Journal of International and Comparative Law

Volume 4, Fall 2013, Issue 1 Article 1

NATO, Cyber Defense, and International Law

David P. Fidler

Richard Pregent

Alex Vandurme

NATO, CYBER DEFENSE, AND INTERNATIONAL LAW

David P. Fidler*
Richard Pregent**
Alex Vandurme***

INTRODUCTION

Cybersecurity threats pose challenges to individuals, corporations, states, and intergovernmental organizations. The emergence of these threats also presents international cooperation on security with difficult tasks. This essay analyzes how cybersecurity threats affect the North Atlantic Treaty Organization (NATO), which is arguably the most important collective defense alliance in the world.[1] NATO has responded to the cyber threat in policy and operational terms (Part I), but approaches and shifts in cybersecurity policies create problems for NATO—problems that NATO principles, practices, and politics exacerbate in ways that will force NATO to address cyber threats more aggressively than it has done so far (Part II). Whether NATO can adapt its approach before a major cybersecurity crisis affects the Alliance's ability to carry out its missions effectively remains, at the present time, in doubt.

---

* James Louis Calamaras Professor of Law, Indiana University Maurer School of Law; and Senior Fellow, Indiana University Center on Applied Cybersecurity Research.
** Legal Advisor, NATO Allied Command Counterintelligence.
*** Head, Technical Center Engineering, NATO Computer Incident Response Capability.

[1] This essay integrates the three panel presentations focused on NATO at the St. John's University School of Law Symposium on "Cyberconflict: Threats, Responses, and the Role of Law" held April 12, 2013, namely: "NATO Cyber Defence: An Operational Perspective" (Alex Vandurme), "Cyber Operations and Collective Self-Defense" (Richard Pregent), and "NATO, Cybersecurity, and International Law" (David P. Fidler). The analysis and views in this essay are individual perspectives and opinions only and do not represent the official policies or positions of NATO or any NATO member.

I. NATO AND NATO CYBER DEFENSE

A. NATO: History, Evolution, and Emergence of the Cyber Threat[2]

Understanding NATO's responses to cyber threats requires some background in NATO's history and evolution. Established in 1949, NATO emerged out of the geopolitical turmoil of the late 1940s that featured military and political threats from the Soviet Union against Western European nations, many of which World War II had devastated and left vulnerable to external attack, foreign-sponsored subversion, or revival of nationalistic militarism.[3] The twelve founding NATO members created a cooperative security organization premised on a commitment to collective defense—an armed attack against any NATO member would be an attack against all members, triggering the rights of individual and collective self-defense under which NATO would respond collectively to the attack, including, if necessary, with the use of armed force.[4]

Once established, NATO became a core commitment and institution in the West's efforts to establish and maintain peace in Western Europe and confront, compete with, deter, and, if necessary, defeat the Soviet Union and its allies. NATO's role in the West's strategy to defend against the Soviet threat required building effective political decision-making processes and military capabilities. Under the North Atlantic Treaty, NATO members created the North Atlantic Council as the pre-eminent political body and the military infrastructure necessary to implement Council decisions and defend the Alliance from military threats posed by the Soviet Union, and, after 1955, the Warsaw Pact.[5] NATO expanded to include Greece and Turkey in 1952 and West Germany in 1955 as key participants in its collective defense efforts.

---

[2] This section is based primarily on Richard Pregent's Symposium presentation, "Cyber Operations and Collective Self-Defense."

[3] *See, e.g.*, NATO, *A Short History of NATO*, http://www.nato.int/history/nato-history.html (last visited June 13, 2013).

[4] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2244, 34 U.N.T.S. 243, 246.

[5] *Id.* at art. 9.

As an alliance of many countries, NATO operated on the basis of fundamental principles and understandings. NATO's focus was on defending its members from military attack, which meant that NATO did not function "out of area" despite the global scale of the West's competition with the Soviet bloc. Politically, NATO made decisions on the basis of consensus, meaning all members agreed on (or did not oppose) steps NATO needed to take to meet its objectives. Making and implementing NATO decisions often revealed political or legal constraints NATO members had domestically that affected NATO policies. In terms of military and other capabilities, NATO had what its members provided in terms of funding, armed forces, and weaponry.

Despite challenges and crises during the Cold War, NATO maintained its central role in the West's confrontation with the Soviet Union. The end of the Cold War in the late 1980s and the collapse of the Soviet Union in the early 1990s presented NATO with questions about its purpose in a post-Cold War world. Rather than disband, NATO expanded its membership (now at 28 nations),[6] began to engage in "out of area" security and military operations (e.g., in Bosnia-Herzegovina, Kosovo, Iraq, Afghanistan, and Libya), and started working more broadly with non-NATO countries through partnerships. NATO also adapted to address new security threats, such as international terrorism after 9/11, piracy off the Horn of Africa, and cyber attacks, especially after the cyber attacks Estonia, a post-Cold War NATO member, experienced in 2007.[7]

Although NATO's evolution in the post-Cold War period has involved NATO moving away from its classical collective self-defense mission and into new geographical contexts and security threats, the emergence of cybersecurity threats re-highlighted NATO's collective defense mission because of challenges to the Alliance and its members created by societal, governmental, and intergovernmental dependence on new information technologies, especially the Internet. However, cyber threats constitute a different collective defense problem than deterring Soviet tanks from charging through the Fulda Gap.

---

[6] NATO, *NATO Member Countries*, http://www.nato.int/cps/en/natolive/nato_countries.htm (last updated Apr. 9, 2013).

[7] On the Estonian cyber attacks, *see* ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14–34 (2010).

With the Internet's global reach and the interconnectedness of every NATO member with cyberspace, conceiving of cyber threats to NATO as "in area" or "out of area" makes little sense. In the cyber context, collective self-defense in NATO plays out on a global scale *vis-á-vis* state and non-state actors. As described below, NATO's responses to the cyber threat have required adapting the core mission of collective defense to a threat that defies analogies to, or precedents from, NATO's past.

