Research Division

NATO Defense College

NDC Policy Brief

April 12, 2022

The Future of NATO Cybersecurity Training: Cyberwarfare Games

Cordelia Gilligan, Chaeyoung Oh, Gabrielle Tedder, Paola Andreu

Executive Statement

- Cyber threats to NATO security are becoming more frequent, complex, destructive, and coercive – cyberattacks against NATO countries originating from Chinese IP addresses have increased 116% since Russia invaded Ukraine on Feb. 24.
- As part of its training, NATO has begun to incorporate cyberwar games and exercises into its annual war games. However, NATO's cyber war games, in their current state, are flawed training systems that ill-equip NATO members to effectively defend against cyberattacks in the real world.
- In light of the increased occurrence of cyberattacks, NATO's Warfare Development Command, Allied Command Transformation must further develop its cyberwar games through consideration of current events and non-state actors, and implementation of Structured Analytic Techniques.

Introduction

In 2018, Russia interfered in NATO's Operation Trident Juncture by jamming the GPS systems of the conventional weapons involved in the operation, prompting a warning to civilian aircraft that their navigation equipment could be blinded. (Wheeler and Ertan 1). This interference exposed the weaknesses of NATO's cyber security operations and made clear that the system needed improvement.

Following Russia's invasion of Ukraine on Feb. 24, cyberattacks against NATO countries originating from Chinese IP addresses have increased 116%.

Following Russia's invasion of Ukraine on Feb. 24, cyberattacks against NATO countries originating from Chinese IP addresses have increased 116% (Conklin 1).

In this day and age, cybersecurity and security are synonymous. Hostile forces are not limiting their attacks to conventional methods, and conventional attacks are often paired with cyberattacks. For this reason, cyber defense must be an utmost priority for NATO.

NATO's main focus in cyber defense is to protect its own networks, operate in cyberspace (including through the Alliance's operations and missions), help Allies to enhance their national resilience, and provide a platform for political consultation and collective action. In July 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. Allies also made a Cyber Defense Pledge in July 2016 to enhance their cyber defenses, and have continued to bolster their national resilience as a matter of priority. At the 2018 NATO Summit in Brussels, Allies agreed to set up a Cyberspace Operations Center as part of NATO's strengthened Command Structure. In February 2019, Allies endorsed a NATO guide that sets out a number of tools to further strengthen NATO's ability to respond to significant malicious cumulative cyber activities. Most importantly, NATO continuously reinforces its cyber capabilities, including through education, training and exercises.

As part of its training, NATO has begun to incorporate cyberwarfare into its annual war games, as well as construct distinct cybergames. In 2021's Cyber War Game, "Locked Shields," military cyber security specialists played out the largest cyber war game in the world, using the fictional NATO member state of Berylia. The scenario was based on an attack on the fictional country and an adversary called Crimsonia.

In the exercise, non-NATO member "Crimsonia" attacked vital infrastructure such as water supplies and mobile networks, as well as the financial sector on the island state of "Berylia" ("Fake News Attacks…" 2). In addition to maintaining more than 150 complex IT systems per team, the teams had to be efficient in reporting incidents, executing strategic decisions, solving forensic, legal and media challenges, and dealing with hostile information operations. Crimsonia was also engaging in information warfare, persuading the people of Berylia that their government was responsible for a series of accidents through fake news and social media posts.

While efforts such as Locked Shields are an important step in the right direction, NATO's cyber war games, in their current state, are flawed training systems that ill-equip NATO members to effectively defend against cyberattacks in the real world. Because these exercises are planned primarily by conventional security experts, they lack the element of surprise that would go into a real world situation which creates misconceptions about levels of preparedness should an attack occur either during conventional battle or as a discrete cyberattack. Such misconceptions create a dangerous level of vulnerability to the cyber security of NATO.

Methodology

In an article for Foreign Policy, Tarah Wheeler and Amy Ertan, cybersecurity fellows at Harvard Kennedy School's Belfer Center, highlight the shortcomings in NATO's war games vis-a-vis cybersecurity. Their work was instrumental in our consideration of NATO's cyber war games.

