National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

NATO'S CYBER DEFENCE POLICY: A 21ST CENTURY MAGINOT LINE?

Maj R.W.C. Tyler

JCSP 43	PCEMI 43
Exercise *Solo Flight*	Exercice *Solo Flight*
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 – PCEMI 43
2016 – 2017

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

NATO'S CYBER DEFENCE POLICY: A 21ST CENTURY MAGINOT LINE?

Maj R.W.C. Tyler

"This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

Word Count: 5341

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Compte de mots: 5341

INTRODUCTION

Enhanced Forward Presence (EFP) is the North Atlantic Treaty Organization's (NATO) deployment to the Baltic States in an attempt to deter further Russian expansionism.[1] This deployment will see NATO forces standing against an old foe. However, this time in addition to the traditional land, air, and sea based stand-off, with all the capabilities that modern day militaries bring; this new deployment will add a new battlespace. On this new battlefield information will be king, with battles being fought to win the influence of the general public using both information and disinformation. In addition to these information operations, the ongoing development of the cyber realm will further stress NATO/Russian stability. Much like the development of air warfare during the 20th century, this century is set to be defined by the development of cyber warfare.

NATO's first exposure to this new form of war occurred in 2007 when, allegedly, Russia initiated a multi-pronged assault on Estonia over the movement of a WWII Soviet memorial.[2] The attack included information operations, the use of dissidents to initiate violent protests both in Tallinn and at the Estonian Embassy in Moscow, and a cyber-attack that over the span of weeks, crippled Estonian banks and sporadically shut down government communications.[3] This provided the wakeup call needed for NATO to take action on the cyber front; though it has not been enough to convince NATO to take advantage of the full spectrum of cyber operations.

Discussing the entirety of state based cyber warfare is too large a topic to be addressed here; however one aspect that has not been fully addressed within NATO is that of offensive cyber warfare, a must when considering further Russian cyber operations in Georgia and

[1] NATO, "Boosting NATO's Presence in the East and Souteast," last modified 15 Mar 2017, http://www.nato.int/cps/en/natohq/topics_136388.htm?selectedLocale=en.

[2] Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy*, Vol 27, No 3 (May 2008): 227.

[3] *Ibid.*, 228.

Ukraine.[4] This paper will argue that NATO must add an offensive cyber capacity to its current defensive posture. Doing so will give NATO commanders an additional tool, and, over the longer term, will add a sense of stability to the cyber battlefield between NATO and Russia, much like it did on the nuclear front.

Developing an offensive cyber strategy within NATO is no simple task. First of all there is disagreement amongst NATO members on the role of cyber warfare.[5] Second, cyber capacities vary greatly amongst NATO countries, [6] and much like other highly technical weapons, states are hesitant to share their research and development. Third, there remain serious questions about the use of cyber warfare, primarily: attribution, the role of non-state actors and cyber targeting.

In order to address these issues and demonstrate why an offensive cyber capacity is so crucial, the first step is to understand the current NATO defensive policy, how it developed and in response to what events. From here the concept of NATO forces conducting offensive operations can, in general, be used to show why an offensive cyber capacity is not counter to NATO's defensive posture. How to use this offensive option must also be addressed, in this sense the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) provides an excellent starting point, especially in the development of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[7] This paper will finish by discussing how NATO's declaration of an offensive capacity may lead to enhanced stability in the NATO/Russia relationship.

[4] James Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence," *CCDCOE Tallinn Paper* No 8 (2015): 5.

[5] NATO, *The North Atlantic Treaty* (1949), 1-2.

[6] Lewis, *The Role of Offensive Cyber Operations*…7.

[7] NATO CCDCOE, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," accessed 11 Apr 2017, https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf.

NATO's cyber operations have been the subject of much discussion, though heavily focused on either the technical aspects of defending the NATO networks, or the legal considerations of the cyber realm. What is lacking is a serious discussion of how increasing NATO's cyber posture to include offensive operations may be beneficial to the Alliance. The development of the CCDCOE, a NATO centre of excellence that strives to provide expertise on cyber "technology, strategy, operations and law,"[8] has provided an excellent resource for tracking the discussion on cyber within NATO.

