Understanding NATO's Central Role in the Future of Global Cyber Defense

By Samantha Brletich

NATO and non-NATO countries, who have emerging cyber capabilities and regularly face cyber threats, are starting to demand an international organization to provide guidance on cyber norms and cyber-attack responses. Many countries look to NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE) to increase their own cyber capabilities through training, education, and coordination and to outline policy and military responses to cyber-attacks. The CCDCOE sponsored the writing of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* to examine how existing international law applies to cyberspace and cyber operations. The expansion of CCDCOE membership to include non-NATO and non-Euro-Atlantic countries illuminates the urgency of the cyber issue, the collaborative-oriented and global future of NATO's cyber efforts, and the need for comprehensive guidance to formulate cyber strategy.

The CCDCOE, headquartered in Tallinn, Estonia, is a collective and collaborative cyber knowledge hub for education, research, and the development of global cyber norms and cybersecurity training requirements. The CCDCOE supports NATO command arrangements, provides opportunities to practice varying cyber interdisciplinary approaches, and hosts cyber training simulations to build relations and cyber strategies between member states.[1] Cyber is now the fifth domain; the newest theater of warfare and category of combat. The CCDCOE was established in 2008 after Estonia suffered a crippling cyber-attack executed by Russia in 2007 following the Bronze Soldier statue relocation row. The attack on Estonia was a watershed moment, demonstrating the vulnerability of state-level networks and sparking a global conversation about cyberwarfare and the international response.

NATO's CCDCOE is a model for collective cyber defense and serves as the center of cyber integration. Currently, the CCDCOE cyber defense policy is network defense and protection of NATO networks and does not include offensive cyber capabilities, a sticking point for many NATO members who rely on NATO for collective defense. The CCDCOE works with international alliances including industry and academia (through the NATO Industry Cyber Partnership) to enhance the protection of NATO's networks and to build knowledge among CCDCOE members. The CCDCOE's requirements and the complexity of cyber operations will force nations to develop their own cybersecurity policies and explore regional and international organizations to assist in their cyber defenses. The EU committed to more cooperation with the CCDCOE at the 2008 Warsaw Summit through the EU Agency for Network and Information Security, creating the potential for stronger cyber security policy, information sharing, and more resilient networks in Europe.[2] The CCDCOE's International Conference on Cyber Conflict, serves the cyber security community's technical experts, strategic thinkers, policymakers, and lawyers as an interdisciplinary platform for networking and sharing knowledge.[3]

When to Take Action: The Tallinn Manuals and the Use of Force

NATO collective defense is enshrined in Article V of the NATO Charter: an attack on one is an attack on all. Article V has not been invoked because of a cyber-attack but might be invoked if a cyber-attack occurred within a conflict and had the same impact as a physical attack. However, no consensus exists among NATO members, CCDCOE members, and the international community on what cyber-attacks constitute a physical attack. By design, some cyber-attacks cause immediate damage, such as a global malware attack, while the consequences of others may not be immediately known and can cause damage years later. The impact of a cyber-attack and what type of cyber operation would provoke the use of force is therefore difficult to measure. Furthermore, cyber integration into conventional warfare makes it difficult to determine if an offensive cyber action/operation was solely a cyber-attack or part of a larger military or intelligence campaign. The situation becomes murkier when cyber operations enable or support a conventional warfare operation that results in civilian deaths or human rights abuses. No court to prosecute cybercrimes or malicious cyber actions/operations exists. However, Norwegian Judge Stein Schjolberg proposed a court called the "International Criminal Tribunal for Cyberspace" to deal with cybercrime, forgery, identity theft, and fraud.[4] The 2001 Council of Europe Convention on Cybercrime (the Budapest Convention) marked a milestone as countries agreed upon efforts to "pursue a common criminal policy aimed at the protection of society against cybercrime" and increasing cooperation among nations "to ensure that their domestic laws criminalize" cybercrime.[5]

Appropriate and proportional responses need to be developed, as an overreaction may lead to cyber warfare, conventional warfare, or an armed attack. The most capable cyber state adversaries posing a global threat—China, Russia, and North Korea—use cyber to support their foreign policy objectives. Cyber-attacks foreshadowed Russian military incursions into Georgia and Ukraine. Georgia suffered from Distributed Denial of Service (DDoS) attacks, spamming, dissemination of malicious software, and possible attempts to conduct a "cyber blockade," which involved rerouting all Georgian Internet traffic

through Russia, according to a CCDCOE document.[6] Similarly, Russian cyber-attacks against Ukraine in 2016 and 2017 led to attacks on the power grid and the financial system. Current policy responses including sanctions and public shaming have done little to stop cyber-attacks, weaken state-sponsored cyber programs, or deter cyber criminals and future cyber operations.