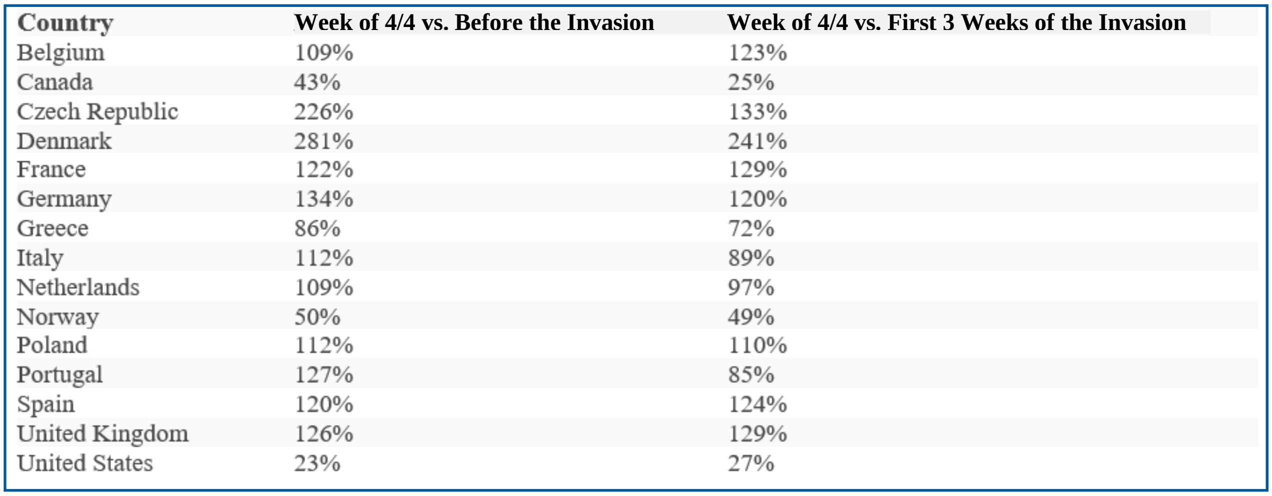
The Koerner article explains the inner workings of war games and how war game operations are carried out. This article, along with the Miguel Alberto Gomez and Christopher Whyte article on cyber uncertainties, was essential in providing backg-round knowledge on war games and how these operations would benefit the cyber security of institutions such as NATO when performed properly. We were able to use the information on war game exercises that the Pentagon practices and the importance of protection of the unknown in the cyber sphere to apply it to a larger scale institution like NATO.

Tim Stickings' article published in The National on the NATO cyber war games simulation paired with the *Training by Gaming* article published by NATO, were the centerpiece for our recommendation. The gaming technique introduced by NATO is essential to the war games method of cyber security that we propose. The exercise discussed in the Stickings article demonstrated that while the methods used by NATO to enhance cyber security are on the right path, they still need improvement. The limitations set by the current methods of enhancement are simply not enough to defend against threats in the real world.

The FOX Business article by Audrey Conklin on recent attacks on NATO countries' cyberspace by China was a key element in forming our argument. The Russian invasion of Ukraine has created a sense of vulnerability among NATO countries in the field of cyber security, because of their focus on the war in Ukraine and the fact that cyber attacks "fall below the threshold of war" (Conklin 5). This article demonstrates that now, more than ever, the security of cyberspace is of the utmost importance.

Jamie Shea's article *NATO: Stepping up its game in cyber defence* was fundamental in our recommendation making process. The article provides an understanding of where NATO cyber security stands now and where experts think it will be going in the future. We were able to use this information to create our own

Figure 1. Frequency of Chinese Cyberattacks Before and After the Russian Invasion of Ukraine



Country	Week of 4/4 vs. Before the Invasion	Week of 4/4 vs. First 3 Weeks of the Invasion
Belgium	109%	123%
Canada	43%	25%
Czech Republic	226%	133%
Denmark	281%	241%
France	122%	129%
Germany	134%	120%
Greece	86%	72%
Italy	112%	89%
Netherlands	109%	97%
Norway	50%	49%
Poland	112%	110%
Portugal	127%	85%
Spain	120%	124%
United Kingdom	126%	129%
United States	23%	27%

This table shows the increasing frequency of Chinese cyberattacks on NATO countries after Russia invaded Ukraine.

recommendations with the improvement of modern technology.

