Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO

Authors:

Michaela Prucková

In reporting on the unfolding events in Ukraine, media and social platforms have repeatedly discussed as novel the possibility of Article 5 of the North Atlantic Treaty being triggered by a cyber attack on one or more Member States. This article presents a brief overview of the topic and explains that the possibility a cyber attack could lead to the invocation of Article 5 has been established since 2014; hence it is not a novelty and definitely not a response to the latest events on NATO's eastern flank.

NATO's cornerstone

Article 5 of the North Atlantic Treaty, NATO's founding document, stipulates that:

'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 the right 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 the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.'

As one of the core provisions of the Alliance, Article 5 confirms solidarity amongst Member States (Allies) in the event of an armed attack, which can be summarised as *one for all, all for one* in the spirit of Alexandre Dumas's musketeers. Collective defence does not involve merely using armed forces and sending military units; rather, it binds Allies to provide possible and appropriate help to the affected Party.

In NATO's history, Article 5 has been invoked only once, after the 9/11 terrorist attacks on the United States in 2001. That decision, first, showed solidarity with the US after the attacks and, second, enabled the country and the Alliance to take further steps in responding to them.

It is therefore clear that invocation of Article 5 is not an everyday measure but a major political decision on which all 30 Allies have to agree.

The cyber agenda is not new to the Alliance's portfolio; the first reference to cyber attacks appeared in the Prague Summit Declaration of 2002 (Para. 4). This type of public document reflects the outcomes of debates and decisions made at the highest political level of NATO Member States.

Since 2002, the cyber agenda started to increasingly appear in NATO's documents until 2014 when the Wales Summit Declaration acknowledged for the first time the possibility of cyber attacks triggering Article 5. However, the relevant section (Para. 72) focuses on the potential attack's effects and magnitude; it does not question a cyber attack's ability to invoke Article 5 and is couched in terms of *when*, not *if*. In 2014, no one denied that operations in cyberspace could be equal in impact to conventional attacks.

At the next NATO summit in 2016, the Allies went even further by declaring cyberspace a new operational domain, taking its place alongside air, land and sea (Para. 70). The Warsaw Summit Communiqué thus reaffirmed cyberspace as part of NATO's core task of collective defence, following the proclamation of 2014. The possibility of the invocation of Article 5 in reaction to a cyber attack was reiterated in 2021 in Para. 33 of Brussels Summit Communiqué. On all those occasions, evaluation on a case-by-case basis was the guiding principle.

The same applies to space and hybrid warfare. Space was declared the fifth domain of operations during the foreign ministers' meeting in 2019 in the London Summit Declaration (Para. 6). The affirmation that attacks to, from or within space may invoke Article 5 was also reaffirmed two years later in the Brussels Summit Communiqué (Para. 33). As for hybrid warfare, the statements that it may invoke Article 5 have appeared, for example, in Para. 72 of Warsaw Summit Communiqué (2016) or Para. 31 of Brussels Summit Communiqué (2021).

A game-changing cyber attack

We need to keep in mind that cyber attacks have been a 'persistent challenge' for years to NATO, with Russia being a stable originator of limited cyber activities, avoiding further escalation until now. None of the cyber incidents Allies has thus far experienced has led to the invocation of Article 5 and neither has the Alliance stated openly what level or damage the triggering attack would have to cause.

Even though this possibility is sometimes criticised for being a vague statement without clearly drawn lines, it is also logical. As NATO Secretary-General Jens Stoltenberg has stated, both the extent of such an attack and the Allied response under Article 5 '*must remain purposefully vague*'. Hence, the Alliance does not provide potential adversaries with knowledge of the threshold between an *everyday* cyber attack (see, for example, the live map of ongoing attacks by FireEye) and an armed attack in cyberspace. This uncertainty serves as a deterrent and can motivate a potential adversary to exercise self-restraint in their malicious cyber activities and avoid launching a large-scale attack that could cross the blurred threshold. Such a position of strategic ambiguity is reflected in the documents which discuss evaluation on a case-by-case basis.

Put simply, NATO does not want to weaken its position by revealing its red lines and reaction measures in cyberspace. However, we are not entirely blind here. The Alliance has acknowledged, for example, that cyber attacks similar to the ones Estonia experienced in 2007 could lead to Article 5 invocation today.

Since the required gravity and impact of a game-changing cyber attack remain unclear, discussions emerge stirred by the events in Ukraine on what Russian actions in cyberspace aimed at NATO could or would lead to the invocation of Article 5. For example, Michael Schmitt provides an analysis of potential scenarios of Russia's cyber

To summarise, responses to cyber attacks, attacks to, from or within space, and hybrid warfare are part of NATO's collective defence and can, under certain circumstances, lead to invoking Article 5 of the North Atlantic Treaty. Both cyber and hybrid activities can be met with a range of proportional responses by NATO Member States,

which can coordinate, for example, economic or diplomatic measures without having to invoke Article 5. This was stated in Para. 31 of the Brussels Summit Communiqué and by the Secretary-General himself during Cyber Defence Pledge Conference in 2018.

Threats of cyber attacks have featured in NATO policies since 2014. This understanding has developed as a natural response to the evolution of the threat landscape and is not a novelty of the events in Ukraine or an artificial tool aimed at increasing the current geopolitical tensions.

Author: Michaela Prucková, Masaryk University/NATO CCDCOE Law Branch

This publication is a part of the INCYDER database, a research tool on International Cyber Developments (INCYDER), established by NATO CCDCOE to facilitate the work of researchers, lawyers, policy-makers and other cyber security-related practitioners. INCYDER offers up-to-date overviews and easy access to the most relevant legal and policy documents adopted by international organisations active in the cyber security domain along with practical summaries and analysis of recent trends within these organisations written by CCDCOE researchers.

← Library

The NATO Cooperative Cyber Defence Centre of Excellence

ccdcoe-at-ccdcoe.org
+372 7176 800
Address: Filtri tee 12, Tallinn 10132, Estonia

Linkedin
Twitter
Youtube
Flickr
Facebook