8

Article 5 and the Challenges of Cyber Defense

Theo WARNER

Abstract: As cyberspace expands to encompass all aspects of life, so too do the vulnerabilities of critical infrastructure and information expand. The North Atlantic Treaty Organization (NATO) historically has been a force for collective defense and has not shied away from meeting developing cyberthreats from state and non-state entities alike. The primary objective of this short paper is to highlight the unique nature of cyber defense and countering cyberattacks, particularly in the context of NATO's Article 5. I will briefly discuss the language of Article 5, as well as a few of the major challenges that could arise if the article (or any sort of international legal action) were invoked in response to some serious cyberattack, particularly attribution and proportionality, using the infamous 2007 cyberattack against Estonia as a brief case study.

Keywords: Cybersecurity, Cyber Defense, NATO, Article 5, Collective defense, Collective security, Attribution, Proportionality

Introduction

In the late 1980s and early 1990s, the communist system of the Eastern Bloc and Soviet Union disintegrated. The Berlin Wall was toppled in 1989, the Warsaw Pact was dissolved in 1991, and NATO quite suddenly found itself navigating a post-Soviet Europe[604]. As the 1990 NATO Update

[604] Hella Pick, "NATO seeks a new role", *The Guardian*, May 18, 1990, https://www.newspapers.com/image/260321413/.

remarked, "the breathless pace of change does not stop."[605]. Though born in the fledgling years of the Cold War, NATO did not perish with the Soviet Union. In the 21st century, NATO's strategy has shifted to meet new threats, including the rising danger posed by coordinated state-sponsored and non-state cyberattacks[606].

Though coordinated cyberattacks were already causing growing concern in the late nineties, cyber threats shot to the forefront of NATO's security worries in the wake of the massive cyberattack against Estonia in 2007. Since then, NATO has expanded its cyber defense research and capabilities, establishing the Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in 2008 and sponsoring the publishing of the first edition of the Tallinn Manual on the International Law Applicable to Cyber Warfare in 2013. In August 2019, NATO Secretary General Jens Stoltenberg warned that "a serious cyberattack could trigger Article 5 of our founding treaty."[607].

Article 5 is the cornerstone of the collective security agreement codified in the 1949 Washington Treaty that states "an armed attack against one or more of [NATO members] in Europe or North America shall be considered an attack against them all."[608]. The drafters of the treaty did not likely anticipate the scale of interconnectedness brought on by global cyber networks in the 21st century. The world has gotten smaller and information systems, including private and public, rely on innovations in the cybersphere now more than ever before[609].

---

[605] "1990: Summary", NATO Update, last modified August 23, 2001, accessed 11 August, 2020, https://www.nato.int/docu/update/1990/summarye.htm.

[606] "Statement by the North Atlantic Council concerning malicious cyber activities", NATO, last modified June 3, 2020, accessed August 11, 2020, https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.

[607] "NATO will defend itself", NATO, last modified August 29, 2019, accessed August 11, 2020, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.

[608] "The North Atlantic Treaty", NATO, last modified April 10, 2019, Accessed August 11, 2020, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

[609] Sitara Noor, "Cyber (In) Security: A Challenge to Reckon With", *Strategic Studies* 34, no. 2/3 (2014): 1–19, accessed August 12, 2020, doi:10.2307/48527537.

Article 5, buttressed by NATO's conventional defensive capabilities, has acted as a powerful deterrent against acts of aggression against member states[610]. Though the Secretary General's warning was likely a type of "cyber-deterrence", it is nevertheless worth examining what a deployment of Article 5 under such conditions would look like.