B. NATO Cyber Defense: The Policy Commitment

Although the watershed moment for NATO cyber defense was the cyber attacks Estonia suffered in 2007, NATO started to address cyber threats before this event. During the Kosovo operation in 1999, NATO members and military forces experienced crude cyber attacks, involving denial of service attacks and webpage defacements.[8] These incidents did not adversely affect NATO operations in Kosovo, but they occurred at a time when political and military concerns about cybersecurity were growing.[9] In 2002, the NATO summit in Prague identified the need for NATO to strengthen its capabilities to defend against cyber attacks and established the Cyber Defence Program.[10] This Program created the NATO Computer Incident Response Capability (NCIRC) in order to provide NATO with better capacity to prevent, detect, and respond to cyber threats.[11] In 2005, NATO included the cyber threat in the Comprehensive Political Guidance document[12] and reinforced the need to protect

---

[8] Jason Healey & Leendert van Bochoven, Atlantic Council*, NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, at 2 (Feb. 2012), *available at* http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow.

[9] *See, e.g.,* U.S. Dep't of Def., *An Assessment of International Legal Issues in Information Operations*, at 5 (May 1999) (observing that "the proliferation of global electronic communication systems and the increased interoperability of computer equipment and operating systems . . . have made information systems that are connected to any kind of network . . . vulnerable to computer network attacks").

[10] NATO, *NATO and Cyber Defence*, http://www.nato.int/cps/en/natolive/topics_78170.htm? (last updated Oct. 22, 2013) [hereinafter *NATO and Cyber Defence*].

[11] Healey & Bochoven, *supra* note 8, at 2.

[12] *Id.*

NATO information systems at the Riga summit,[13] indicating that NATO's interest in cybersecurity reflected mounting worries about social, political, and military vulnerabilities the deepening dependence on cyberspace was creating.

Even though NATO started to respond to cyber threats earlier, the cyber attacks on Estonia in 2007 revealed the inadequacy of NATO's activities and sparked a significant scaling up of NATO political commitment and operational capabilities in this area. The Estonian incident helped bring the stakes of cyber threats into sharper perspective for NATO.[14] Cyber threats presented challenges to NATO's image and reputation, its ability to ensure secure communications supporting military operations conducted by the Alliance, its capabilities to function effectively when cyberspace represents a new battlefield or domain of military conflict, and the ability of NATO members to contribute to the Alliance's objectives and missions.

The increased policy commitment can be seen in the outcome of the Bucharest summit in 2008, at which NATO members noted their adoption of a Policy on Cyber Defence, which stressed "the need for NATO and nations to protect key information systems; to share best practices; and to provide a capability to assist Allied nations, upon request, to counter a cyber attack."[15] NATO continued to give prominence to cyber defense in its Strategic Concept[16] adopted at the Lisbon summit (2010),[17]

---

[13] *NATO and Cyber Defence, supra* note 10.

[14] Stéphane Abrial, *NATO Builds Its Cyberdefenses*, N.Y. TIMES (Feb. 27, 2011), http://www.nytimes.com-/2011/02/28/opinion/28iht-edabrial28.html?_r=1&# (commander of NATO's Allied Command Transformation observing that the damage caused by the cyber attacks on Estonia "was a wake-up call for NATO").

[15] NATO, *Bucharest Summit Declaration* para. 47 (Apr. 3, 2008), http://www.nato.int/cps/en/natolive/official_texts-_8443.htm.

[16] NATO, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, at 16 (Nov. 2010), http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf [hereinafter *NATO Strategic Concept*] (highlighting the need for NATO to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks").

[17] NATO, *Lisbon Summit Declaration* para. 2 (Nov. 20, 2010), http://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf.

the Cyber Defense Concept, Policy, and Action Plan (2011),[18] and the Chicago summit declaration (2012).[19]

Through these policy developments, NATO has established, or encouraged the creation of, mechanisms to implement, with the NCIRC, the strategy of improving cyber defense within the Alliance and in NATO members, including the:

- Cyber Defence Management Board (CDMB), which is the main NATO body overseeing NATO cyber defense activities;[20]
- Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia, as a research and educational enterprise not formally part of NATO but supported by NATO members that collaborates with NATO on cyber defense issues;[21]
- Meetings of NATO Defence Ministers dedicated to cyber defense;[22] and
- Holding cyber defense exercises with NATO members.[23]

NATO also integrated cyber defense into existing policy processes. The Cyber Defence Concept, Policy, and Action Plan of 2011 connects the cyber defense effort overseen by the CDMB with the Defence Policy and Planning Committee in Reinforced Format (DPPC(R)) established in 2010, which manages NATO's planning processes.[24] NATO has also made more transparent the

---

[18] NATO, *Defending the Networks: The NATO Policy on Cyber Defence* (2011), http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf [hereinafter *NATO Policy on Cyber Defence*].

[19] NATO, Chicago Summit Declaration para. 49 (May 20, 2012), http://www.nato.int/cps/en/natolive/official-_texts_87593.htm?mode=pressrelease.

[20] *NATO and Cyber Defence, supra* note 10.

[21] NATO Cooperative Cyber Defence Centre of Excellence, https://www.ccdcoe.org (last visited Sept. 8, 2013).

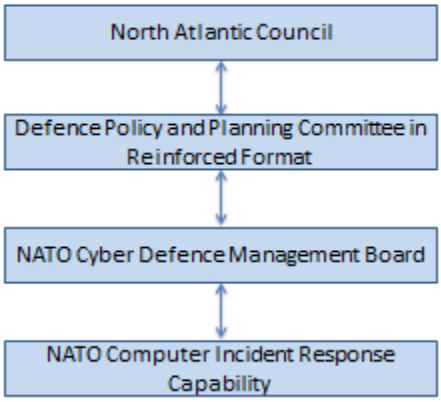
[22] NATO, *Defence Ministers Make Progress on Cyber Protection*, http://www.nato.int/cps/en/natolive/news-_101143.htm (last updated Jun. 4, 2013).