Cyber operations that violate the prohibition of the use of force in international relations, impede a state's ability to exercise the right of self-defense, and occur during armed conflict were examined in the first Tallinn Manual.[7] According to Professor Michael Schmitt, the main architect of both Tallinn Manuals, a cyber-attack requires the same impact as a physical attack or a kinetic strike to prompt the use of force (Rule 11 in Tallinn Manual). The Tallinn Manual draws legal conclusions from the UN Charter, international law, and other international court cases and applies those norms derived and decisions reached to present-day cyber scenarios. However, the Tallinn Manual is not NATO policy, but rather a legal guide for anyone interested in law and its application to cyber warfare. One criticism of the first Tallinn Manual was that the manual reflected the viewpoints of the International Group of Experts and that there was no NATO-member consensus. The second popular criticism was that the Tallinn Manual created no new laws regarding cyberspace and failed to define solid criteria to determine if a cyber-attack required a collective defense response.

Rule 10 of the Tallinn Manual addresses the use of force: "a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[8] This prohibition is customary international law and extends to non-members of the UN unless attributable to a member state. Any threat of the use of force is illegal based on UN Charter 2(4). The impact on state sovereignty requires examination if the cyber-attack leaves physical and "virtual borders" vulnerable to attack. Russian meddling in the 2016 US election arguably degrades US democratic institutions and can be interpreted as a violation of sovereignty and of the political independence of the US.[9]

Rule 11 of the Tallinn Manual proposes an approach, also known as the Schmitt Analysis, which identified factors to determine a use of force. The factors are, but not limited to, severity, immediacy, directness, invasiveness, measurability of effects, responsibility, and state involvement.[10] Creating a multi-point scale of intensity would permit an effective application of the approach. Individual country inputs and contributions are required to reach an international consensus creating consistency when interpreting cyber operations and the use of force. As stated in the Tallinn Manual 2.0, "the law of armed conflict will govern cyber operations conducted in the context of that conflict" and the Schmitt analysis would be best applied here.[11] Cyber operations can potentially also bring conflict into existence and cyber operations can be "silent" as cyber activity can be undetected. Cyber operations would coincide with conflict (e.g. insurgencies), within the rules of engagement or cyber rules of engagement, and efforts to mitigate conflict would also mitigate cyber operations within. For example, cease-fires are often a tool to de-escalate conflict.

Rule 11 also references the ruling of *Nicaragua v. United States of America* (1986) ICJ 1 (settled by the International Court of Justice) that defined the concept of the threshold "scale and effects" as the "criteria that distinguish actions qualifying as an armed attack from those that do not."[12] The Nicaragua case determined that scale and effects were to distinguish between an armed attack and a "mere frontier incident," meaning "an isolated minor incident which, by the manner in which it takes place, cannot be mistaken for a threat to the safety of the State [and] would not qualify as armed attack under Article 51 of the UN Charter."[13] However, the criteria for scale and effects remain unsettled and "in essence to acknowledge that the atrocity of war cannot always be systematically quantified as per a certain set of guidelines."[14] The Tallinn Manual addresses a "composite armed attack," which is the sum of multiple attacks, and if the attacks constitute a use of force.[15] Another factor impacting if a cyber-operation is an armed attack is the definition of a cyber weapon. It is a piece of malware, ransomware, or other cyber technique used to commit cyberwarfare and reach a military or intelligence objective; it is a cyber tool that can cause physical damage or injury to persons and critical infrastructure.

The Tallinn Manual also addresses the use of force and actor involvement. It presents the idea that a use of force does not require a military or other armed forces. Citing the Nicaragua case, it claims that "arming and training a guerilla force [(not a conventional military)] that is engaged in hostilities against another State [qualifies] as a use of force."[16] Thus, supplying an organized group with malware and relevant training to conduct hostilities against a state would qualify as the use of force.[17] But, the Nicaragua case also states that funding guerillas does not qualify as the use of force; the cyber equivalent is funding a hacktivist group.[18] Cyber operations and actions by non-state actors in any form of conflict is a contentious issue. Many states conduct cyber operations by proxy, making attribution more difficult and allowing the offending state to deny involvement. Governments using proxy groups may fall under the category of cybercrime. Advancements in technology and the dark web make tracking cyber actors, their activity, and funding channels harder, but not impossible.