A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis, published by the US Government in 2009 provided us with a robust understanding of structured analytic techniques—a key recommendation to redress the current war games’ shortcomings.

Results and Conclusions

War games are military exercises that are designed to test tactical experience, these usually include field exercises and post exercises (Koerner 3). Unlike observational studies, war games provide strategists with the opportunity to observe the intricacies of decision-making in analogous situations (Kreps and Schneider 2019). The utility of war games decreases dramatically when simulated situations are dissimilar to the kinds of attacks NATO will face. Presently, NATO’s war games do not simulate the full scope of cyberthreats.

There are two ways in which NATO’s war games inadequately prepare for the reality of cyberattacks. The first is when conventional war games fail to account for cyberattacks. For instance, NATO’s Operation Trident Juncture simulated war off the coast of Norway in October 2018. Cyberattacks did not figure in the war game at all—which proved foolish when Russia began jamming the GPS systems of the conventional weapons involved in the operation.

Those involved in the planning of Operation Trident Juncture possessed the traditional backgrounds of those involved in military strategy; this group shares the belief that computers necessary to the function of not only transportation and conventional weaponry, but also the equipment in barracks, are not legitimate targets for cyberattacks. Russia’s behavior highlighted that NATO’s enemies don’t share such a belief. Even after this incident, NATO has not updated its war games to account for the domain of cyber warfare, instead continuing to hold separate war and cyberwar games.

The second way in which NATO’s war games don’t reflect reality is in the construction of cyber war games. NATO does not include nonstate actors in its annual cybergames. The war games thus fail to provide an accurate reflection of potential scenarios for several reasons.

First, it is increasingly likely an attack will come from somewhere other than a recognized hostile nation. Organized terrorist cells, individuals, and mercenaries could all hack into NATO systems without regard for formal conventions of engagement (although Russia has already demonstrated how even other states operate under a different set of rules than NATO allies).

Second, the nature of cyberwarfare is more flexible and limitless than that of conventional warfare. Cyberattacks could take place during battle, attack civilian outposts such as hospitals, or crash infrastructure, to name only a few possible targets. In order to be prepared for the wide array of forms a cyberattack may take, it is necessary for war games to be developed in a way that counters conventional thinking. In this sense, bringing in hackers who do not possess a conventional security background would make cyber war games more useful.

War games, however, are not without their disadvantages. Despite the degree of control afforded, these are not comparable with experimental designs that test the internal validity of processes under investigation. War games are also susceptible to developing extreme or unrealistic scenarios that do not take current events into account. Although nothing prohibits designers from testing behavior at the boundaries of reality, these are less likely to provide useful observations, especially if a scenario fails to consider recent developments in the real world. For example, the increased likelihood of espionage attacks on Pfizer and BioNTech facilities during the Covid-19 pandemic.

Key Definition:
War games are military exercises that are designed to test tactical experience, these usually include field exercises and post exercises

Structured Analytic Techniques

Structured Analytic Techniques are often used in intelligence agencies and designed to help analysts and teams explore and challenge their analytical arguments and mindsets. In relation to cyberwar games, applying these Structured Analytic Techniques can help broaden the bounds of institutional creativity, predict attacker tactics, and most importantly prevent groupthink.

Each technique has a distinct purpose: diagnostic techniques highlight analytic arguments, assumptions, or intelligence gaps; contrarian techniques challenge status quo reasoning; and imaginative thinking techniques provide new insights, different perspectives and/or develop alternative outcomes (*A Tradecraft Primer…* 7).

One diagnostic technique, “Indicators or Signposts of Change,” tracks events, monitors targets, spots emerging trends, and warns of unanticipated change by periodically reviewing a list of observable events or trends. By providing an objective baseline for tracking events or targets, indicators can instill rigor into the process of organizing cyber war games and enhance the credibility of scenarios.

