PilibosMUN

NATO Crisis Committee

Background Guide

NATO

Crisis Committee: Responding to a Cascading Cyber Attack on Critical Infrastructure

Chairperson: Abraham Kirakosian (akirakosian@pilibos.org)

Dias: Areni Baboomi (arbaboomi@pilibos.org) & Araxi Maraian (amaraian@pilibos.org)

Committee Background

NATO is confronted with a particularly complex security environment where cyber threats against the critical infrastructures represent a danger comparable to a conventional military threat. This background information guide will prepare delegates for a simulating scenario inside a NATO Crisis Committee, in which a coordinated, large-scale cyberattack targeting essential infrastructure within multiple member states has taken place. This issue calls for rapid decision making, changing intelligence, escalation management, alliance cohesion and civilian protection.

Cyber operations are fundamentally different from regular military actions. They can be completely anonymous, occur incredibly fast, and make it difficult to determine whether it is a domestic or foreign attack. In this scenario, there are failures in energy, communications, transportation, and public services that threaten not only national stability but also NATO's credibility as a collective defense alliance.

The Evolution of Cyber Threats to Critical Infrastructure

The vulnerability that comes with critical infrastructure is constantly growing as modern society becomes more digitized. Systems that used to be isolated like industrial control systems, are becoming more connected to improve efficiency and reduce cost. This resulted in essential services being exposed to cyber exploitation.

2010 was a major turning point in the discovery of Stuxnet, a cyber operation that caused physical damage to Iranian nuclear centrifuges. Although Stuxnet didn't target civilian infrastructure, it demonstrated that cyber tools could produce destructive effects both physically and online. This attack shifted global perceptions regarding espionage and disruption to one capable of strategic coercion.

Similar incidents also incited more fear amongst countries and citizens. In 2015 and 2016 cyberattacks against Ukraine's power grid caused blackouts across the country. Showing the world that civilians could directly be affected by such threats. These acts increased distrust with civilians and their governments and served political and strategic agendas.

The 2017 NotPetya attack highlighted the danger of cascading effects. The attack was only initially aimed at Ukraine but was able to spread through global networks and disrupt lots of vital infrastructure. The economic damage this caused spread beyond its target and demonstrated how cyberattacks could escalate rapidly.

An analysis of more recent ransomware attacks, such as the 2021 Colonial Pipeline incident in the United States, revealed the risk of cyberattacks against private infrastructure posing threat to national security. Although there was no physical impact, the shortages of the fuel, the panic among people, and the emergency response by the government indicate that cyber attacks are severe.

Nato's Cyber Posture and Collective Defense

There has been an improvement in NATO response to cyber threats over the years. Since time immemorial, cyber defence was perceived as a domestic undertaking than as an international one. However, with the increase in cyber attacks, NATO started incorporating the cyberspace in its overall security structure.

In 2016, NATO officially accepted cyberspace as an area of operation like land, seas, air, and space. This realization indicated that NATO was aware that cyber activities may have adverse consequences just like conventional armed conflict.

Nevertheless, they failed to create a hub cyber force. To achieve this, the alliance chose to depend on the sovereign cyber capability of member states, coordination based on similar doctrine, intelligence sharing and collective exercises.

During the 2021 Brussels Summit, NATO reaffirmed that a cyberattack could, in certain circumstances, trigger Article 5 collective defense obligations. NATO avoided defining a threshold for such a response. This ambiguity is used to strengthen deterrence but makes crises decision-making complicated and impacts alliances.

Critical Infrastructure and Cascading Effects

Critical infrastructure systems provide vital functions for economic stability such as, energy grids, water systems, telecommunications, financial networks, etc. These systems are interconnected, meaning that disrupting one sector would cause a “domino effect” and magnify damage to critical infrastructure.

Within NATO, the resilience of infrastructure can vary. Differences in regulation, investment, cybersecurity standards, and public-private coordination create uneven vulnerabilities. Meaning a coordinated attack could affect some allies much worse than others. This variability puts strain on alliance solidarity and complicates response.

The scenario presented to the committee involves simultaneous attacks across multiple sectors and countries, overwhelming national response capacities and creating pressure for NATO-level action. Delegates neet to consider to to allocate resources, support allies, and prevent escalation.

Attribution, Law, and Ethical Constraints

Attribution remains one of the most difficult challenges in cyber conflict. Cyberattacks barely ever leave any reliable evidence to track. Attacks route operations through third-party infrastructure, reuse common tools, or plant misleading indicators. Technical forensic analysts require lots of time while political decisions need to be made on a whim.

NATO's consensus-based decision-making process complicates situations. Allies usually possess different intelligence assessments or political priorities, further hindering response effectiveness. Acting too quickly can escalate the situation further ruining the effectiveness of the collective response.

International law does apply in cyberspace, but is often interpreted in many different ways. Principles such as sovereignty, non-intervention, necessity, and proportion are widely accepted, but are difficult to apply when it comes to cyberspace. Debates have been sparked during cyberattacks that constitute them as armed attacks justifying self-defense or collective defense under international law.

Alliance Politics and Decision-Making

NATO' alliances having cohesion is crucial to the decision-making effectiveness. Member states differ in threat perceptions, cyber capabilities, and tolerance to attacks. Some states argue for a strong response which includes article 5, to deter future attacks and demonstrate resolve. Other urge caution, if attribution is difficult to determine or there are political constraints that limit options.

Adversaries usually look for exploits in these divisions through disinformation campaigns, selective targeting, or diplomatic pressure. For that reason, public communication is

very important to maintain peace amongst civilians and assure that misinformation is suppressed and not exposing sensitive vulnerabilities.

Many of NATO members' infrastructure is owned and operated by private companies. There needs to be coordination between companies and governments to assure effective responses. Information sharing is a very large part of maintaining proper response and rapid restoration of services after an attack. Legal liability concerns and different cyber security standards amongst different NATO members can complicate cooperation if not addressed.

Conclusion

This scenario challenges delegates to navigate uncertainty, manage escalation, and preserve alliance in a domain where traditional concepts are not always applicable. Effective response requires good judgment, proper coordination, and ethical consideration as NATO confronts modern era security challenges

Questions to Consider

I. What are the most critical infrastructure sectors currently affected (energy, communications, transportation, healthcare, finance), and which require immediate stabilization?
II. How should NATO prioritize its response when multiple member states are simultaneously impacted?
III. How should NATO ensure alliance cohesion when member states differ in threat perception, vulnerability, and willingness to escalate?
IV. What immediate steps should NATO take to prevent further cascading failures across energy, communications, transportation, and public services?
V. What long-term reforms should NATO pursue after the crisis to strengthen cyber resilience and reduce uneven vulnerabilities among allies?
VI. How should NATO respond in the first 24–48 hours to stabilize affected member states while avoiding escalation into conventional conflict?

Bibliography

Greenberg, Andy. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” Wired, August 22, 2018.

NATO Cooperative Cyber Defence Centre of Excellence. Cyber Defence and International Law. Tallinn: CCDCOE, 2022.

North Atlantic Treaty Organization. Brussels Summit Communiqué. Brussels: NATO, June 14, 2021.

North Atlantic Treaty Organization. NATO Cyber Defence. Brussels: NATO. Accessed 2024.

Rid, Thomas. Cyber War Will Not Take Place. Oxford: Oxford University Press, 2013.

Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014.

United Nations Group of Governmental Experts. Report on Developments in the Field of Information and Telecommunications in the Context of International Security. New York: United Nations, 2021.

U.S. Department of Homeland Security. Colonial Pipeline Cyber Incident. Washington, DC: DHS, 2021.