process.

Member governments agreed to carry out yearly self-assessments and increase their cyber resilience and response capacity as part of the Pledge (https://www.nato pa.int/download-file? filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev. %201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf). Therefore, seven key goals must be pursued by allies (NATO, 2016a):

"I. Develop the fullest range of capabilities to defend our national infrastructures and networks […];

II. Allocate adequate resources nationally to strengthen our cyber defence capabilities; III. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen cooperation and the exchange of best practices;

IV. Improve our understanding of cyber threats, including the sharing of information and assessments;

V. Enhance skills and awareness, among all defence stakeholders at the national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences; VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;

VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends."

Timeline of Key Events

NATO's history is of great importance because it has been a major force in the preservation of peace and stability in Europe and the wider world. NATO was formed in 1949 as an alliance in order to counter the threat of Soviet aggression in Europe. Since then, it has grown to include 30 member states and has played an important role in preserving peace and stability in Europe, combating (cyber)terrorism, and providing humanitarian assistance around the world. NATO's history also serves as a reminder of the need for international cooperation and collective action to address global security threats. The timeline presented draws on information sourced

from

- https://www.reuters.com/article/us-nato-summit-history idUSL3151283520080331 ● https://www.govtech.com/blogs/lohrmann-on cybersecurity/nato-countries-hit-with unprecedented-cyber-attacks
- https://em360tech.com/top-10/top-10-most-notorious-cyber-attacks-history ● https://www.nato.int/nato-welcome/

Date Event

April 4th, 1949 NATO is founded in Washington D.C, United States.

1952 Greece and Türkiye join NATO.

May 6th, 1955 Germany joins NATO.

May 14th, 1955 Warsaw Pact is formed between the USSR and others.

1982 Spain joins NATO.

December 26th, 1991 USSR dissolves; Warsaw Pact alliance eventually disbands.

December 16th, 1995 NATO launches military operation in support of Bosnia.

1999 Czechia, Hungary and Poland join NATO.

1999 Melissa Virus is first warning of cyber threat in a new technological era.

September 11th, 2001 NATO invokes Article 5 after terror attacks on the U.S.

2004 Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, Slovenia join NATO.

2007 Estonia falls victim to approximately sixty (60) cyber attacks.

April 1st, 2009 Albania and Croatia join NATO.

June 5th, 2017 Montenegro joins NATO.

March 27th, 2020 North Macedonia joins NATO.

September, 2022 Montenegro and Estonia are hit by cyber attacks.

Major Parties Involved

North Atlantic Treaty Organization (NATO)

In recent years, NATO has placed an increased focus on cybersecurity due to the growing threat from cyber-attacks. NATO has established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. The Centre focuses on research and development, training and education, as well as policy development and analysis (https://ccdcoe.org/).

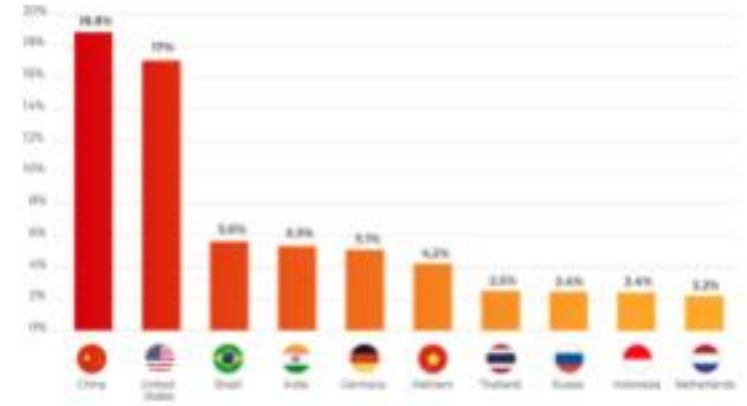
The CCDCOE is also responsible for developing strategies for the defence of NATO networks and information systems. NATO has also established the NATO Cyber Defence Pledge, which is an agreement between member states to contribute to the cyber defence of NATO networks and information systems (https://www.nato.int/cps/en/natohq/official_texts_133177.htm). The Pledge also commits member states to cooperate in the development of cyber defence capabilities and to support the sharing of best practices.

In addition, NATO has implemented the Cyber Coalition Exercise, which is an annual event held at the CCDCOE (https://mil.ee/en/landforces/ccdcoe/). The exercise is designed to simulate a cyber attack on NATO networks and information systems, and involve the participation of member states, industry partners, and other stakeholders. The exercise is used to evaluate the effectiveness of the member states' cybersecurity capabilities and to identify areas for improvement.

