Research Report

Model United Nations Oud-Beijerland 2026

Crisis Committee

Addressing cyberattacks against NATO infrastructure and the potential for collective military response

Lea van Alphen and Cynthia de Jong

Introduction

Cyberattacks have become an increasing threat over the last few years to international security as countries and militaries rely more heavily on digital technology. The definition of a cyberattack is an attempt to break into, damage, or steal data from computer systems, networks, or digital devices without permission. These attacks can target military communication, government databases, and infrastructure. NATO (North Atlantic Treaty Organisation) has to decide how to respond to cyberattacks against its infrastructure and when these attacks can be considered a threat to collective security. Under Article 5 of the North Atlantic Treaty, an armed attack against one member can lead to a collective response from all members. However, cyberattacks are not always easy to investigate, and it can be difficult to identify the responsible country or determine how serious an attack is.

General Overview

NATO has been improving its cyber defence approach as digital threats have become more complex. In 2016, the Alliance recognised cyberspace as an operational domain, alongside land, air and sea. This means that cyber defence is now an important part of NATO's military planning and activities. The Alliance also works to improve the security of its own networks and supports cooperation between member states. However, protecting NATO infrastructure is complicated because member states have different cybersecurity levels and rely on both public and privately owned systems. A weakness in one country's networks could create risks for other members, especially when military information and communication systems are connected.

Although Article 5 establishes NATO's collective defence commitment, not every cyberattack is considered serious enough to justify action. NATO has stated that a single cyber incident or a series of malicious cyber activities could reach the level of an armed attack. Each situation must be looked at and acted on based on its circumstances and consequences. Even when Article 5 is invoked, military action is not automatic. Each member decides what action it considers necessary to assist the Ally under attack. This allows NATO to consider different forms of assistance depending on the situation. One of the main challenges in responding to cyberattacks is determining who is behind them. Attackers can hide their

identities or make their activities appear to originate from another country. This uncertainty creates difficulties when deciding whether a cyberattack should lead to a collective response. NATO members need enough evidence to assess the attack and determine who may be responsible. If responsibility is incorrectly put on someone from a country, the consequences could cause diplomatic issues or further conflict. At the same time, gathering sufficient evidence can take time. This all is further complicated by the fact that certain nations have been known to recruit organised cybercriminals to carry out such attacks, making it very difficult to effectively identify a responsible actor.

International law is also important when considering whether a military response to a cyberattack is justified. Article 51 of the United Nations treaty allows individual and collective self-defence in the event of an armed attack. A collective military response could increase tensions between NATO and the country believed to be responsible for an attack. The accused country might react with further cyber operations or military action, potentially leading to a wider conflict. However, choosing not to respond to serious cyberattacks also carries risks. It could create the impression that NATO members are vulnerable or that attacks against them will have few consequences. This could weaken the Alliance's deterrence. Deciding when a cyberattack calls for a stronger response remains a challenge for the Alliance.

Major Parties Involved

1. United Nations Security Council (UNSC)
The UN Security Council is responsible for maintaining international peace and security. It can investigate threats to international peace and authorise certain collective measures under the UN treaty. It is relevant to this topic because a major cyberattack could threaten international stability or contribute to an armed conflict.
2. United Nations Office for Disarmament Affairs (UNODA)
UNODA supports the UN's work on disarmament and international security, including discussions about information and communication technologies. It is relevant because cyber operations can increase tensions between countries and possibly create conflict. Its work supports international discussions about responsible behaviour and reducing security risks in cyberspace.
3. NATO Cyberspace Operations Centre (CyOC)
Helps NATO military commanders understand threats in cyberspace and coordinates NATO's operational activities in that area. It is especially relevant to deciding how cyber threats could affect military operations and defence.
4. NATO Cyber Security Centre (NCSC)
Protects NATO's own computer networks. It detects cyber threats, responds to incidents, and helps NATO recover from attacks.

Possible Solutions

1. Strengthening NATO's cyber defences
NATO could invest more in cybersecurity, regularly update its computer systems, and organise cyber defence exercises. Backup communication systems could help NATO continue military operations during an attack.

2. Identifying who is responsible for cyberattacks

NATO members could share intelligence and technical evidence to identify the actors behind cyberattacks. Common investigation standards could help prevent countries from making accusations without sufficient evidence.

3. Preventing cyberattacks from escalating into conflict

NATO could strengthen communication with other countries to reduce misunderstandings and prevent cyber incidents from escalating into wider conflicts. Members might support international agreements on responsible behaviour in cyberspace.