[23] NATO, *Exercising Together Against Cyber Attacks*, http://www.nato.int/cps/en/natolive/75747.htm (last updated Oct. 9, 2012).

[24] NATO, *The NATO Defence Planning Process*, http://www.nato.int/cps/en/SID-F7C21EDE-DEEA4EA7/natolive/topics_49202.htm (last updated May 18, 2012).

process through which NATO will make decisions on cyber threats that might implicate collective defense under the North Atlantic Treaty. In essence, NCIRC will notify the CDMB of threats it has identified that might raise collective defense concerns, and CDMB will inform and work with the DPPC(R) if threats warrant higher-level involvement. The North Atlantic Council retains the authority to declare whether a cyber attack constitutes an "armed attack" under the North Atlantic Treaty. See Figure 1.

Figure 1. NATO Cyber Defense Governance



Source: NATO[25]

[25] *NATO Policy on Cyber Defence, supra* note 18, at 1.

C. NATO Cyber Defense: An Operational Perspective[26]

1. NATO's cyber threat landscape

NCIRC is NATO's main source of technical and operational expertise and capabilities in cyber defense. It works to protect NATO entities (e.g., NATO headquarters) and missions (e.g., International Security Assistance Force (ISAF) in Afghanistan) and to help NATO members address cybersecurity threats to their information technology systems. The diversity of these tasks creates different challenges for NCIRC. For example, ensuring information security in NATO military operations requires balancing operational needs for speed, secrecy, and mobility with risk management, data security, and information sharing—all tasks that characterize effective cybersecurity. Working in other areas, such as protecting the everyday functioning of NATO information systems from infiltration, creates other demands on NCIRC.

NATO confronts a cyber threat landscape that involves generic and specific threats NCIRC has to address. The generic threats include malware, such as viruses and worms, that circulate globally and are often designed by cyber criminals to steal information or money. NATO systems encounter such malware, even when it is not intentionally aimed at NATO or its personnel. However, NATO is the target of a range of cyber intrusion attempts, including those perpetrated by organized criminal organizations, foreign governments engaging in cyber espionage, and "hacktivists" opposed to NATO policies or activities. NATO also has to deal with issues related to its personnel whose on-line behaviors sometimes create risks for the integrity of NATO information systems.

Cyber criminals and foreign governments target NATO systems by using sophisticated email messages that appear credible and authentic to the recipient. However, these emails include "trojan horse" malware that—if activated by the recipient, for example, by clicking on an attachment—attempts to gain access to NATO computers, upload documents, collect information (e.g., passwords, network architecture), use infected computers to

[26] This section is based on Alex Vandurme's Symposium presentation on "NATO Cyber Defence: An Operational Perspective."

compromise other machines and networks, and download more malware (e.g., more advanced programs for exfiltrating information). NATO is an espionage target for foreign governments because of its importance as one of the world's pre-eminent security alliances, and NATO makes a tempting target for cyber criminals because, among other reasons, they can sell information they steal from NATO to a range of willing buyers, including governments.

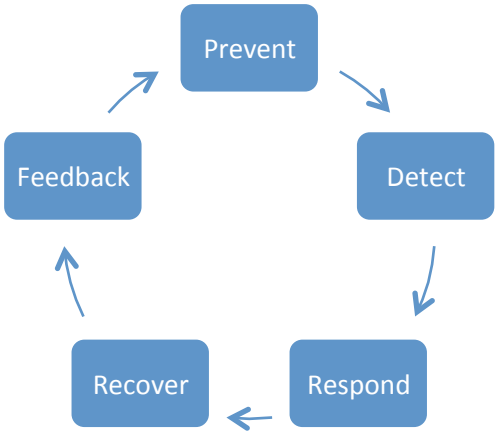
The hacktivist threat to NATO has emerged more recently, with hacktivism aimed at NATO becoming more prominent toward the end of 2011 and continuing through 2012. Among the hacktivists targeting NATO, perhaps the most well-known has been Anonymous, a global, shadowy collection of like-minded (and very smart) hackers who coordinate their activities for maximum impact. Hacktivists seek publicity through damaging NATO's image and reputation, so NATO has experienced webpage-defacement attacks, both successful and unsuccessful.

NATO also has to deal with cybersecurity problems created by "insiders"—NATO personnel whose behaviors, both intentional and unintentional, generate threats and risks to NATO information systems. Targeted email attacks, as described above, rely on recipients to click on attachments or other embedded code, and, unfortunately, just like any other organization, NATO personnel click on things they should not, which means NCIRC has to address threats created by such actions. Even though NATO's systems for storing and sharing classified information are not connected to the Internet, NCIRC has documented NATO personnel attempting to transmit classified information by email over the Internet—behavior that puts NATO security, and sometimes NATO forces, at risk.

2. NCIRC's approach to cyber defense

NCIRC addresses the cyber threats NATO faces through an integrated approach that stresses prevention of threats, detection of intrusions, response to incidents, recovery from infiltrations, and applying lessons learned through feedback into prevention, detection, response, and recovery strategies (Figure 2). In each aspect of this approach, NCIRC continues to develop capabilities and services to improve NATO's cyber defense.

Figure 2. NCIRC's Methodology



In terms of prevention, NCIRC emphasizes secure engineering of information systems to "harden the target" in order to reduce potential vulnerabilities—or the "attack surface"—and provides continuous, NATO-wide anti-malware support. NCIRC strengthens prevention through (1) assessing the vulnerability of NATO systems, including penetration testing, as part of risk assessment and management; and (2) improving NATO personnel awareness through training, exercises, educational materials, and notifications.

