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 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. 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.

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. 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.

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.
the law of armed conflict will govern cyber operations. As stated in the Tallinn Manual 2.0, consistency when interpreting cyber operations and are required to reach an international consensus creating an effective application of the approach. Individual country inputs and contributions 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. 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.” 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. 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.” The Tallinn Manual addresses a “composite armed attack,” which is the sum of multiple attacks, and if the attacks constitute a use of force. 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.

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. 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. 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.” 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. 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.” The Tallinn Manual addresses a “composite armed attack,” which is the sum of multiple attacks, and if the attacks constitute a use of force. 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.

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.” 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.

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. 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. 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.
According to the CCDCOE, NotPetya and WannaCry “raise questions about possible response options” as both were linked to state groups. 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. 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 qualify as armed attacks.” Additionally, NotPetya was designed to be destructive. The only documented incident of a cyber-attack causing physical damage would be “Stuxnet,” which affected Iran’s nuclear program’s uranium enrichment processes. The worm disrupted nuclear operations and damaged devices, which could have caused a nuclear disaster and mass casualties. 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,
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 defense 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.

16. Ibid., 46.
17. Ibid.
18. Ibid.
23. Ibid.
24. Ibid.
25. Ibid.
31. Ibid.

Samantha Britetch 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. Britetch 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.