This discussion is helped particularly by the Tallinn Papers series. In his contribution to the series, James Lewis argues the need for an offensive capability and some of the issues this may create; ultimately, he concludes that: "A cyber defensive orientation is the equivalent of a static defence, defending fixed positions rather than manoeuvering, and conceding initiative to opponents."[9] This same train of thought was expressed earlier in the development of the United States Cyber Command. In an article to *Foreign Affairs*, then Deputy Secretary of Defence William Lynn III stated: "In cyberspace the offense has the upper hand…adept programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions. In an offense-dominant environment, a fortress mentality will not work."[10]

Based on this thinking the concept of offensive cyber operations has slowly begun to creep into the NATO mindset. In 2016 the former Deputy Secretary General of NATO, Alexander Vershbow stated: "My own view is given the evolving nature of warfare, NATO would be tying one hand behind its back if it deprived itself at least of the option of cyber

[8] NATO CCDCOE, "About Us," last accessed 11 Apr 2017, https://ccdcoe.org/about-us.html.
[9] Lewis, *The Role of Offensive Cyber Operations*…12.
[10] William Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, Issue 5 (Sep/Oct 2010), 99.

offense."[11] This was followed by a comment that NATO is currently debating the role of offensive cyber; however, it is highly likely that if NATO is having these discussions internally, they are classified and thus not available for analysis in this forum.

The literature is not heavy on the role that NATO could have if it were to adopt a more balanced cyber posture, there is enough to demonstrate that the idea is being considered. Therefore this paper will expand on several points to stress the benefits to NATO/Russian relations if NATO were to declare an offensive capacity.

DEFENSIVE VS OFFENSIVE OPERATIONS

Before delving into the creation of NATO's cyber policy it is important to discuss what is meant by cyber operations. As per the CCDCOE there are few agreed upon terms when it comes to cyber;[12] however in accordance with their cyber definitions resource the United States Department of Defence (DOD) defines cyber operations as: "The employment of cyber capabilities where the primary purpose is to achieve objectives in, or through, cyberspace."[13] Further, the DOD differentiates between defensive and offensive operations; defensive operations are defined as: "Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[14] Whereas offensive operations are defined as: "Cyber operations intended to project power by the application of force in and through cyberspace."[15]

[11] Jordana Mishory, "Vershbow: NATO Needs to Invest in Offensive Cyber Capability," *Inside the Pentagon*, Vol 32, No 51 (22 Dec 2016).

[12] NATO CCDCOE, "Resources: Cyber Definitions," accessed 18 Apr 2017, https://ccdcoe.org/cyber-definitions.html.

[13] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (Washington, DC: Joint Chiefs of Staff, 2013), I-1.

[14] *Ibid.*, GL-4.

[15] *Ibid.*

Therefore the key consideration between offense and defense is the projection of force. The fact that the force projected is a collection of ones and zeros, whizzing through cyberspace, as opposed to bullets flying through the air is immaterial. What does differentiate cyber from the physical realm is that there is no physical action to define a cyber-attack. As described by Thomas Rid, in conventional warfare: "A combatant's or insurgent's triggering action – say pushing a button or pulling trigger – will rather immediately and directly result in casualties."[16] Whereas within the realm of cyber operations: "In an act of cyber war, the actual use of force is likely to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties."[17]

There are few examples of this "sequence of causes and consequences" but the most famous is likely the Stuxnet attack on Iranian nuclear centrifuges. This demonstrated how a virus, allegedly, created by US and Israeli forces, managed to infiltrate specific computers within the nuclear facility in Natanz. Once into the system the virus launched its own software, reprogramming the motors which controlled the speed at which the centrifuges would spin. This forced the centrifuges to change speeds at rates they were not designed for, ultimately destroying the centrifuge motors.[18] In this case software, through a long sequence of events managed to result in physical damage, counter to the conventional means of destroying equipment.

THE ROAD TO WARSAW

To understand NATO's current Cyber Defence Pledge it is important to understand how cyber became important to the North Atlantic Council. The first mention of cyber came following the 2002 Prague Summit, where NATO leaders pledged the: "Initiation of measures to

[16] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol 35, No 1 (2012): 9.