NCIRC monitors NATO systems to detect intrusions, including checking emails for malware and web sites for infiltrations. Detection leads to intrusion analysis to determine the nature and scale of a threat and inform responses to it. NCIRC continues to improve its ability to respond to cyber incidents, including (1) expanding its currently limited 24/7 response capability and computer forensic services; and (2) developing a rapid reaction team to mobilize against serious incidents, such as those Estonia experienced in 2007. NCIRC provides on-line and on-site recovery support services and post-incident verification of recovery in order to minimize the adverse effects of cyber intrusions. Prevention, detection, response, and recovery activities produce information NCIRC analyzes into order to develop and share "lessons learned," identify trends, and build a more informed picture of NATO's cyber defense efforts and security posture.

NCIRC's operations demand extensive and intensive collaboration within the Alliance (e.g., between NATO agencies

and member nations) and with non-NATO partner countries, intergovernmental organizations (e.g., the European Union), national law enforcement authorities, private industry, and academia. Further, the more robust NCIRC's operational capabilities become, the more collaboration is critical for NATO cyber defense.

II. NATO CYBER DEFENSE, CYBERSECURITY POLICY TRENDS, AND INTERNATIONAL LAW[27]

The establishment and strengthening of NCIRC's operational capabilities for cyber defense demonstrates that the cyber threat to NATO is a clear, present, and growing danger. As important as such capabilities are, NATO cyber defense takes place in a context affected by policy and legal considerations. This part of the essay analyzes NATO cyber defense efforts against trends in cybersecurity policy and the legal implications of these trends, especially the international legal implications. This analysis situates NATO cyber defense in the broader context of cybersecurity policy developments and international legal challenges that policy makers face. The analysis also raises questions about NATO cyber defense in the future, including questions that identify obstacles to NATO's ability to improve cyber defense sufficiently in light of mounting cybersecurity threats.

A. General Breakdown of Cybersecurity Policy Approaches

Stepping back from NATO, we need to acknowledge that efforts to address cyber threats have created different policy pathways. Three pathways have become prominent—the cyber threat, cyber defense, and cyber technology approaches (Figure 3). Although these approaches are not mutually exclusive, they are distinct. Under the cyber threat approach, we classify a specific cyber threat into traditional policy categories, namely armed conflict, espionage, terrorism, or crime. These categories have policy prescriptions and legal rules that we apply to the cyber

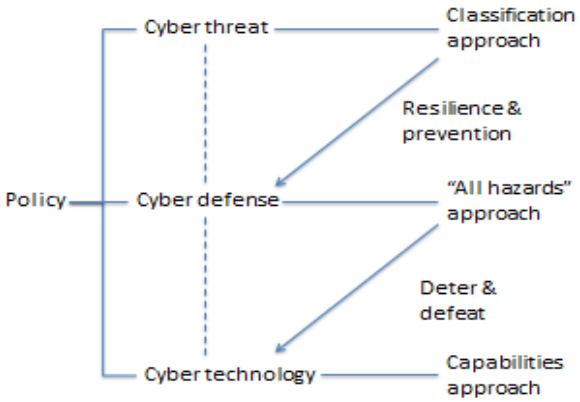
[27] This part is based on David P. Fidler's Symposium presentation on "NATO, Cybersecurity, and International Law."

threat in question, and the categories are defined in ways that are not technology specific.

Despite the prominence of the cyber threat approach, concerns exist that it does not, and cannot, provide robust cybersecurity. Classifying cyber threats into traditional categories does little, the critique goes, for preventing attacks and building resilience against attacks prevention activities do not stop. Instead, the cyber defense approach counsels cybersecurity policy to concentrate on defending against threats regardless of their source or characterization under existing policy and legal categories. This approach is an "all hazards" strategy advising prevention of threats and resilience in responding to and recovering from threats that get through. In other words, effective cybersecurity through prevention and resilience does not depend on classifying a threat as an act of war, espionage, terrorism, or crime or knowing a threat's source.

However, the cyber defense approach faces criticism as well, typically that an emphasis on defense is inadequate to deliver sustainable cybersecurity. Cyber threats have developed to the point where policy has to focus on not only defensive measures but also capabilities to deter and, if necessary, defeat adversaries. This emphasis on such full-spectrum capabilities characterizes the cyber technology approach, which stresses that cybersecurity is ultimately about having technological capabilities to defend against, deter, and defeat cyber threats and those responsible for them. Under this approach, technological capabilities for offensive as well as defensive activities must form part of cybersecurity policy.

Figure 3. Cybersecurity Policy Breakdown



B. *Cybersecurity Policy Approaches, International Law, and NATO*

1. *NATO's commitment to law and NATO's legal ecosystem*

NATO's emphasis on cyber defense across its missions is embedded within a broader Alliance commitment to legal principles and the rule of law. NATO's *Strategic Concept* captured this sentiment in stating that NATO constitutes "a unique community of values, committed to the principle of individual liberty, democracy, human rights and the rule of law" and that NATO will act "[a]lways in accordance with international law."[28]

Applied to cyber defense, this commitment to law means that legal challenges NATO faces in this realm will be many and complex. NATO faces these challenges in a complicated legal ecosystem composed of national law, transnational law applicable to NATO members which are European Union (EU) members, and international law. NATO cyber defense activities have to navigate this legal ecosystem to find approaches that produce legal convergence or harmonization among NATO members. Strategies that conflict with, or raise questions under, national, EU, or international law will reveal—or create—legal divergence or fragmentation within the Alliance. Given that cybersecurity presents challenges to national, EU, and international law regardless of NATO's activities, legal issues are important features of NATO's efforts on cyber defense—a reality recognized by CCD COE's work on legal questions related to cybersecurity.[29]

2. *Law and the cyber threat approach: Struggling with* lex lata

As described above, the cyber threat approach classifies incidents into existing policy and legal categories, which means that this approach operates on the basis of a significant body of national and international law. The classification process involves, first, determining whether a state or non-state actor perpetrated a