“Devil’s Advocate” is a contrarian technique that challenges a strongly held view or consensus by developing a compelling alternative explanation. NATO's Warfare Development Command has an obligation to look at all possible scenarios and outcomes, fully understanding where there are weaknesses in cybersecurity that could be exploited. Thus, the “Devil’s Advocate” process can highlight weaknesses in a cyber war game setup.

Finally, the "Alternative Futures Analysis" is an imaginative thinking technique that systematically explores multiple ways a situation can develop when there is a high complexity and uncertainty. "Alternative Futures Analysis" is particularly helpful in situations prone to ambiguity, such as cyber war game development. This framework produces a range of outcomes, which reflects how cyberattacks can play out in real-life (*A Tradecraft Primer…* Government 34).

Implications/Recommendations

- Encourage NATO's Warfare Development Command, Allied Command Transformation to incorporate current events, international developments, and non-state actors into their simulations.

This will address the current weaknesses in NATO cyberwarfare games, which do not reflect a contemporary reality, where non-state actors such as terrorist cells, individuals, and mercenaries are increasingly prevalent. Moreover, current international developments demonstrate how even state actors like Russia and China do not follow formal conventions of engagement.

- Invite independent hackers to participate in the cyber war games, given that traditional information technology assumptions may not be the basis for a real-world cyberattack.

Traditional information technology assumptions lack the diversity of perspective that independent hackers bring to the table. Diverse perspectives can predict larger ranges of attacks, thus allowing Allied nations to protect themselves better.

- Implement Structured Analytic Techniques of intelligence agencies so as to maximize consideration of all scenarios and effectiveness of cyber war games overall.

The implementation of the CIA's Structured Analytic Techniques will enhance the credibility of scenarios, produce a range of outcomes that reflect how cyberattacks may play out in real-life, and highlight potential weaknesses in a cyber war game setup, supplementing the preceding recommendations.

References/Useful Sources

A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis . Mar. 2009, https://www.cia.gov/static/955180a45afe3f5013772c313b16face/Tradecraft-Primer-apr09.pdf.

Conklin, Audrey. "Chinese Cyberattacks on NATO Countries Increase 116% since Russia's Invasion of Ukraine: Study." *Fox Business*, Fox Business, 26 Mar. 2022, https://www.foxbusiness.com/technology/chinese-cyberattacks-nato-increase-ukraine.

"Fake News Attacks Feature in NATO Cyber War Game." *Barron's*, Barrons, 15 Apr. 20, https://www.barrons.com/news/fake-news-attacks-feature-in-nato-cyber-war-game-01618505714/.

Gomez, Miguel Alberto, and Christopher Whyte. "Cyber Uncertainties: Observations from Cross-National War Games." *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, Routledge, 16 Feb. 2022, https://www.research-collection.ethz.ch/handle/20.500.11850/534271.

Koerner, Brendan. "How Do the Pentagon's 'War Games' Work?" *Slate Magazine*, Slate, 17 Sept. 2002, https://slate.com/news-and-politics/2002/09/how-do-the-pentagon-s-war-games-work.html.

Nato. "NATO Science Presents: Training by Gaming." *NATO*, https://www.nato.int/cps/en/natohq/news_180639.htm.

Shea, Jamie. *NATO: Stepping up Its Game in Cyber Defence*. Henry Steward Publications, 10 May 2017, https://www.henrystewartpublications.com/sites/default/files/CSJ1_2_Shea.pdf.

Stickings, Tim. "NATO Holds 'Locked Shields' Cyber War Games with Hackers Targeting Fictional Island Nation." *The National*, The National, 1 July 2021, https://www.thenationalnews.com/world/europe/nato-holds-locked-shields-cyber-war-games-with-hackers-targeting-fictional-island-nation-1.1203672.

Wheeler, Tarah, and Amy Ertan. "NATO, We Want to Go to War with You." *Foreign Policy*, Foreign Policy, 22 Dec. 2020, https://foreignpolicy.com/2020/12/22/nato-we-want-to-go-to-war-with-you/.