Countries and scholars alike turn to the Tallinn Manual 2.0 to develop a policy response to large-scale cyber-attacks such as malware or ransomware. The Tallinn Manual 2.0 "rests on the understanding that pre-cyber

international law applies to cyber operations, both conducted by and directed against states."[19] It addresses common incidents and threats that countries face on a day-to-day basis that fall below the threshold for using force or armed conflict in the fifth domain whereas the first Tallinn Manual focused on more severe cyber operations. The NATO Defense Ministers agreed upon a framework of political and legal principles to guide the integration of cyber into Alliance military operations at their meeting in November 2017.[20] Countermeasures, actions or omissions taken against a state to force it to comply with its own legal obligations, were integrated into the Tallinn Manual 2.0. Countermeasures, while ambiguous, are not considered a use of force, but rather the equivalent of a "hack-back" through cyber or non-cyber means and do not affect third-party countries (Rule 25 of Tallinn Manual 2.0).[21] It is widely accepted that countermeasures in response to cyber aggression should not amount to the use of force; an accepted idea in military cyber policy.

In June 2018, the CCDCOE released a statement regarding the NotPetya worm that wreaked havoc on multiple countries' local systems including Russia.[22] The center noted that NotPetya included leaked NSA exploits indicating the involvement of a state actor.[23] Collecting a ransom was most likely a way to cover that state-sponsored involvement.[24] The CCDCOE then suggested that NotPetya could have been practice, as it was sloppy and included no way to determine who paid the ransom.[25] Other technology and news outlets corroborated CCDCOE reporting and analysis on the use of National Security Agency (NSA) exploits. According to the Tallinn Manuals, the concepts of collective defense and self-defense do not apply since NotPetya did not produce results equivalent to a physical attack. According to the CCDCOE, NotPetya and WannaCry "[raise] questions about possible response options" as both were linked to state groups."[26] However, "if the [cyber] operation could be linked to an ongoing international armed conflict, then [the] law of armed conflict would apply, at least to the extent that injury or physical damage was caused by [the operation]," since WannaCry and NotPetya affected government systems, the cyber-attacks possibly violated state sovereignty.[27] Based on Rule 13 of the Tallinn Manual, "cyber operations that [result in the] brief or periodic interruption of non-essential cyber services, do not quality as armed attacks."[28] Additionally, NotPetya was designed to be destructive.[29]

The only documented incident of a cyber-attack causing physical damage would be "Stuxnet," which affected Iran's nuclear program's uranium enrichment processes.[30] The worm disrupted nuclear operations and damaged devices, which could have caused a nuclear disaster and mass casualties.[31] The deployment of the cyber weapon may be a use of force and violation of state sovereignty based on the Tallinn Manuals.

The Future of NATO and Cyber

Calls for a "Cyber NATO" increased after the July 2018 NATO summit. The CCDCOE may naturally evolve into a "Cyber NATO" as cyber is an enlargement issue. CCDCOE membership will most likely reflect global cyber-attack trends and focus on countering sophisticated ransomware, malware, and attacks on critical infrastructure. For example, the Black Sea Region has experienced an uptick in cyber-attacks originating from Russia. The cyber-attacks are driven by Russian aggression and Russia's foreign policy in the region. Multiple countries,

including Romania and Montenegro, have cited Russian cyber-attacks as reasons for seeking accession to the CCDCOE in 2019.[32] To counter cyber-attacks and foster collaboration, Romania strives to be the region's security leader and an outpost for NATO cyber operations.

Montenegro, once part of Serbia, joined NATO in 2017, angering Russia. Since joining, Montenegro has seen an increase in attacks on its institutions and media outlets executed by Russia's Fancy Bear cyber hacking group.[33] The Republic of Northern Macedonia membership in NATO and in the CCDCOE faces opposition from Russia who fears losing a foothold in the Balkans and in the Black Sea region. Greece blocked the Northern Republic of Macedonia's accession to NATO at the 2008 Bucharest Summit because of the name dispute.[34] The name change opens the door for the Republic of Northern Macedonia to join NATO. The Republic of Northern Macedonia is committed to enhancing cyber security with the assistance of the World Bank and the Global Cyber Security Capacity Center.[35] If Georgia and Ukraine joined the CCDCOE, since NATO membership is not required, their accession would likely prompt more cyber aggression from Russia or lead it to use cyber operations to support pro-Russian separatists in South Ossetia and Eastern Ukraine.