---

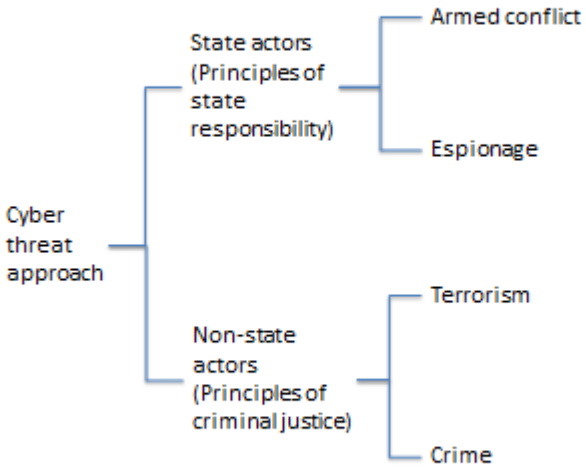
[28] *NATO Strategic Concept, supra* note 16, at 6, 7.

[29] NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, *Focus Areas*, https://www.ccdcoe.org/37.html (last visited Sept. 19, 2013).

cyber incident and, second, slotting the incident into a specific category that contains the policy and legal guidance for addressing it (Figure 4). In terms of the first step, international legal principles are important in assigning responsibility for cyber incidents. The international law on state responsibility affects whether and how a state victimized by a cyber attack can attribute it to another state actor. For attribution and non-state actors, international law on human rights includes principles that regulate the application of criminal law against terrorists or ordinary criminals.

The second step requires classifying an incident according to long-standing policy and legal categories—for state actions, armed conflict or espionage (both traditional and economic espionage); for non-state actors, terrorism and crime. Each category contains international law governing responses to incidents that fall within it. For armed conflict, *jus ad bellum* and *jus in bello* apply. International law is permissive with respect to espionage, even when countries criminalize espionage in national law. States have adopted treaties to address terrorism, and international law includes both generic instruments on crime (e.g., extradition treaties; mutual legal assistance treaties) and treaties addressing specific international crimes (e.g., torture, genocide, crimes against humanity). Overall, the cyber threat approach implicates a great deal of existing international law.

Figure 4. Cyber Threat Approach



However, much of the international law implicated is not specific to the cyber threat but involves "legacy rules" developed before cybersecurity challenges emerged.[30] The only category in which cyber-specific international legal rules exist is in the criminal realm, where, for example, the Council of Europe has produced the Convention on Cybercrime.[31] Cybersecurity policy debates have addressed whether international legal rules not specific to cyber threats are adequate or insufficient. In terms of armed conflict, the recently published *Tallinn Manual on International Law Applicable to Cyber Warfare* contributes to this debate by systematically applying the existing law of armed conflict to cyber means and methods of warfare.[32] The permissiveness of international law on espionage has come under heightened scrutiny as the problem of economic cyber espionage has escalated.[33] Although no acts of cyber terrorism have occurred, none of the existing anti-terrorism treaties would apply effectively to such acts. For countries that are not state parties to the Convention on Cybercrime, they can use more all-purpose bilateral extradition and mutual legal assistance treaties to cooperate on cyber crime, but using these treaties effectively against cyber crime faces numerous difficulties.

More pointedly, whether the cyber threat approach, including the laws it implicates, can support an effective strategy is unclear. The approach is mainly a reactive one—a cyber incident happens, it must be discovered and classified to identify what laws apply, and then the applicable laws have to be implemented against the perpetrators, assuming the incident can be technically attributed to a specific actor in a manner that supports imposing legal responsibility. The experience of the Convention on

---

[30] Applying laws developed before the emergence of cyber threats to such threats is also sometimes called applying "law by analogy." *See, e.g.,* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV, 1023, 1029 (2007) (questioning the "law-by-analogy approach to government cyberoperations").

[31] Convention on Cybercrime, Nov. 23, 2001, ETS No. 185, 2296 U.N.T.S. 167.

[32] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., Cambridge University Press 2013) [hereinafter TALLINN MANUAL].

[33] *See, e.g.,* WHITE HOUSE, DEF. SECURITY SERVICE, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 1 (2013).

Cybercrime, which has only been ratified by 39 states,[34] suggests that moving from legacy rules to cyber-specific principles is not an adequate response in a number of ways, including that it does not change the reactive nature of the cyber threat approach or provide effective deterrence against state and non-state use of cyber technologies for various purposes.

Despite problems connected with the cyber threat approach, it remains part of cybersecurity policy and law nationally and internationally, even where the law applied consists only of legacy rules. Thus, it is relevant for thinking about NATO cyber defense. As a collective defense organization, how international law on armed conflict applies to cyber threats is critical. The NATO-affiliated CCD COE facilitated the development of the *Tallinn Manual* given the importance of these international legal questions.[35] Even though the *Tallinn Manual* is not an official NATO document, statement of NATO policy, or the reflection of any NATO member's position, it will be a seminal analysis in terms of how NATO and NATO members think about and apply the international law on armed conflict to cyber means and methods of warfare.