Cyberspace has solidified itself as a crucial component of the "fifth domain." Just as land, sea, air, and space are domains through which war is waged, cyberspace exists as a growing part of the information operations domain[611]. In 1999, members of the Pentagon's Joint Task Force for Computer Network Defense warned that in the case of a cyber war critical infrastructure including air traffic control and financial systems could be "held hostage."[612]. More than twenty years later, cyberspace has permeated nearly all aspects of contemporary life, including commerce, finance, and military. This growing reliance on cyberspace increases the susceptibility of necessary aspects of society to attack. As former president of Estonia Toomas Hendrik Ilves points out, "the more modern and the more digitized you are, the more vulnerable you are."[613].

In spite of rising global threats, NATO's relevance in the 21st century has come under growing criticism, particularly from political leadership within the United States[614]. American President Donald Trump has frequently questioned the extent of the United States' financial commitment to

---

[610] Edgar Buckley and Ioan Mircea Pascu, "Article 5 and Strategic Reassurance", (Washington DC: The Atlantic Council, 2010), accessed August 14, 2020, www.jstor.org/stable/resrep03320.

[611] Can Kasapoglu, "Cyber Security: Understanding the Fifth Domain", (Istanbul: Centre for Economics and Foreign Policy Studies, 2017), accessed August 11, 2020, www.jstor.org/stable/resrep14048.

[612] David Abel, "Hackers kept allies on the defensive", *The Boston Globe*, June 20, 1999, accessed August 11, 2020, https://www.newspapers.com/image/441818908.

[613] Toomas Hendrik Ilves, "The Consequences of Cyber Attacks", *Journal of International Affairs* 70, no. 1 (2016): 175–81, accessed August 14, 2020, www.jstor.org/stable/90012601.

[614] Phil Stewart and Idrees Ali, "U.S. to withdraw about 12,000 troops from Germany but nearly half to stay in Europe", *Reuters*, July 29, 2020, accessed 11 August 2020, https://www.reuters.com/article/us-usa-trump-germany-military/u-s-to-withdraw-about-12000-troops-from-germany-but-nearly-half-to-stay-in-europe-idUSKCN24U20L.

the organization and has avoided explicitly endorsing Article 5[615]. Though high profile voices in American political discourse have affirmed the U.S.'s commitment to Article 5, including James Mattis, Mike Pompeo, and Mike Pence, the lack of acknowledgement from the head of state has fomented anxiety among NATO member states[616, 617]. French President Emmanuel Macron has lambasted American distancing from the organization, dubbing recent developments the "brain death of NATO"[618].

The growing danger posed by cyberthreats as well as the presently tepid relationship between the United States and NATO stress the importance of continued study into the challenges of mitigating future attacks. Though this article is limited in scope, I hope to expand on the logistical problems involved in responding to cyberattacks, particularly as it relates to Article 5 of the Washington Treaty.

Defining Terms: NATO and Cyberspace

NATO was established on 4 April 1949 with the signing of the Washington Treaty and has grown considerably since its inception. At its founding, NATO had 12 members. To date, 30 members are in NATO, with the most recent addition being North Macedonia in March 2020[619]. NATO's founding treaty establishes the standard of collective defense binding the member states. This notion is enshrined in Article 5, which states in part:

---

[615] Rosie Gray, "Trump Declines to Affirm NATO's Article 5", *The Atlantic,* May 25, 2017, accessed August 14, 2020, https://www.theatlantic.com/international/archive/2017/05/trump-declines-to-affirm-natos-article-5/528129/.

[616] Gray, "Trump Declines".

[617] Dave Reynolds, "Hailing NATO, Pompeo urges alliance to counter new threats", Share America, November 21, 2019, accessed August 14, 2020, https://share.america.gov/pompeo-hails-nato-urges-it-counter-new-threats/.

[618] "Emmanuel Macron warns Europe: NATO is becoming brain-dead", *The Economist*, November 7, 2019, accessed August 11, 2020, https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead.

[619] "Member countries", NATO, last modified March 24, 2020, accessed August 14, 2020, https://www.nato.int/cps/en/natohq/topics_52044.htm.

> 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[620].