People's Republic of China (China)

China has been accused by the U.S and other Western countries of launching cyber attacks against their networks and systems (https://apnews.com/article/technology business-china hacking-6cd7d59f1b6aa4a0539d987e5340b705). China has denied these allegations, but there have been reports of malicious cyber activity originating from China. In response to these allegations, the US has taken a number of steps to strengthen its cybersecurity, such as imposing sanctions on Chinese companies and individuals linked to cyber espionage. As a matter of fact, both China and the U.S are reported to be the most common sources of cyber maliciousness, respectively (**Fig. 3**) (https://www.govtech.com/security/hacking-top-ten.html). The US and other countries have also called on China to engage in meaningful dialogue on cybersecurity issues.

Fig. 3: *Highest 10 Countries of Origin for Cyber Attacks*



DavidPuc, N. (n.d.). Which Countries are Most Dangerous? Cyber Attack Origin – by Country. [online] blog.cyberproof.com. Available at: https://blog.cyberproof.com/blog/which-countries-are-most-dangerous [Accessed 30 Dec. 2022].

United States of America (U.S)

US cyber-attacks can take many forms, including malware or virus infections, phishing and social engineering attacks, distributed denial of service (DDoS) attacks, and state-sponsored cyber espionage and sabotage (https://www.csis.org/programs/strategic-technologies program/significant cyber-incidents, https://www.globaltimes.cn/page/202209/1274627.shtml). The US government is known to have used cyber attacks against other countries, such as Iran and North Korea (https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war), as well as against adversaries like ISIS. US agencies such as the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and the Department of Homeland Security (DHS) work to protect U.S citizens and government systems from cyber attacks. They also work to identify and prosecute those who perpetrate cybercrimes, as is the country's responsibility and role as [the most powerful] member of NATO.

Republic of Estonia (Estonia)

In 2007, Estonia was the victim of a series of cyber attacks (https://em360tech.com/ top-10/top-10-most-notorious-cyber-attacks-history), which were believed to have been conducted by individuals in Russia (which they denied, 2008). The attacks targeted websites belonging to the government, banks, newspapers, and other organisations, and caused outages and disruptions for months. The Estonian government responded to the attacks by increasing its cybersecurity measures, as well as by appealing to

the international community for assistance. In addition, Estonia and other Nordic states referred the incident to the United Nations Security Council. The CCDCOE is also based in Estonia's capital city, Tallinn.

Possible Solutions

Incident response team

A potential step forward would be for NATO to create an incident response team composed of experts from each member state to coordinate its response to cyber attacks. This team should be responsible for monitoring threats, developing strategies to respond to them, and coordinating the response. It would be the responsibility of the delegates to discuss who this team would comprise of, and its precise function, however could prove to be an invaluable asset alongside NATO, the United Nations (UN), and other already established parties.

It is important to note that NATO has already established plans to materialise instant response capabilities in this field (https://www.infosecurity magazine.com/news/nato-rapid-cyber response/ #:~:text=NATO%20has%20announced%20plans%20to,Madrid%2C%20Spain%2C%20last% 2 0week), however this idea could potentially be furthered and/or built upon.

Improving information sharing

When contemplating solutions, delegates may also look to encourage enhanced information sharing between member states in order to better identify and respond to cyber threats. This should include the sharing of threat intelligence, best practices, and information on how to respond to cyber-attacks. As with any issue, fluid multilateral cooperation and collaboration between member states are often what is most crucial to come to an appropriate and sufficient consensus on the resolution to an issue. As the digital age in which we live continues to grow, so do the threats to cybersecurity within the newfound battlefield of digital cyberspace, and hence the ever-present need to revise, consider, and improve our defence strategies and counter capabilities to these threats.

Bibliography

Check Point. “Check Point Research: Cyber Attacks Increased 50% Year over Year.” *Check Point Software*, 10 Jan. 2022, blog.checkpoint.com/2022/01/10/check-point research-cyber attacks-increased-50-year-over-year/.

Coker, James. “NATO to Develop Rapid Cyber Response Capabilities.” *Infosecurity Magazine*, 4 July 2022, www.infosecurity-magazine.com/news/nato-rapid-cyber response/ #:~:text=NATO%20has%20announced%20plans%20to.

CSIS. “Significant Cyber Incidents | Center for Strategic and International Studies.” *Www.csis.org*, 2022, www.csis.org/programs/strategic-technologies program/significant cyber-incidents.

DavidPur, Niv. “Which Countries Are Most Dangerous? Cyber Attack Origin – by Country.” *Blog.cyberproof.com*, blog.cyberproof.com/blog/which-countries-are most-dangerous. Accessed 30 Dec. 2022.