As described earlier, NATO is a target of foreign governments engaging in cyber espionage, and NATO faces this threat in a context in which international law does not prohibit or restrict espionage activities. Does the threat of cyber espionage, including economic cyber espionage, suggest that NATO and its members should re-think the permissive nature of international law on espionage? More specifically, how will NATO and NATO members respond to U.S. diplomatic efforts to change attitudes and practices on economic espionage in light of revelations of alleged Chinese economic cyber espionage on a massive scale?[36]

Part of NATO's post-Cold War evolution involved addressing as an Alliance the threat of international terrorism,[37]

---

[34] *Convention on Cybercrime* (June 13, 2013), C.E.T.S. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
[35] TALLINN MANUAL, *supra* note 32, at 1.
[36] *See* WHITE HOUSE, *supra* note 33.
[37] NATO, *NATO and the Fight Against Terrorism,* http://www.nato.int/cps/en/SID-8E7AA87D-4AEBB4C6/natolive/76706.htm (last updated Oct. 12, 2012).

and NATO members have widely ratified anti-terrorism treaties.[38] With mounting indications, especially from the United States,[39] that counter-terrorism is beginning a transformation from the policies that have characterized the post-9/11 world, NATO faces questions about how it will coordinate its cyber defense activities with its on-going (and probably shifting) counter-terrorism efforts. What this transformation in counter-terrorism will be is still not entirely clear, but it will probably involve addressing terrorist activities less from an armed conflict approach and more from a criminal and law enforcement strategy. Such a shift would connect NATO cyber defense against cyber terrorism with cyber crime strategies, triggering questions about how strongly NATO should support international law on cybercrime (specifically the Convention on Cybercrime) given doubts about its effectiveness. More generally, how much NATO should be engaged in criminal and law enforcement activities in the cyber realm is an issue when NATO is, first and foremost, a collective defense organization.

3. *Law and the cyber defense approach: Arguing about* lex ferenda

As described above, the perceived problems afflicting the cyber threat approach have fed into support for the cyber defense approach—the "all hazards" strategy to defend cyber infrastructure and systems from attacks regardless of source or intent. NATO experiences cyber intrusions perpetrated by both foreign governments and cyber criminal organizations, often using the same techniques (e.g., malware-infested emails). Foremost, NATO needs to defend against this kind of threat no matter whether a state or non-state actor is responsible. Thus, classifying such attacks as espionage or crime is secondary to deterring or mitigating such attacks and creating resilience against successful infiltrations. Being fundamentally distinct in policy terms, the

---

[38] For ratification status of these instruments, *see* United Nations Treaty Collection, *Text and Status of the United Nations Conventions on Terrorism*, http://treaties.un.org/Pages/DB.aspx?path=DB/studies/page2_en.xml.

[39] *See, e.g.,* President Barack Obama, Remarks by the President at the National Defense University (May 23, 2013), http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university.

cyber defense approach generates legal issues different from those the cyber threat approach implicates.

Generally, the type of policy measures associated with strengthening cyber defense tend to trigger questions about, or tensions between, these measures and existing legal rules. This pattern stimulates debates about what the law should be (*lex ferenda*) to support more robust cyber defense rather than how existing law (*lex lata*) should be applied to categorized cyber threats. In other words, the cyber defense approach generally supports changing law, where necessary, to reflect the challenges presented by cyber threats. But, again, these changes seek to bolster defensive strategies to prevent attacks and build resilience rather than to make legacy rules in the reactive cyber threat approach more specific to cyber threats. Opposition to these changes is often embedded in fundamental principles of international and national law, which pits support for these principles against claims that cyber defense requires new rules or new applications of existing principles.

Three strategies to strengthen cyber defenses illustrate this dynamic. Strong cyber defense requires "situational awareness," meaning that (1) governments need to conduct more surveillance of information systems to understand the pattern and nature of cyber threats in circulation; and (2) state and non-state actors must share more information more frequently in order to heighten the public and private sectors' understanding of threats and abilities to defend against them. However, advocates of civil liberties, such as the right to privacy, tend to oppose on constitutional and international human rights grounds proposals to increase governmental authority to conduct electronic surveillance[40] and increase information sharing between governments and non-governmental entities.[41]

---

[40] *See, e.g.,* Clapper v. Amnesty Int'l U.S., 133 S. Ct. 1138, 185 L. Ed. 2d. 264 (2013) (Supreme Court decision rejecting on standing grounds a challenge by Amnesty International and others against the constitutionality of the Foreign Intelligence Surveillance Act Amendments Act).

[41] *See, e.g.,* Michelle Richardson, *CISPA: A Legislative Threat to Privacy and Civilian Control of the Internet*, AMERICAN CIVIL LIBERTIES UNION (Apr. 4, 2013), http://www.aclu.org/blog/national-security-technology-and-liberty/cispa-explainer-1-what-information-can-be-shared (critical privacy analysis of a legislative proposal in Congress that seeks to increase information sharing).

A second example involves the debate over protecting critical infrastructure owned and operated by the private sector. The strategy of improving cyber defenses requires encouraging or mandating that the private sector improve its cybersecurity practices, especially when private-sector enterprises control or manage critical cyber infrastructure, critical infrastructure operated through Internet applications, or critical infrastructure dependent on the Internet to function. This requirement brings the question of regulating the private sector for cybersecurity purposes into play, and, as the United States has experienced, political disagreements about such regulation have led to stalemate in the U.S. federal legislature.[42] As with proposals for improving situational awareness, this fight is marked by disagreements about the appropriate scope of governmental power and legal authority to defend against cyber threats. International law does not contain any rules or instruments on protecting critical infrastructure in the cyber context, so the legal tensions arise from national legal systems.

The third example focuses on proposals for cyber defense to be active rather than just passive. What "active defense" means is part of the debate about cyber defenses, and the concept means different things to different people. Generally, "active" defenses are distinguished from "passive" defenses in that "active" measures extend beyond a defender's own information systems to identify, track, probe, infiltrate, or retaliate against the source of a cyber intrusion. Included in discussions about active defenses are tactics such as "trace back," "hack back," surveillance for "situational awareness," and "counter-strike." Debates about active defenses include arguments that such defenses deployed by private entities could create problems under national criminal laws. Active defenses could also generate worries that such defensive activities could violate principles of sovereignty and non-intervention in international law.

