North Atlantic Council

A Collective NATO Response to Disinformation Campaigns and Cyberattacks

Research Report

Leiden Model United Nations 2022

Fake news

Forum: *North Atlantic Council*

Issue: *A Collective NATO Response to Disinformation Campaigns and Cyberattacks*

Position: *Head Chair*

Introduction

Hybrid threats are an increasingly dangerous threat to the peace and security among North Atlantic Treaty Organisation (NATO) member states. Some of the most common threats include the employment of disinformation campaigns in combination with cyberattacks. NATO works hard to centralise its communications in order to dismantle disinformation while preventing cyberattacks. Disinformation and cyberattacks have been gaining attention steadily since the illegal annexation of the Crimean Peninsula in Ukraine by the Russian Federation and the subsequent disinformation spread by the Russian Federation in tandem with cyberattacks on Ukraine's infrastructure.

Definition of Key Terms

Disinformation:
Disinformation is false information that is covertly spread with the intention of creating or deepening division

Hybrid Tactics:
Hybrid tactics are the combined use of military and nonmilitary methods of warfare, as well as covert and overt means. This includes cyberattacks, disinformation campaigns, economic pressure, and various similar tactics

Forgeries:
Doctored letters, social media posts, or fake interviews, often of a low quality

Fake Personas:
The employed use of a single-use account on social media to share content and then be abandoned

Outreach:
Spoofed emails sent to NATO or other government and media organisations with the intention of provoking a response

Botnets:
A form of a denial of service attack (DDoS) that links various devices together to strengthen the blow of the attack significantly, overloading the system that is being targeted

General Overview

Disinformation

Disinformation seeks to create division, often between our NATO members. NATO has been dealing with disinformation campaigns since its founding, but has had to significantly increase its operations countering disinformation campaigns since the illegal Russian annexation of the Crimean Peninsula in Ukraine in 2014.

Both the 2018 Brussels Summit Declaration and the 2019 London Declaration solidified NATO members' commitment to countering disinformation aggressively, using methods that allow the organisation "to prepare for, deter, and defend against hybrid tactics that seek to undermine [its] security and societies". Hybrid tactics are at the core of this issue as disinformation campaigns are often paired with cyberattacks to worsen the blow to the victims of these crimes.

NATO approaches countering disinformation with a multifaceted approach that aims to 'understand' and 'engage'. The first part of this approach involves Information Environment Assessments that track relevant information to NATO operations and allows it to evaluate its communications. The latter half of the approach is where NATO tackles disinformation directly through the use of its external communications. NATO's approach to countering disinformation, like many areas of its operations, involves a heavy emphasis on collaboration between its members.

To understand NATO's approach to countering disinformation, it is important to understand the methods of disinformation used. Some of the forms of disinformation that NATO has encountered include forgeries, fake personas, and outreach. All of these techniques were used between April 21 and 22, 2020 as a part of coordinated disinformation campaigns that targeted Latvia, Lithuania, and Poland. The goal of these attacks was to spark division within NATO but were all disarmed by NATO before the campaigns reached mainstream media.

In Latvia, a phoney interview and an edited screenshot from a NATO battlegroup led by Canadians, were posted on Latvia's Facebook page. These posts claimed that the Canadian troops brought COVID-19 to Latvia. These claims were entirely false as there were quarantine measures in place to prevent this and as such, NATO was able to swiftly respond to this campaign.

In Lithuania, a forged letter addressed to the Lithuanian Defence Minister from the NATO Secretary-General claimed that NATO would withdraw troops from Lithuania due to a COVID-19 outbreak in the Lithuanian battlegroup. The letter was eventually sent to the NATO headquarters and combined with a false news story and a doctored video that were spread through fringe media outlets and blogs.

Poland saw a very similar disinformation campaign where a forged letter was laundered through blogs and media sites that appeared to be from a Polish Brigadier General to the Polish War Studies Academy that criticised a US-led military exercise as well as the presence of US troops in Poland. The letter was emailed to Polish media at a later point during the campaign by an address that appeared to be a former Member of the Polish Parliament.

NATO's 'engagement' strategy relies on their secure and fact-based network of communications. This strategy is its most effective tool to counter disinformation campaigns. It works to spread factual information while actively exposing and debunking disinformation to build resilience within global communities. NATO additionally translates a lot of its communications into several languages, predominantly English, French, Ukrainian, and Russian.

Cyberattacks

NATO's SPS Programme (Science for Peace and Security) is responsible for cyber defence including the protection of critical infrastructure, supporting cyber defence capabilities, and situational awareness of cyber threats. It is critical to keep in mind that NATO collectively affirms the application of international law in cyberspace.

NATO recognised in July 2016 that cyberspace is equally as important for defence as defence is on land, air, and sea. They also agreed to cooperate with the European Union on cyber defence that same year. The cooperation entails exchanging information, training, research, and collaborating on exercises.

NATO facilitates its cyber defence capabilities through the NATO Computer Incident Response Capability programme (NCIRC) which allows it to keep up with the growing threat of cyberattacks. Conducting training exercises is essential to its defence capabilities.

One instance of a NATO coordinated response to a cyberattack occurred as a result of mounting tensions between the Russian Federation and Estonia. A former Soviet country, Estonia planned to move a statue of a Soviet soldier that reminded the citizens of the nation of the more than 50 years of Soviet occupation in their country. They moved the statue from the centre of Tallinn, to a less visited part of the city on April 27th, 2007. The removal triggered Russian President Vladimir Putin to denounce this action and begin a widespread offensive of cyberattacks on Estonia.