[17] *Ibid.*

[18] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, Vol 53, No 1 (2011), 23-25.

strengthen defence against cyber-attacks."[19] A rather vague and non-committal intent, somewhat excusable as few in the world truly understood the potential of the cyber threat; it did lead to the creation of the NATO Computer Incident Response Capability (NCIRC) and the NATO Cyber Defence Programme.[20] This was followed by similar comments at the 2006 Riga Summit.[21] The benefit of hindsight allows us to see that for NATO may not have been taking the cyber threat seriously enough.

This cyber threat became much clearer in April 2007. As previously discussed, the Estonian government decided to move a monument commemorating the Soviet liberation of Estonia during World War II from a prominent location within the city of Tallinn to a nearby grave yard; a move which was considered a major affront to the Russian minority population living in Estonia. [22] Shortly thereafter a well-organized, and highly coordinated, unconventional assault was mounted on the government and people of Estonia; the first major interstate cyber-attack.[23] The coordinated operation began with violent demonstrations in Tallinn, initiated by the Russian minority population. These were timed to happen concurrently with demonstrations at the Estonian Embassy in Moscow. Simultaneously, an information operation targeting Russian minorities in Estonia, and the Western media, was launched to destabilize the Estonian government, labeling them as fascist and illegitimate.[24]

While these physical and media attacks were ongoing, Russian hackers began a two pronged cyber operation. The first strikes were nuisance attacks on Estonian government

[19] North Atlantic Treaty Organization, *The Prague Summit and NATO's Transformation*: *a Reader's Guide* (Brussels, NATO, 2003), 12.

[20] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," *Defence Studies*, Vol 15, No 4 (2015), 305.

[21] North Atlantic Treaty Organization, *Riga Summit Declaration*, 2006, last modified 29 Nov 2016, http://www.nato.int/cps/en/natohq/official_texts_37920.htm.

[22] Blank, *Web War I*…227.

[23] Geoff Van Epps, "Common Ground: US and NATO Engagement with Russia in the Cyber Domain," *Connections: The Quarterly Journal*, Vol 12, No 4 (Fall 2013): 29.

[24] Blank, *Web War I*…228.

websites, replacing the content with anti-Estonian propaganda declaring an apology for the movement of the monument.[25] More serious attacks followed with highly choreographed distributed denial of service (DDOS) attacks on Estonia's two largest banks, government communications and internet infrastructure, and media outlets. This resulted in banking restrictions lasting for several days and short, sporadic, disruptions in government communications lasting several weeks.[26]

While the cyber-attacks on Estonia resulted in little longer term damage, they demonstrated a capability. Though it was never fully proven that the Russian government was responsible for the attacks; the circumstantial evidence, in conjunction with the organization and finances required, make a very compelling argument for a Russian government backed assault.[27] Additionally, the psychological effects on both the people of Estonia and the larger political arena were far more important. These attacks were an obvious violation of Estonian sovereignty, and likely the first time the world had seen one state violate the sovereignty of another within the cyber realm.

In the wake of the Estonian attacks, NATO established the Cooperative Cyber Defence Centre of Excellence, in Tallinn, Estonia, and tasked to conduct research and training on cyber warfare.[28] Additionally, NATO published its first Policy on Cyber Defence in January 2008, reinforcing the defensive nature of NATO cyber operations. While this policy would undergo minor changes in 2012 and 2014, the defensive nature remained steadfast.[29] Finally during the 2016 Warsaw Summit the council added to its cyber policy by recognizing the importance of the

[25] Kenneth Geers, *Strategic Cyber security* (Tallinn: NATO CCDCOE, 2011), 85.

[26] *Ibid.*, 84.

[27] Van Epps, *Common Ground*…30.

[28] North Atlantic Treaty Organization, "NATO Opens New Centre of Excellence on Cyber Defence," last modified 14 May 2008, http://www.nato.int/docu/update/2008/05-may/e0514a.html.