NATO's emphasis on cyber defense overlaps in important ways with the thrust of the cyber defense approach. Table 1 lists

---

[42] Michael S. Schmidt & Nicole Perlroth, *Obama Order Gives Firms Cyberthreat Information*, N. Y. TIMES, Feb. 12, 2013, at A16 (reporting on the issuance by President Obama on an executive order on improving cybersecurity for critical infrastructure as an alternative to Congress' failure to pass legislation addressing this issue).

strategies often associated with improving cyber defenses and describes aspects of NATO's efforts that reflect these strategies. This overlap does not mean NATO's activities embrace more controversial issues implicated by the cyber defense approach, such as pursuing more intrusive government surveillance, more regulation of private-sector critical infrastructure, and more "forward-leaning" active defenses. However, because these controversies are alive in NATO members and beyond, they will affect NATO cyber defense efforts by, at the very least, raising questions about what NATO does. For example, will NATO members' sensitivities about sovereignty keep NATO cyber defense activities completely passive and reactive even as cyber threats expand in scope, intensity, and sophistication? How will strengthening NATO cyber defense deal with differences within the Alliance about the privacy and other civil liberties in light of the cyber threat? What impact will U.S. and EU debates about improving private-sector cybersecurity have on NATO cyber defense activities?

Table 1. NATO and the Cyber Defense Approach

Cyber Defense Strategy	**NATO Cyber Defense Efforts**
Defend against any type of cyber attack	• Strengthen cyber defenses of NATO systems against all kinds of cyber attacks (e.g., NCIRC)
Expand information collection, retention, sharing, and analysis	• Improve information collection, analysis, and sharing • Better consultation, early warning, and situational awareness • Greater use of "open source" intelligence for cyber defense
Extend reach of cyber defense activities	• Cover NATO military wing and NATO civilian agencies • Improve NATO member cyber defenses • Work with the private sector in NATO members on cyber defense • Cooperate with non-NATO countries on cyber defense • Set requirements for non-NATO contributing nations in crisis management mission
Move from "passive" to more "active" measures	• NATO rapid response teams • NATO "penetration" testing of its systems • NATO awareness of technical, policy, and legal debates about more "active" defenses
Integrate cyber defense with other defense planning	• Integration of cyber defense into NATO Defence Planning Process

4. Law and the cyber technology approach: Harnessing cyber capabilities

The cyber technology approach holds that the key to cybersecurity is development of full-spectrum technological capabilities to detect, deter, and defeat cyber threats. This focus on capabilities rejects both the reactive categorization of the cyber threat approach and the emphasis on defense in the cyber defense approach. Further, the cyber technology approach believes that the other two approaches are, in fact, dependent on technological capabilities more than on policy prescriptions and legal principles. For example, as described above, the cyber threat approach makes attribution critical to assigning accountability under each threat category, which constitutes a dilemma for this approach given the difficulty of attribution in cyberspace. According to the cyber technology approach, the only way to improve attribution is through better, more powerful technological capabilities, not through policy or legal maneuvering. Similarly, the ability to defend against cyber threats through an "all hazards" strategy requires cutting-edge technological capabilities to prevent, monitor, detect, respond, and recover from cyber intrusions. Moving from passive to active defenses also requires technological prowess to achieve defensive objectives and minimize policy or legal issues active defenses might raise.

The strategic objective of strengthening cybersecurity through technology means law has different functions under this approach, namely facilitating development of full-spectrum cyber capabilities (e.g., through research and development programs and cybersecurity workforce enhancement efforts) and regulating the use of such capabilities. The development of more powerful and versatile full-spectrum capabilities will put power into the hands of government actors, and policy and legal issues will arise concerning how such power is exercised. These issues can arise in different contexts, including the risks of secrecy in using powerful cyber technologies for law enforcement, intelligence, and military purposes; constitutional tensions between executive and legislative prerogatives in national security; and balance of power dynamics in international relations. On these issues, international law either does not exist (e.g., on developing new cyber capabilities, regulating secrecy, or managing constitutional tensions) or is perceived to be weak (e.g., controlling balance of power politics).

As with the other approaches, the cyber technology approach generates questions for NATO's cyber defense strategy. As the description of NCIRC above indicates, NATO cyber defense requires operational capabilities, but, at the present time, NATO members are not sharing their most advanced technologies with NATO. How can NATO keep its defensive capabilities relevant when offensive cyber means and methods continue to advance? Can NATO's cyber defense efforts be cutting-edge without developing offensive capabilities?

Further, if NATO deployed more advanced technologies, the level of secrecy about NATO cyber defense activities would likely increase. How would such heightened secrecy affect NATO and NATO members? Would more secrecy on cyber defense in NATO generate backlash within constituencies in NATO members or beyond? Similarly, having access to more powerful technological capabilities could elevate NATO's role in the cybersecurity dilemma emerging among the great powers in international politics, especially as between the United States and China. Will equipping NATO will more full-spectrum capabilities fuel the "cyber arms race" that is already underway?

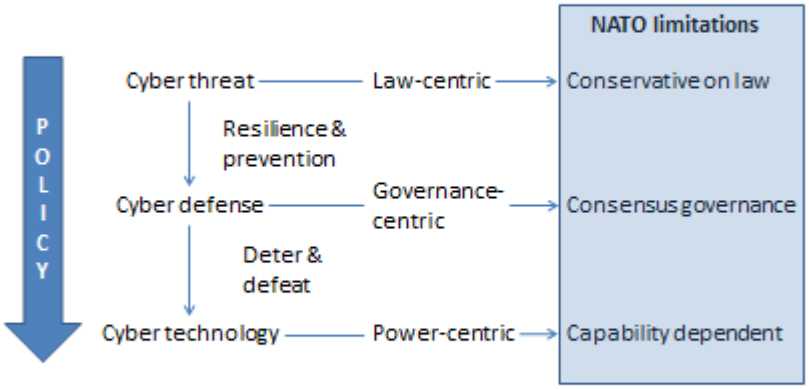
C. Cybersecurity Policy Shifting: Legal Implications and Challenges for NATO[43]

