NATO and Article 5 in Cyberspace

NATO has designated cyberspace as a domain of warfare and recognized that an adversarial cyber campaign could trigger the Alliance's collective defense mechanism under Article 5. Given the complexities of cyberattacks and the difficulties of designing an effective response, it is unknown whether and what kind of cyberattack(s) might trigger a collective defense response from the Alliance.

By Sarah Wiedemar

The NATO Cooperative Cyber Defence Centre of Exellence (CCDCOE) in Tallinn, Estonia, during the Locked Shields cyber defense exercise on April 2019. *Ints Kalnins/ Reuters*

At the NATO Summit in Wales nearly a decade ago, NATO recognized that cyber defense is an inseparable part of collective defense. Therefore, a cyberattack against one or more member states can trigger the collective defense clause enshrined in Article 5 of the Washington Treaty, the cornerstone of the military alliance. Article 5 is based on the principle that an attack against one member state is considered an attack against all member states, and that by exercising their right of individual or collective self-defense – as recognized in Article 51 of the UN Charter – Allies may take collective action to restore the security of the North Atlantic area. Once triggered by one or more member states, the North Atlantic Council (NAC), the principal decision-making body of the Alliance, must unanimously decide whether the attack warrants the use of Article 5. If so, it is up to each individual member to determine how to respond and to what extent assistance will be provided in concert with the other NATO partners. Since its inception in 1949, Article 5 has only been invoked once, following the terrorist attacks on 11 September 2001.

The overarching mission of NATO is to safeguard the freedom and security of its member states by political and military means. With Article 5 equally applying to cyberspace, the Alliance recognized that cyberattacks could reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. NATO has not laid down any specific red lines that, once crossed, would lead to the invocation of Article 5. Instead, the Alliance's posture relies on strategic ambiguity and is guided by the principle that each attack would be dealt with on a case-by-case basis. Depending on the scope and scale of the attack(s) or campaign, the political will of each member state would guide NATO's response. This can range from diplomatic and economic retaliation, to offensive cyber operations, or military strikes. While flexibility in the application of Article 5 is essential to the integrity of the Alliance, it also creates specific uncertainties when it comes to cyberspace. Determining the effects an attack had, who carried it out, and what the political intentions of the attackers are is generally deemed more difficult in cyberspace than it is in real space.

© 2023 Center for Security Studies (CSS), ETH Zürich

Following a disruptive cyber campaign against the NATO member state Albania in the summer of 2022, Albanian Prime Minister Edi Rama considered turning to the NAC to invoke Article 5 as a response option. Albania's triggering of Article 5 would have been the first time NATO's collective defense clause would have been activated in response to a cyberattack. As such, it would have set a precedent for the Alliance. While the Albanian government ultimately refrained from raising the issue with the NAC, the incident nonetheless spurred renewed discussions on how Article 5 ought to apply in cyberspace.

NATO and Cyberattacks in the Past

Operation Allied Force 1999: During the Kosovo war (1998/1999), the NATO military campaign Operation Allied Force sought to force the Serbian military out of Kosovo. Various nationalistic hacktivist groups from Serbia, Russia, and China (especially after the bombing of the Chinese embassy in Belgrade on 7 May 1999) attempted to disrupt NATO's warfighting capability through a series of distributed denial-of-service attacks (DDoS – see box on p. 3) and website defacements.

Estonia 2007: In 2007, NATO member Estonia experienced a persistent DDoS campaign conducted by patriotic Russian hacktivists that lasted 22 days and targeted a host of Estonian public and private networks, including Estonia's e-government system, banks, and media outlets. The incident occurred shortly after the relocation of a controversial World War II statue from the center of Tallinn, which for the Russian-speaker minority symbolized Victory Day, while for ethnic Estonians served as a reminder of the Soviet occupation and repression. This type of sustained DDoS campaign, coupled with the tense geopolitical environment, was unprecedented at the time.