In NATO's 71-year history, Article 5 has only been invoked once in response to the September 11, 2001 terrorist attacks against the United States. A cyberattack large enough in scale to trigger Article 5 would be wholly unprecedented, thus attempting to predict the future or envision what such an event would look like would be exceedingly ambitious for a paper of this scope. Nevertheless, the language employed in Article 5 and the broader issues involving an international response to a cyberattack are worth examining.

Cyberspace is the environment through which digital information is sent, received, and stored. NATO recognizes cyberspace as a unique operational domain, including it with the conventional domains of air, land, and sea[621]. This classification as an operational domain expands NATO's defense capabilities. As Gen. Larry D. Welch further writes, cyberspace is the domain "embedded in all domains."[622]. Technological advancement in the conventional domains has become invariably bound with advancements in cyber capabilities.

Cyberspace is a vast domain that can be divided into more manageable subdomains. The Tallinn Manual stratifies cyberspace into three layers: the physical layer, the logical layer, and the social layer[623]. The physical layer

---

620 "The North Atlantic Treaty".

621 "NATO will defend itself".

622 Larry Welch, "Cyberspace – The Fifth Operational Domain", IDA, 2011, https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx.

623 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed, (Cambridge: Cambridge University Press, 2017), 12, doi:10.1017/9781316822524.

refers to the tangible "network components", including infrastructure like computers and servers, the logical layer is the series of connections that interlink the physical layer, including "applications, data and protocols", and the social layer includes the interactions between people in cyberspace[624]. The proliferation of the internet has cultivated a physical, logical, and social infrastructure that is susceptible to cyberattacks.

A cyberattack is an assault on any of the aforementioned layers of cyberspace – physical, logical, or social. "Cyberattack" is an unavoidably catch-all term that ranges from nuisance phishing scams or distributed denial of service (DDoS) attacks to a damaging or even deadly assault on a power grid[625]. This wide range in severity contributes in part to the difficulty of establishing international legal standards and expectations for responding to cyberattacks.

NATO is no stranger to cyberattacks. The earliest targeted attacks against the organization took place in the late nineties. In the spring of 1999, in the midst of the NATO bombing of Yugoslavia during the Kosovo War, NATO's computer systems in Brussels were bombarded with "thousands of e-mails and potent computer viruses" which briefly crippled the organizations cyber infrastructure[626]. In 2007 Estonia, which acquired NATO membership in 2004, experienced a series of coordinated cyberattacks linked to Russian operatives[627]. In 2014, in the midst of tensions over the Crimean crisis, NATO websites were hit by a series of DDoS attacks linked tentatively to pro-Russian "hacktivists."[628]. Though these attacks range in severity, they all fall under the same umbrella.

---

[624] Schmitt, *Tallinn Manual.*

[625] Brian Barrett, "Security News This Week: An Unprecedented Cyberattack Hit US Power Utilities", Wired, September 7, 2019, accessed August 14, 2020, https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/.

[626] Abel, "Hackers".

[627] Alison Lawlor Russell, "Cyber Attacks on Estonia", In *Cyber Blockades*, (Washington, DC: Georgetown University Press, 2014), 69–95, www.jstor.org/stable/j.ctt9qdsfj.9.

[628] Adrian Croft and Peter Apps, "NATO websites hit in cyber attack linked to Crimea tension", *Reuters*, March 15, 2014, accessed August 14, 2020, https://www.reuters.com/article/us-ukraine-nato/nato-websites-hit-in-cyber-attack-linked-to-crimea-tension-idUSBREA2E0T320140316.