Experts have been cautious to call this cyber-offensive a 'war' as the attack was very one-sided and was perpetrated through the use of botnets. Initially, the botnet attacks were aimed at government infrastructure, as well as Postimees Online, a well-known media outlet in Estonia. As a country that had heavily invested in hi-tech infrastructure, this attack was a surefire way of hitting Estonia where it hurt the most. Not only was banking nearly entirely online in Estonia, but so too were government systems, being described as "paperless" by Estonia's Defence Ministry's Head of Information Technology (IT), Mihkel Tammet.

As a response to this swift attack, Estonia reformed a task force that it had created initially to support its preparation for cyberattacks. The task force included security experts, police, intelligence service, and more parties. In this case what was notable was that the type of attack was one typically performed by low-level hackers, expected to be a weak attack. The attacks turned out to be difficult to combat and appeared to be masterminded by sophisticated hackers. Estonian IT experts later traced the attacks back to Russia, specifically to a computer within the Kremlin. NATO's response to the incident was conducting internal assessments on its infrastructure defences and furthering the development of its programme for cyber security.

Major Parties Involved

Russian Federation

Russia is one of the most infamous countries for cyber attacks and disinformation, with its various hybrid attacks in former Soviet countries such as Lithuania and Ukraine. Russia has been accused of cyber crimes and spreading disinformation in countries across the world, including other NATO member states. Russia regularly propagates disinformation in tandem with sophisticated cyber attacks.

European Union

The European Union works closely with NATO in regards to cybersecurity, coordinating communications, and sharing information, as it shares a commitment with NATO to

maintaining peace and security in Europe.

North Atlantic Treaty Organisation (NATO)

NATO works tirelessly to respond to disinformation campaigns and cyberattacks. It centralises communications with its NCI Agency, debunking disinformation and spreading factual communications. It also works through its SPS programme to prevent cyberattacks by strengthening infrastructure in cyberspace and responds to cyberattacks in a swift manner so that it can minimise the damage of these attacks.

Timeline of Events

4th April, 1949	NATO is formed in Washington D.C. in the United States of America
1971	The NATO Integrated Communications Systems Management Agency is created
2012	The NATO Communications and Information Agency is established (NCI Agency)
2014	NATO adopts a new policy towards cyber defence at the annual summit in Wales
13 March 2014	Russia launched an 8-minute long DDoS attack in an attempt to destabilise Ukraine's computer networks and communications
July 2016	NATO recognises the cyberspace as equally as critical for defence as land, air, and sea
2018	Brussels hosts the NATO Summit
20 January 2020	Suggestions that a Latvian lab was responsible for COVID-19 originates from Russian state controlled media and pro-Russian outlets
21, 22 April 2020	Various disinformation campaigns are carried out upon NATO Member States Lithuania, Latvia, and Poland
13 February, 2022	The first malware is reported by Microsoft, being used to target the Ukrainian government along with multiple other institutions as a

precursor to Russia's War in Ukraine

24 February, 2022 Russia begins their war on Ukraine

Possible Solutions

When it comes to hybrid threats that involve disinformation campaigns and cyberattacks, it is essential to respond with a multifaceted approach. Delegates could put in place measures to aggressively fund countertactics to disinformation, expanding operations and working outside of the organisation with other United Nations member states. Delegates should keep in mind that the NATO Communications and Informations Agency (NCI Agency) is currently responsible for overseeing all NATO communications and working to counteract disinformation. As was previously mentioned, translation into languages is a useful tool of NATO's NCI Agency that allows it to spread truthful information within NATO Member States and outside of these countries. We recommend that delegates consider translation into a wider variety of languages to allow NATO communications on disinformation to be more widely accessible and to further the reach of NATO, as well as solidifying trust in NATO within its own Member States.

In regards to cyber defence, we strongly encourage delegates to consider bolstering NATO's current programmes. It is essential that NATO continues to learn from past and current instances of cyberattacks, particularly pertaining to Russia's cyberattacks in Ukraine and NATO member states. Analysis of Russia's methods and countermeasures are two solutions delegates should consider. It is also important to keep in mind that in NATO's founding treaty, Article 5 states; "*The parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain peace in the North Atlantic area.*" Although this article does not specify cyberspace as an armed attack, delegates should consider whether they should include cyberspace as a part of Article 5.

Bibliography

"2007 Cyberattacks on Estonia." *Wikipedia*, 16 Apr. 2021, en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia#NATO.

"About Us." *NCI Agency*, NATO, www.ncia.nato.int/about-us.html. Accessed 17 Sept. 2022.

Gordon, Max. *LESSONS from the FRONT: A CASE STUDY of RUSSIAN CYBER*

WARFARE. AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY, Dec. 2015, www.hsdl.org/?view&did=816673.

Merriam-Webster. "Definition of DISINFORMATION." *Merriam-Webster.com*, 2019, www.merriam-webster.com/dictionary/disinformation.

NATO. "Collective Defence - Article 5." *NATO*, 23 Nov. 2021, www.nato.int/cps/en/natohq/topics_110496.htm.

---. "NATO's Approach to Countering Disinformation." *NATO*, 17 July 2020, www.nato.int/cps/en/natohq/177273.htm#approach.

Przetacznik, Jakub, and Simona Tarpova. "Russia's War on Ukraine: Timeline of Cyberattacks." *European Parliament*, June 2022, www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Psaropoulos, John. "Timeline: Six Months of Russia's War in Ukraine." *Al Jazeera*, 24 Aug. 2022, www.aljazeera.com/news/2022/8/24/timeline-six-months-of-russias-war-in-ukraine.

"SPS - Key Priorities." *NATO*, www.nato.int/cps/en/natohq/85291.htm. Accessed 15 Sept. 2022.