[29] North Atlantic Treaty Organization, "Cyber Defence: Evolution," last modified 17 Feb 2017, http://www.nato.int/cps/en/natohq/topics_78170.htm.

cyber realm, it declared cyberspace as a distinct domain of operations: “Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.”[30]

While the previous paragraph glossed over the 2014 Wales Summit, one point that came from the summit needs to be addressed as it speaks to the stability issues currently affecting relations between NATO and Russia. A key outcome of the summit was the Enhanced Cyber Defence Policy, and in particular was the addition of a cyber-attack to the list of actions that could trigger an Article 5 response:

> Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO’s core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.[31]

What would the result have been had this policy been in effect in 2007 and Estonia had invoked Article 5? Would this have resulted in action against Russia? If so, what exactly could NATO have done? Whereas the most politically effective response may have been a tit-for-tat cyber exchange, being limited by a purely defensive policy removes that possibility; thus NATO would have been limited to diplomatic, economic, or physical responses. Further, what is the ‘red-line’ that must be crossed before a cyber-attack warrants a physical strike in response? Increasing the number of unknowns will lead to further instability between NATO, Russia, and other non-NATO states.

[30] North Atlantic Treaty Organization, “Warsaw Summit Communique,” last modified 9 Jul 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[31] North Atlantic Treaty Organization, “Wales Summit Declaration,” para 72 (2014), last modified 26 Sep 2016, http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber.

NATO – OFFENSE VS DEFENSE

It becomes obvious that within its current cyber policy NATO is attempting to live up to its collective defence roots, but does this align with recent changes within the Alliance and expansion into more offensive roles. As per the preamble to the North Atlantic Treaty, NATO was established with the sole purpose of providing the collective defence of its member states: "They [member states] are resolved to unite their efforts for collective defence and for the preservation of peace and security."[32] This intent held true throughout the Cold War when there were no requests, or requirement, to deploy NATO forces, beyond Western Europe; NATO's primary concern from 1949-1989 was to deter potential aggression against NATO states.[33] However, with the end of the Cold War, and for reasons that go beyond this paper, NATO's purpose began to evolve, with a focus more on the global "preservation of peace and security" than the collective defence aspect of the North Atlantic Treaty.

This shift began in the mid 1990's with the out-of-area bombing of Bosnia and Kosovo, in order to force an end to Slobodan Milosevic's genocide. Was continued in Afghanistan when NATO forces supported the overthrow of the Taliban government after 9/11; followed by the attempted re-stabilization of the country. Most recently this shift in focus saw the NATO lead air campaign overthrow the Qaddafi regime in Libya. Over the past twenty-five years NATO has expended from being a purely defensive organization to one concerned not only with the safety of its member states but also with global peace and security.

In order to uphold this peace and security NATO, through its member states, maintains multiple capabilities, on land, in air and on/under water. The vast majority of these capabilities hold both a defensive and offensive capacity. The current use of fighter aircraft to conduct the air

[32] North Atlantic Treaty Organization, *The North Atlantic Treaty*…1.

[33] North Atlantic Treaty Organization, "Operations and Missions: Past and Present: From 1949 to the early 1990s," last modified 21 Dec 2016, http://www.nato.int/cps/en/natohq/topics_52060.htm.

policing mission over Romania demonstrates a predominantly defensive posture; however when those same aircraft were used to bomb Libya their role was obviously offensive in nature. The same argument can be used with land forces; EFP will soon be in place in the Baltics, with the four Battle Groups providing a defensive posture to deter potential Russian aggression. But, the deployment of NATO forces to Afghanistan to conduct counter-insurgency operations, in order to stabilize the country, is an example of how NATO ground forces can be used in an offensive role.

Therefore, if it can be established that NATO is more than a defensive coalition to protect its member states, and that weapons systems within NATO can maintain both a defensive and offensive capacity. Then the same should hold true for cyber operations. While NATO’s primary capacity must be in the protection of its own networks, it should be capable of conducting offensive cyber operations, without betraying its fundamental collective security mandate.