Davis, Susan. *SCIENCE and TECHNOLOGY COMMITTEE (STC) NATO in the CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE General Report*. 2019, www.nato-pa.int/download file?filename=/sites/default/files/2019-10/

REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-

%20NATO%20IN%20THE%20CYBER%20AGE.pdf.

Hanna, Andrew. “The Invisible U.S.-Iran Cyber War.” *Usip.org*, 2019,

iranprimer.usip.org/blog/ 2019/oct/25/invisible-us-iran-cyber-war.

Harris, Matt. “Top 10 Most Notorious Cyber Attacks in History | EM360.” *Em360tech.com*, 22 Sept. 2022, em360tech.com/top-10/top-10-most-notorious cyber-attacks-history.

Imperva. “What Is Cyber Warfare | Types, Examples & Mitigation | Imperva.”

Learning Center, 2022, www.imperva.com/learn/application-security/cyber warfare/. Knell, Knoelle. “Top 10 Countries Where Cyber Attacks Originate.”

GovTech, 23 Apr. 2013, www.govtech.com/security/hacking-top-ten.html.

Lohrmann, Dan. “NATO Countries Hit with Unprecedented Cyber Attacks.” *GovTech*, 4 Sept. 2022, www.govtech.com/blogs/lohrmann-on cybersecurity/nato-countries-hit-with unprecedented-cyber-attacks. McDonald, Joe. “China Rejects Hacking Charges, Accuses US of Cyberspying.” *AP NEWS*, 20 July 2021, apnews.com/article/technology-business-china hacking-6cd7d59f1b6aa4a0539d987e5340b705.

NATO. “Cyber Defence.” *NATO*, 23 Mar. 2022,

www.nato.int/cps/en/natohq/ topics_78170.htm.

---. “Cyber Defence Pledge.” *NATO*, 6 July 2016,

www.nato.int/cps/en/natohq/ official_texts_133177.htm.

---. “NATO 2022 Strategic Concept.” *NATO 2022 Strategic Concept*, 29 June 2022, www.nato.int/strategic-concept/.

---. “Publications.” *NATO*, 31 Mar. 2022,

www.nato.int/cps/en/natohq/79511.htm. ---. “Relations with the European

Union.” *NATO*, 2022, www.nato.int/cps/en/natohq/ topics_49217.htm. ---.

“What Is NATO?” *NATO*, www.nato.int/nato-welcome/index.html.

“NATO Cooperative Cyber Defence Centre of Excellence.” *Estonian Defence Forces*, 30 Mar. 2022, mil.ee/en/landforces/ccdcoe/.

NATO Cooperative Cyber Defence Centres Of Excellence. “CCDCOE - the NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise.” *Ccdcoe.org*, 2019, ccdcoe.org/.

North Atlantic Treaty Organization. *NATO Cyber Defence*. 2016, www.nato.int/ nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-

factsheet-cyber defence en.pdf.

---. “NATO Review - NATO: Changing Gear on Cyber Defence.” *NATO Review*, 8 June 2016, www.nato.int/docu/review/articles/2016/06/08/nato-changing gear-on-cyber-defence/ index.html.

---. *North Atlantic Treaty Organization Www.nato.int/Factsheets Factsheet NATO Cyber Defence*. 2021, www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet cyber defence-en.pdf.

Singh, Jas. “Cyber Security vs Cyber Defense: Know the Difference?” *Cyber Security Kings*, 2022, cybersecuritykings.com/2020/04/21/what-role-do-cyber-security and-cyber-defense play-in-keeping-your-online-data-safe/.

Siwei, Zhao. “Exclusive: Evidence Shows US’ NSA behind Attack on Email System of Leading Chinese Aviation University - Global Times.” *Www.globaltimes.cn*, 5 Sept. 2022, www.globaltimes.cn/page/202209/1274627.shtml.

Staff, Reuters. “Timeline of Key Events in NATO’s 59-Year History.” *Reuters*, 31 Mar. 2008, www.reuters.com/article/us-nato-summit-history-idUSL3151283520080331.

STRATEGIC FORESIGHT ANALYSIS 2017 REPORT NATO UNCLASSIFIED -PUBLICLY DISCLOSED. 2018, www.act.nato.int/application/files/1016/0565/9725/171004_sfa_2017_report_hr. p df. *The Secretary General’s*. Mar. 2022, www.nato.int/nato_static_fl2014/assets/pdf/2022/3/ pdf/sgar21-en.pdf.

Zheng, Yu, et al. “Dynamic Defenses in Cyber Security: Techniques, Methods and Challenges.” *Digital Communications and Networks*, vol. 8, no. 4, July 2021, https://doi.org/10.1016/ j.dcan.2021.07.006.