Australia and Japan, non-NATO members who are outside of the Euro-Atlantic region, joined the CCDCOE, as both countries have seen an increase in attacks from Russia. Australia's and Japan's memberships signal an expansion of concerted cyber response within the CCDCOE, but not necessarily within the Euro-Atlantic region. As cyber-attacks become more sophisticated and integrated into intelligence and military campaigns, the need may arise for coordinated global defensive cyber and policy responses. Within NATO, member states and prospective member states should reaffirm their commitment to institution building and strengthening, network protection, training cyber personnel, and reducing large-scale cyber-crimes.

Individual cyber security policies will only strengthen NATO cyber defenses and the CCDCOE. For example, Estonia's Defense Force, the combination of all its cyber elements, became operational on 1 August 2018 and will make responses more efficient since Estonia is a digital nation (many Estonian government operations reside in cyberspace) and "every conventional war today always has a clear cyber dimension."[36] Denmark will also join the CCDCOE in 2019, indicating European countries view cyber as a serious threat and cyber-attacks not confined to the US.[37]

While many questions surround the classification of a cyber use of force and the appropriate cyber response, the Tallinn Manual may influence a revival of UN efforts to establish law and cyber norms. Using international forums to reach consensus and develop scales of impact, while looking to regional bodies for guidance is a step towards developing criteria to determine policy, cyber, and military cyber responses. National-level cyber security strategies will assist in the application of the Tallinn Manual, and strengthen and support the CCDCOE mission and NATO cyber defenses. The CCDCOE, within the larger NATO framework, will support the NATO Cyber Operations Center and benefit from other NATO cyber academic institutions.

Samantha Brletich is a frequent contributor to multiple publications focusing on conflict, Russia and Central Asia, particularly economics, defense, regional relations, economics, and extremism and social issues. Ms. Brletich possesses a Master's Degree in Peace Operations Policy from George Mason University and is an employee of the U.S. Department of Defense. Opinions are her own.

1. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," NATO Cooperative Cyber Defence Center of Excellence, accessed August 7, 2018, https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf; "About Cyber Defence Center," NATO Cooperative Cyber Defence Center of Excellence, accessed August 7, 2018, https://ccdcoe.org/about-us.html; "Locked Shields 2017," NATO Cooperative Cyber Defence Center of Excellence, accessed August 7, 2018, https://ccdcoe.org/locked-shields-2017.html; "Exercise Crossed Swords Practised Cyber-Kinetic Operations in Latvia," NATO Cooperative Cyber Defence Center of Excellence, last modified February 5 2018, https://ccdcoe.org/exercise-crossed-swords-practised-cyber-kinetic-operations-latvia.html.
2. "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," NATO Cooperative Cyber Defence Center of Excellence, last modified July 8 2016, http://www.ccdcoe.org/sites/default/files/documents/NATO-160708-JointDeclarationNATOEU.pdf; "EU Cybersecurity Package: New Potential for EU to Cooperate with NATO," NATO Cooperative Cyber Defence Center of Excellence, last modified November 20, 2017, https://ccdcoe.org/eu-cybersecurity-package-new-potential-eu-cooperate-nato.html.
3. Kubo Mačák, "Is the International Law of Cyber Security in Crisis," accessed August 7, 2018, https://ccdcoe.org/cycon/2016/proceedings/09_macak.pdf.
4. Megan Wakefield, "International Criminal Tribunal for Cybercrime and Human Rights," Human Rights Brief, last modified October 10, 2012, http://hrbrief.org/hearings/18652-2/.
5. "Details of the Treaty No. 185, Convention on Cybercrime," Council of Europe, last accessed 15 August 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; Judge Stein Schjolberg, "An International Criminal Tribunal for Cyberspace," March 2012, accessed August 7, 2018, http://www.cybercrimelaw.net/documents/ICTC.pdf.
6. Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, "Cyber Attacks Against Georgia: Legal Lessons Identified", November 2008, last modified 31 August 2018. http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf.
7. "Research," NATO Cooperative Cyber Defence Center of Excellence, accessed August 7 2018, https://ccdcoe.org/research.html.
8. Schmitt, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013), 42-43.
9. Abby Vesoulis and Abigail Simon, "Here's Who Found That Russia Meddled in th 2016 Election," last modified August 7, 2018, http://time.com/5340060/donald-trump-vladimir-putin-summit-russia-meddling/. http://time.com/5340060/donald-trump-vladimir-putin-summit-russia-meddling/
10. Schmitt, Tallinn Manual, 48-52.
11. Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd Edition. (Cambridge University Press, 2017), 385.
12. "Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)," (International Court of Justice, June 27 1986), accessed August 7, 2018, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf; "Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (NICARAGUA v. UNITED STATES OF AMERICA) (MERITS)," (International Court of Justice), accessed August 7, 2018, http://www.icj-cij.org/files/case-related/70/6505.pdf; "Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (NICARAGUA v. UNITED STATES OF AMERICA) (MERITS)," (International Court of Justice), accessed August 7, 2018, http://www.icj-cij.org/files/case-related/70/6505.pdf.
13. Karl Zamanek, "Armed Attack," Oxford Public International Law, last accessed August 18, 2018, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241.
14. J. S. Caso, "The rules of engagement for cyber-warfare and the Tallinn Manual: A case study," The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent, 2014: 252-257. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6917470&isnumber=6917419.
15. Schmitt, Tallinn Manual, 56.
16. Ibid., 46.
17. Ibid.
18. Ibid.
19. "Research," NATO Cooperative Cyber Defence Center of Excellence, accessed August 7 2018, https://ccdcoe.org/research.html.
20. "NATO Defence Ministers agree to adapt command structure, boost Afghanistan troop levels," North Atlantic Treaty Organization, last modified November 10, 2017, https://www.nato.int/cps/ic/natohq/news_148722.htm.
21. Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd Edition. (Cambridge University Press, 2017), 133.
22. "NotPetya and WannaCry Call for a Joint Response from International Community," NATO Cooperative Cyber Defence Center of Excellence, last modified June 30 2018, https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html.
23. Ibid.
24. Ibid.
25. Ibid.
26. Tomáš Minárik, Raimo Peterson and Maarja Naagel, "WannaCry Campaign: Potential State Involvement Could Have Serious Consequences," last modified May 16 2017, https://ccdcoe.org/wannacry-campaign-potential-state-involvement-could-have-serious-consequences.html
27. "NotPetya and WannaCry Call for a Joint Response from International Community," NATO Cooperative Cyber Defence Center of Excellence, last modified June 30 2018, https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html.
28. Schmitt, Tallinn Manual, 55.
29. "NotPetya and WannaCry Call for a Joint Response from International Community," NATO Cooperative Cyber Defence Center of Excellence, last modified June 30 2018, https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html.
30. Kim Zetter, "An Unprecedented Look at Stuxnet: the World's First Digital Weapon," last modified November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
31. Ibid.
32. "Montenegro to Join NATO Cyber-Defence Center," Balkan Insight, last modified July 23, 2018, http://www.balkaninsight.com/en/article/montenegro-to-beef-up-cyber-defence-by-joining-nato-center-07-20-2018
33. Dusica Tomovic, Maja Zivanovic, "Russia's Fancy Bear Hacks its Way Into Montenegro," Balkan Insight, last modified March 5, 2018, http://www.balkaninsight.com/en/article/russia-s-fancy-bear-hacks-its-way-into-montenegro-03-01-2018.
34. Predrag Tasevski, "Macedonian Path Towards Cybersecurity," Information and Security: An International Journal, vol. 32 (2015), https://it4sec.org/system/files/3204_macedonia.pdf.
35. "Macedonia pledges to strengthen its cybersecurity capacity," Macedonian Information Agency, last modified February 1, 2018, https://www.mia.mk/en/Inside/RenderSingleNews/61/134090461.
36. "Defence Forces cyber command takes up operations", Err.ee, last modified August 1, 2018, https://news.err.ee/850719/defence-forces-cyber-command-takes-up-operations.
37. "Denmark to Join the CCD COE in Tallinn," Err.ee, last modified August 5, 2018, https://news.err.ee/829634/denmark-to-join-ccd-coe-in-tallinn.