NATO and Cyber

After an onslaught of DDoS (see box on p. 3), website defacements, and e-mail spamming campaigns aimed at NATO and member state institutions in the wake of Operation Allied Force in 1999 (see box on p. 2), there was a growing understanding among individual member states that they needed to improve their cybersecurity and defense capabilities to protect their own information and communications systems.

Partly because of this experience, the Alliance put cyber defense on the political agenda of the NATO Prague Summit in 2002. There, NATO also adopted the Cyber Defense Programme, which kicked off the creation of the NATO Computer Incident Response Capability (NCIRC), whose task is to prevent, detect, and respond to cyber incidents affecting the Alliance. But it was not until the unprecedented DDoS campaign against NATO member Estonia in 2007 that the Alliance realized the scope of the threat and the full political implications of cyberattacks (see box on p. 2). The Estonian request for assistance following the DDoS campaign was a wake-up call for NATO. Ten months later at the NATO Summit in Bucharest, the Allies approved their first Policy on Cyber Defense. The member states recognized the need for NATO to not only protect information systems critical for the Alliance, but also to share best practices and provide support to Allies in case of a cyberattack. Concerns also arose as to whether and how a cyberattack could become a significant component in warfighting. At the 2014 NATO Wales Summit, the member states declared that cyber defense is part of NATO's core task of collective defense. At the NATO Warsaw Summit in 2016, the Alliance reinforced this commitment by declaring cyberspace a new operational warfighting domain in addition to air, land, and sea.

At the NATO Brussels Summit in 2021, the Alliance went a step further and recognized that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack. This shift to a cumulative approach was likely adopted in reaction to the wave of ransomware campaigns (see box on p. 2) against digital infrastructure in the United States and other NATO member states that affected nearly all critical infrastructure sectors, including healthcare, agriculture, and energy.

> In 2021, NATO recognized that the impact of malicious cumulative cyber activities might be considered as amounting to an armed attack.

Article 5 in Cyberspace

On 25 February 2022, the day after Russia's invasion of Ukraine, NATO Secretary General Jens Stoltenberg was quick to reaffirm that cyber defense is an inseparable part of collective defense and highlight that the Alliance will not give a potential adversary the privilege of defining when Article 5 would be triggered. Although Article 5 equally applies to cyberattacks, the peculiarities of cyberspace create a multitude of additional challenges. For example, the issue of attribution – meaning pinning down who exactly is responsible for a cyberattack – is both tedious, time-consuming, and might not rise to the level of certainty necessary to legally justify specific political or military responses (see CSS Analysis No 244). Similarly, the variety of relationships and quasi-linkages between state and non-state actors in the cyber domain, as well as the physical location from which they operate, does raise questions as to who exactly ought to be punished for what.

Another fundamental problem arises from NATO's position of strategic ambiguity. The Tallinn Manual 2.0, an expert document on how international law might apply to cyberspace, defines a cyberattack as a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. The Manual also clarifies that there is no requirement for an attack to result in physical damage to either objects or people. For quite a long time though, the common assumption has been that the effects of a cyberattack must be tantamount to that of a kinetic strike to cross the threshold of an armed attack and elicit a lawful military response.

Since the 2021 Brussels Summit, NATO has adapted its view on this issue. Nowadays, the Alliance states that the impact of multiple malicious cyber activities conducted below the threshold of an armed attack can accumulate to be significant enough to amount to an armed attack qualifying for collective action under Article 5. As a result of this shift, it has become even less clear which adversarial cyber activities might fall within NATO's scope. A simple comparison with a kinetic strike no longer holds true. There are also unresolved questions as to what might follow if Article 5 is triggered in response to a cyberattack. Due to NATO's case-by-case approach it is unclear whether the Allies are currently in agreement or could achieve consensus on what type or effects and what type of severe impact from cyberattacks would be eligible for invoking Article 5.