Cyber defense is the action taken to prevent a cyberattack. At present, NATO has made clear that cyber defense is a core component of collective defense, however the early 2000s witnessed a relatively limited endeavor to preempt cyberthreats[629]. The 2002 Prague Summit Declaration, which included a lengthy pledge to counter terrorism and expand NATO's conventional forces, dedicated a one-line commitment to cyber defense: "[To] strengthen our capabilities to defend against cyberattacks."[630]. Since the now infamous 2007 cyberattacks in Estonia, NATO's cyber defense apparatus has expanded considerably. The organization has underscored not only its commitment to cyber defense, but to deterrence and countering "malicious cyber activities"[631]. This commitment was pronounced by Secretary General Stoltenberg's statements cautioning that the collective security assured by Article 5 extended to "serious" cyberattacks.

Article 5 and Countering Cyberthreats

Article 5 embodies the "principle of collective defense"[632]. The assurance that an attack on one is an attack on all acts as a force that binds members together, however this force is largely theoretical as the article has only been invoked once in the history of the alliance.

The language of Article 5 is purposefully flexible, requiring that events triggering its invocation be handled on a case-by-case basis. The article sponsors "such action as it deems necessary…to restore and maintain [security]" in response to an "armed attack"[633]. Of course, "such action as it deems necessary" is not a precise blueprint, and the restoration of "secu-

---

[629] "Cyber defense", NATO, March 17, 2020, accessed August 14, 2020, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[630] "Prague Summit Declaration", NATO, May 6, 2014, accessed August 11, 2020, https://www.nato.int/cps/en/natohq/official_texts_19552.htm?.

[631] "Statement by the North Atlantic Council".

[632] "Collective defense – Article 5", NATO, last modified November 25, 2019, accessed August 17, 2020, https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=Article%205%20provides%20that%20if,to%20assist%20the%20Ally%20attacked.

[633] "The North Atlantic Treaty".

rity" is not a precise goal. Though Article 5 specifies that an "armed attack" will trigger its invocation, it does not necessitate an armed response, only that all members of the organization respond in some measure. NATO has the ability to respond to an attack with the means it sees fit and has jurisdiction to determine when that response is adequate.

In the context of the Washington Treaty, NATO has indicated that a "serious" cyberattack is equivalent to an "armed attack." This is evidenced by Secretary General Stoltenberg's warning that NATO could invoke Article 5 in the event of a "serious" cyberattack as well as the 2018 Brussels Summit Declaration which declared that "Cyber defence is part of NATO's core task of collective defence."[634]. As mentioned before, the activities that amount to a cyberattack range vastly in severity. Determining which actions constitute a cyberattack in the eyes of international law, let alone a "serious" cyberattack, is of great importance when confronted with *jus ad bellum*.

The language equivocating "armed" attacks to cyberattacks was further parsed in the second edition of the Tallinn Manual. In wake of the 2007 cyberattacks in Estonia, the newly established NATO CCD COE spearheaded the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare, a study examining the limits of international law when it comes to cyberspace[635]. The initial study was published in April 2013 and the second edition followed shortly thereafter in 2017. The study devotes a chapter towards discussion of when a cyberattack constitutes a "use of force" (i.e. an "armed attack") and establishes that "some cyber actions are undeniably not uses of force, uses of force need not involve a State's direct use of armed force, and all armed attacks are uses of force."[636].

With that framework established, the study delves into methods of assigning levels of severity to cyberattacks. Whether or not a cyberattack meets the "use of force threshold" is determined by factors including severity,

---

[634] "Brussels Summit Declaration", NATO, last modified August 30, 2018, accessed August 14, 2020, https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.

[635] Schmitt, *Tallinn Manual*.

[636] Schmitt, *Tallinn Manual*, 333.

immediacy, and directness, to name a few[637]. The first factor, severity, is the "most significant"[638]. As they describe, severity lies on a spectrum ranging from inconvenience to physical harm. The former will "never" qualify as a use of force while the latter is invariably so[639]. Where an attack places on this scale of severity determines its categorization as "use of force".