In addition to identifying the cyber threat, defense, and technology approaches as distinct policy pathways with different legal implications for cybersecurity, analyzing whether policy preferences are shifting in this realm is important, and, if so, what consequences flow from such a shift. Our symposium panel discussed a potential shift in policy away from the cyber threat approach toward the cyber technology approach (Figure 5). Although the cyber threat approach remains part of the mix, problems with it have encouraged more policy interest in improving cyber defenses. But, as described above, a cyber defense emphasis produces awareness of the limitations of defensive strategies and the attractiveness of developing full-spectrum capabilities—thus suggesting an increasing interest in a

[43] In addition to Fidler's Symposium presentation, this section draws on Pregent's presentation on "Cyber Operations and Collective Self-Defense."

capabilities focus. Such a shift has implications for the role of law in cybersecurity because, as Figure 5 depicts, a shift from the cyber threat approach, with its dense legal texture, to the cyber technology approach, with its emphasis on capabilities, involves a move from a strategy grounded in well-traveled legal categories and concepts, to one premised more on the exercise of material power in cyberspace.

Figure 5. Policy Shifts and NATO Cyber Defense



Concerning the three categories and the potential policy shifting described above, NATO finds itself in a difficult situation that, under current NATO practices, will be hard to escape. In terms of the cyber threat, defense, and technology approaches, NATO reflects behavior that puts the Alliance at a disadvantage. NATO tends to be conservative in terms of legal issues, meaning that the Alliance does not promise to be a fruitful forum for adapting or revising legacy rules to reflect the particular challenges cyber poses.

Similarly, with NATO operating on the basis of consensus, the Alliance's decision-making processes might have difficulty handling governance questions created by the cyber defense approach, such as how "active" should NATO cyber defense be. Operationally, NATO cyber defense appears more static and reactive than active in orientation—a situation that could lead NATO cyber defense to become a cyber "Maginot line" rather than an effective defensive strategy. It is not clear whether NATO members could reach consensus on what more active cyber

defense activities would be permissible under international legal principles on sovereignty and non-intervention.

As noted earlier, NATO functions with the capabilities its members make available to it, meaning that NATO's technological capabilities in cyber might not reach cutting-edge status, leaving NATO cyber defense behind the global technological curve in cyberspace. This problem is exacerbated if policy makers in leading powers, such as the United States and China, are placing more reliance on developing, deploying, and using full-spectrum cyber technological capabilities because of the perceived pitfalls of other approaches and the mounting geopolitical competition now affecting cyberspace.

NATO members are also extraordinarily sensitive to the Alliance having any offensive cyber capabilities or even discussing the need to think about the value of cyber capabilities and operations in missions NATO might undertake (as NATO has done with other technological developments affecting its military missions).[44] The North Atlantic Council has not discussed, let alone authorized, the development of offensive capabilities, doctrine, or rules of engagement in the cyber realm.[45] Whether NATO members could agree on what offensive cyber operations international law would permit is also not clear, especially in light of difficulties cyber presents to the international law on armed conflict revealed by the *Tallinn Manual* and other analyses.[46]

Events outside the specific context of NATO cyber defense might also adversely affect NATO cooperation. For example, in June 2013, negative European reactions to the disclosure of a

---

[44] For proposals for how NATO could address offensive cyber operations, *see* Healey & Bochoven, *supra* note 8, at 8 (recommending that NATO should consider coordination of NATO members' offensive cyber operations and "creating a group modeled on NATO's existing Nuclear Planning Group, to consider offensive cyber policy").

[45] NATO's standing rules of engagement (ROE) might theoretically provide a basis for NATO offensive cyber operations under the ROE for information operations, but reliance on such ROE for offensive cyber operations is very unlikely given existing NATO sensitivities about offensive cyber issues. On NATO ROE generally, *see* NATO, NATO LEGAL DESKBOOK 254–62. (2d. ed., 2010).

[46] NATO's reluctance to address offensive cyber operations does not mean that the law of armed conflict prohibits such operations generally or in specific contexts where such operations might be militarily advantageous or ethically preferable.

secret U.S. surveillance program targeting cyber activities of foreign nationals, code-named PRISM, reflected new trans-Atlantic tensions on government surveillance in cyberspace, its implications for privacy and other civil liberties, and the potential for European-American cooperation on cybersecurity. The *Washington Post* reported that "[t]he discontent from Europe pointed to the breadth of fallout from the affair and to the potential for fresh strains between the United States and allies wary of American intrusiveness."[47] Whatever the long-term impact of this political fallout, the short-term consequences will likely not create more willingness among NATO members to become more ambitious with NATO cyber defense.

CONCLUSION

In its sixty-four year history, NATO has been at the center of national security challenges faced by members of the Alliance, whether the challenge involved confronting Soviet military power in Europe, expanding its collective defense strategy in the post-Cold War period, responding to humanitarian crises, or participating in efforts to address international terrorism. NATO's cyber defense strategy means that the Alliance has started to deal with yet another security threat, spurred in particular by the Estonia cyber crisis. However, despite the progress NATO has made with its operational capabilities through NCIRC and its decision-making processes on cyber defense issues, NATO is not, at present, at the center of cybersecurity thinking taking place within the policy circles in NATO members, especially the United States. The more NATO lags behind in cybersecurity policy and law, the more the Alliance will be stuck in a reactive mode—a situation that will reduce NATO's ability to be a more constructive platform for cybersecurity both within the Alliance and between NATO and non-NATO countries. NATO could proactively play a more significant role in global cybersecurity but only if NATO members empower NATO to lead rather than just trail behind.

---

[47] Michael Birnbaum, *Merkel, Other European Leaders Raise Concerns on U.S. Surveillance*, WASH. POST (June 10, 2013), http://www.washingtonpost.com/world/merkel-other-european-leaders-raise-concerns-on-us-surveillance/2013/06/10/305eddda-d1da-11e2-a73e-826d299ff459_story.html.