© 2023 Center for Security Studies (CSS), ETH Zürich

What, Who, Why, and If Ever

Past malicious cyber campaigns targeting or indirectly affecting NATO members have not raised major public discussions on Article 5, except following Albania. The following three cases – the Colonial Pipeline ransomware attack in 2021, the Viasat hack in 2022, and the destructive cyber campaign against Albania in 2022 – illustrate the complexity of crafting an effective international response to cyber incidents.

In 2021, the United States and other western nations faced a wave of ransomware campaigns across their critical infrastructure sectors. The ransomware campaign conducted by Russian cybercriminal group *DarkSide* against Colonial Pipeline in May 2021 is probably the most well-known one. Colonial Pipeline is the largest pipeline operator in the US. *DarkSide* breached the company's IT network, successfully exfiltrated a large amount of data, and subsequently deployed ransomware against the Colonial Pipeline's billing and accounting system. In reaction to the intrusion, the company shut down all of its pipeline operations to contain the attack, which in turn caused temporary fuel shortages and traffic jams along the entire US East Coast. As a result, US President Joe Biden declared a state of emergency in eighteen states, the first ever such declaration in response to a cyberattack.

DarkSide was a highly prolific cybercriminal group likely operating from Russian territory. There has been speculation that the group may be working with Russian government agencies, but no definitive evidence has emerged to support this claim. In response to the attack, the US administration decided to draw a red line. While meeting Geneva Summit in June 2021, US President Biden handed Russian President Vladimir Putin a list of 16 US critical infrastructure sectors that are off-limits to any Russian cyberattack. Biden noted that each individual country must act against cyber criminals operating from their own territory. The ransomware campaign against Colonial Pipeline was a cybercriminal act by a non-state actor that disrupted critical infrastructure, prompted a state of emergency, and turned into a US national security issue. Despite this, the US administration did not turn to NATO and did not openly discuss Article 5. Rather, Washington chose to tackle the issue bilaterally.

There are also unresolved questions as to what might follow if Article 5 is triggered in response to a cyberattack.

In February 2022, several hours prior to the invasion of Ukraine, the global satellite communications provider Viasat fell victim to an offensive cyber operation likely conducted by the Russian military intelligence agency (GRU). The attackers indiscriminately targeted Viasat modems and were successful in wiping around 20,000 devices (see box on p. 3). The operation cut internet access for tens of thousands of people in Ukraine and Viasat users in at least thirteen other European countries, with the biggest service disruptions occurring in the UK and France. In Germany, it took out the remote monitoring and control of 5,800 wind turbines, affecting power generation and distribution. The attack also temporarily paralyzed the communications of Ukraine's military, police, and intelligence services, which was likely the main goal of the operation.

On 10 November 2022, NATO Secretary General Jens Stoltenberg emphasized that the Viasat hack caused collateral damage beyond Ukraine. The US, UK, and EU formally attributed the Viasat hack to the Russian government and condemned the attack. According to the news agency Bloomberg, US intelligence assessed that the GRU willingly took on significant diplomatic and strategic risks, knowing that the attack would affect multiple countries outside of Ukraine. Despite the spillover effects of the attack and the indiscriminate targeting of Viasat modems in the context of an international armed conflict, the Alliance did not publicly deliberate the application of Article 5.

Between May and September 2022, NATO member Albania fell victim to a coordinated destructive cyber campaign. Initial media reports attributed the cyberattack to Russian cyber criminals, in line with other ransomware campaign across the world. With the investigative support of Microsoft, Mandiant, the US FBI and others, the campaign was eventually attributed to four different advanced persistent threat (APT) actors that are likely linked to the Iranian Ministry of Intelligence and Security (see box on p. 3). The four APTs utilized a multi-vector approach that included the encryption of data (ransomware), the deletion of data, the exfiltration of data, and the dumping of data into the public domain to maximize the disruptive effects. Multiple Albanian government websites and e-online services, including the centralized e-Albania portal and the National Agency for Information Society, were taken out by the campaign. Even the state police's total information management system, which stores the data of people entering and leaving Albania, was temporarily unavailable, causing queues at the border.