The study notes the ambiguity that can arise when characterizing a cyberattack as a use of force. They write: "a highly invasive operation that causes only inconvenience, such as temporary denial of service, is unlikely to be classified as a use of force. By contrast, some may categorise massive cyber operations that cripple an economy as a use of force…"[640]. In short, disagreements over what is and is not a cyberattack seem destined to occur, which only make the logistics of any serious consideration of Article 5 murkier.

Issues of territoriality and jurisdiction further complicate international legal processes in cyberspace. As defined earlier, cyberspace is a vast and nebulous environment. This is not as true for the physical layer; however, the logical and social layer are highly abstract in the context of territoriality. As Erin Anzelmo writes, "The internet exists in an immaterial dimension"[641]. It does not abide by the conventional rules of geographic territoriality. This unique facet of cyberspace proves to be more of an issue for disputes in international court, however the territoriality question also bleeds into the issue of attribution[642].

The Washington Treaty makes some note of territoriality in Article 6, which serves to expand upon Article 5. It states that "an armed attack on one or

---

[637] Ibid, 334.

[638] Ibid.

[639] Ibid.

[640] Ibid, 337.

[641] Erin L. Anzelmo, "Cyberspace in International Law: Does the Internet Negate the Relevance of Territoriality in International Law?" *Studia Diplomatica* 58, no. 4 (2005), 155, https://www.jstor.org/stable/44839534?seq=1.

[642] Anzelmo, "Cyberspace in International Law", 157–159. Anzelmo examines issues associated with proposed methods of determining jurisdiction that place emphasis on nationality and geography.

more of the Parties is deemed to include an armed attack: on the territory of any of the Parties in Europe or North America …[or] on the forces, vessels, or aircraft of any of the Parties…"[643]. Cyber infrastructure (territory) is included by virtue of NATO's earlier guarantees that Article 5 applies to cyberattacks.

More than issues of treaty language, attribution and limited evidence present the most vexing roadblock when responding to cyberattacks. More often than not, attributing an attack's origin with certainty is all but beyond the realm of possibility[644]. The US ODNI optimistically dubs the process, "difficult but not impossible"[645]. The difficulty increases substantially, however, when attempting to trace the entity responsible for directing the attack[646]. Accurately identifying the actor responsible, especially if the attack was state-sponsored, is necessary before any counter-response can be crafted.

Attribution is the action of assigning blame. In cyberspace, this proves difficult for a myriad of reasons. For one, identifying an individual is entirely possible, but connecting that culpable individual's motivation to a state proves challenging. Benjamin Edwards et al. point out that "In a world where nonstate actors can readily acquire the ability to conduct cyberattacks, holding a government responsible, even for attacks originating within its borders, is not easy."[647]. They further describe issues associated with attribution, including the ease with which digital evidence can be "spoofed" and digital traces erased[648].

---

643 "The North Atlantic Treaty".

644 Jan Dyment, "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence", Security Intelligence, December 28, 2018, accessed August 17, 2020, https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/.

645 US Office of the Director of National Intelligence, *A Guide to Cyber Attribution*, by the NIO and the National Intelligence Manager for Cyber, Washington, DC: ODNI, 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf (Accessed August 14, 2020).

646 US ODNI, *A Guide to Cyber Attribution*.

647 Benjamin Edwards et al. ""Strategic Aspects of Cyberattack, Attribution, and Blame", *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 11 (2017): 2825, accessed August 17, 2020. doi:10.2307/26480254.

648 Edwards, "Strategic Aspects", 2825.

The issue of attribution played a significant role in the oft-cited 2007 cyber-attack against Estonia. In 2007, Estonia was miles ahead of the global curve in cyberspace. Described as a "leader in … e-governance", Estonia has relied on the internet for carrying out a wide range of social necessities and services[649]. In a 2016 interview with the *Journal of International Affairs*, former Estonian president Toomas Hendrik Ilves describes this integration of the internet and public services, commenting that "…Almost all of bank transactions and income tax returns have been done online since 2000, virtually all prescriptions are online, the land registry exists only digitally, and one third of votes in the last several elections were cast online."[650]. As he later points out, however, Estonia's reliance on the internet left it vulnerable to attack.