On 18 July 2022, an online group or persona known as *HomeLand Justice* (HLJ) took public credit for the destructive campaign. The persona dumped Albanian government documents into the public domain and posted multiple videos on their Telegram channel and website showing,

Cyberattacks: Methods and Tools

A **distributed denial of service (DDoS)** is a type of Denial of Service attack in which the target server, service, or network gets overloaded with traffic originating from several sources – for example, a group of devices. The goal of a DDoS is to make the victim's system inaccessible.

Ransomware is malicious software that aims to encrypt data or block access to it, and to demand that the user pays for unlocking or decrypting the data to regain control. Different varieties of malware can target desktop systems and mobile devices. Ransomware programs target both individuals and organizations. In any case, a successful attack results in downtime and costs for data recovery. But the damage caused by ransomware is not always reversible. For example, the ransomware program may turn out to be a wiper, i.e., a type of malware that ruins or damages data irretrievably.

Advanced Persistent Threats (APTs) are concerted attacks against specific organizations. Typically, APT attacks are government sponsored and use sophisticated malware to penetrate an organization's security defenses.

A **Wiper** is a type of malware that aims to erase (wipe) data from the hard drive of the computer it infects.

Source: Kaspersky IT Encyclopedia

© 2023 Center for Security Studies (CSS), ETH Zürich

among other things, the deployment of ransomware on Albanian servers. In their public messaging, HLJ stated that it performed the cyberattacks to express its anger toward Tirana for hosting the annual conference of Iranian opposition groups in Albania in July of that year. HLJ's logo is also particularly revealing when it comes to attribution. It shows an eagle attacking an Angry Bird (from the eponymous video game) that is surrounded by the Star of David. An Angry Bird is a symbol used by another group known as *Predatory Sparrow*. Back in June 2022, *Predatory Sparrow* ran a destructive cyber campaign against three Iranian steel factories that allegedly belonged to the Iranian Revolutionary Guard Corps. As Predatory Sparrow noted in one of their videos, these cyberattacks were carried out in response to the aggression of the Islamic Republic. It is unknown whether Predatory Sparrow is connected to the state of Israel – but HLJ's symbolism suggests that Tehran might believe they are. Overall, it seems that the four Iranian APTs conducted their campaign not only to send a signal to the Albanian government to not host Iranian opposition groups in exile, but also potentially as a warning to Predatory Sparrow and the state of Israel.

Following the outcome of the forensic investigation, the Albanian government severed all diplomatic relations with Tehran – the first time ever a government has taken such a measure in response to a destructive cyber campaign. During the internal deliberations on how to respond to the incident, the Albanian government also discussed turning to NATO's Article 5. Publicly, Albania's Prime Minister Edi Rama denounced the attacks as the same as a conventional military aggression by other means. However, Rama eventually decided against turning to NATO, noting that he has "too much respect for his friends and Allies to tell them what to do".

As it currently stands, NATO is reluctant to move away from strategic ambiguity.

Implications

The ransomware attack on Colonial Pipeline, the indiscriminate targeting of Viasat modems, and the destructive cyber campaign against Albania vividly show that NATO is in uncharted waters with respect to Article 5 in cyberspace. In none of these cases did the governments affected deem the adversarial campaigns as significant enough to cross the threshold of an armed attack or fulfill the criteria of cumulative effects. To date, it remains an open question whether a cyberattack will ever cause the kind of large-scale destruction and death that occurred on 11 September, or whether it would even be necessary to invoke Article 5.

As it currently stands, the Alliance is reluctant to move away from strategic ambiguity, and the individual member states do not appear inclined to set precedents when it comes to invoking Article 5 in response to cyberattacks. The Alliance will thus continue the balancing act between sustaining unity and political maneuvering space on the one hand, and taking on the challenges – and thus new ambiguities – that cyberspace entails on the other.

For more on cyber security, see CSS core theme page.

Sarah Wiedemar is a Researcher in the Cyberdefence Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Fabien Merz
Language editing: Ally Chandler
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

© 2023 Center for Security Studies (CSS), ETH Zürich
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000610328