The inciting incident was the relocation of the Bronze Soldier of Tallinn, a Soviet-era war memorial erected in 1947[651]. The statue had stood in a city park in Estonia's capital, however early in 2007 the Estonian Parliament, in spite of threats from neighboring Russia, voted to move the monument in addition to adjacent war graves[652]. Protests, and eventually riots, erupted, most notably from ethnic Russians living in Estonia who took issue with the statues relocation.

Shortly thereafter, Estonia suffered a series of cyberattacks unprecedented in their scale and coordination. A day after the statue was relocated, Estonian government sites were inundated with an abnormally large amount of traffic. The next day, the state's mail server was spammed with thousands of emails, causing the Estonian Parliament's server to crash. Media, banking and political websites were overwhelmed by DDoS attacks and an internet service provider went down[653].

---

649 Ilves, "The Consequences of Cyber Attacks".

650 Ilves, "The Consequences of Cyber Attacks".

651 Cyrus Farivar and Vinton Cerf, "Estonia", in *The Internet of Elsewhere: The Emergent Effects of a Wired World*, (New Brunswick, New Jersey; London: Rutgers University Press, 2011), 109–49. www.jstor.org/stable/j.ctt5hjgfh.8.

652 Farivar and Cerf, "Estonia".

653 Farivar and Cerf, "Estonia" 136–138.

Estonia was quick to blame Russia for the attacks, and Russia was quick to deny them. In 2007 Russian ambassador Vladimir Chizhov, brushing off the allegations, remarked that "Cyber-space is everywhere", a tacit reminder of the issues of territoriality and attribution[654]. To this day, one ethnic-Russian Estonian citizen was convicted, but, due largely to the difficulty of attribution, no further charges were pursued.

Of course, the attacks on Estonia did not trigger Article 5, however they did trigger a massive undertaking by NATO to rectify a hitherto inadequate cyber defense apparatus. In 2007, the defence minister of Estonia Jaak Aaviksoo pointed out that "Not a single Nato defence minister would define a cyber-attack as a clear military action at present."[655]. This changed within years when NATO extended the weight of Article 5 to cyberspace.

Conclusion and Final Remarks

To summarize, NATO's Article 5 commits members of the alliance to mutual defense if one is subject to an "armed attack." The language remains vague enough to allow for flexibility, however if invoked this could complicate efforts within the alliance to come to agreement. The article has only been invoked once and would only be invoked in case of a "serious" cyberattack, which to this point has not been concretely defined. In the aftermath of a cyberattack, issues of attribution, proportionality and territoriality could further complicate matters. Attribution is exceedingly difficult to ascertain with a high degree of accuracy, proportionality has seen little precedent, and territoriality is nebulous in cyberspace.

When pondering what constitutes a "serious" cyberattack, it is tempting to wonder if an attack similar in scale to the 2007 attacks in Estonia took place, would it trigger Article 5? The answer is most likely not. While NATO has taken a sharper public stance against cyberthreats, the issue of

---

[654] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian,* May 16, 2007, accessed August 17, 2020, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[655] Traynor, "Russia accused of unleashing cyberwar".

attribution makes it unreasonable to mobilize forces in response. In any case, considering how rapidly cyberspace has evolved and expanded in recent decades, it would not be unreasonable to anticipate some "serious" cyberattack in the future, whatever it may look like.

Article 5 continues to symbolize the collective defense agreed upon by the member states of NATO, however its exceedingly rare invocation coupled with the logistical issues of countering cyberattacks make it highly unlikely that it will be triggered. Nevertheless, NATO serves a critical purpose in cyber defense and should continue to bolster its efforts through the CCD COE and strengthen the cybersecurity systems used to protect the physical, logical, and social infrastructure of NATO and its member states.