In this vein an offensive capability for NATO could have multiple functions: it may be used pre-emptively, striking an adversary who is preparing to attack NATO. It may be used as a stand-alone means, giving the Alliance, and NATO commanders, a tool to strike other states; as a political message or in response to an attack. Or, it may be used in conjunction with other capabilities as part of a larger operation, possibly degrading an adversary’s Integrated Air Defence System (IADS) prior to aerial bombing. However, to accomplish this dual offence/defence capability several issues need to be addressed.

INSTITUTIONAL ISSUES WITH OFFENSIVE CYBER

There are several institutional reasons why an offensive cyber capability will be difficult to implement within NATO. For one, only a handful of NATO countries have an advanced level of cyber capabilities, namely the US, UK, France, and Germany.[34] Second, and linked to the previous point, is the secretive nature of cyber research. Much like the research that went into the development of nuclear weapons, states do not want to share their capabilities or the tools that they have developed. Third there is a distinct difference within the Alliance on how cyber should be used; with the US generally preferring a more offensive approach, and the European Union countries leaning to a more defensive orientation.[35]

From the defensive cyber perspective the sharing of abilities has been addressed through the creation of the NATO Computer Incident Response Capability, tasked with providing a combined capability to defend NATO's networks;[36] and the Cyber Defence Management Authority, which strives to: "integrate the alliance's cyber security functions and provide support for NATO members in the event of cyber-attacks."[37] In this way not only can NATO protect its networks, but member states benefit from the capabilities of the whole. Further, through the pooling of resources two distinct projects have been initiated to ensure the sharing of information, and best practices, amongst member states: the Multinational Cyber Defence Capability Development project; and the Multinational Cyber Defence Education and Training project. The culmination of this cooperation is seen at the NATO Cyber Range and on annual cyber exercises that focus on member states integrating cyber capabilities.[38]

This highlights that although there is a disparity in cyber capabilities across the Alliance; NATO has developed a means to share information and tools that will see collective defence strengthened. But how can NATO address the larger disparity in offensive capabilities?

[34] Lewis, *The Role of Offensive Cyber Operations*…7.

[35] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," *Defence Studies*, Vol 15, No 4 (2015), 310-312.

[36] Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy*, Vol. 34, No. 1 (2013), 54.

[37] Burton, *NATO's Cyber Defence*…307.

[38] North Atlantic Treaty Organization, "Cyber Defence: Principle Cyber Defence Activities," last modified 17 Feb 2017, http://www.nato.int/cps/en/natohq/topics_78170.htm.

As mentioned above, offensive cyber capabilities are highly secretive. The time and resources required to develop a cyber weapon are immense; developing the Stuxnet virus was believed to have taken the equivalent of several man years.[39] Further, the intelligence assets that must have been required to identify the four zero-day events required to allow the virus to work must have been intense.[40] After all this work and expenditure of resources, shortly after the virus was released it was isolated, reverse engineered and patches developed to prevent the virus from being effective.[41] Showing how even after the time and money required to develop these weapons they are only effective once.

This reinforces the idea that the few NATO members with the ability to conduct offensive operations are going to be very hesitant to release control of their assets to NATO command. However, this is not vastly different from how NATO controlled and commanded nuclear weapons during the Cold War. Throughout the Cold War a process existed that would allow NATO command to warn nuclear capable states that there may be a requirement for the use of their weapons. This advanced notice would allow the military and political command structures of these states to decide if they were willing to support. If approved, the weapons would then be released to NATO control for employment, if required.[42]

In much the same way, cyber weapons can be developed and maintained by individual states, with their request for use being sent to governments by NATO commanders. This allows states to decide if they are willing to release the weapon, accounting for the inherent risks of losing the research and intelligence that would have been invested in its development. This

[39] Kim Zetter, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target," *Wired*, last modified 23 September 2010, https://www.wired.com/2010/09/stuxnet-2.

[40] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, Vol 53, No 1 (2011), 24.

[41] *Ibid.*, 23 and 27.

[42] Lewis, *The Role of Offensive Cyber Operations*…8.

process may actually be more suitable to the cyber domain as the longer timelines required to launch a cyber-attack would allow for a more thorough analysis of the situation.

Joe Burton in his writing on NATO's cyber defence discusses a transatlantic divide between the US and Europe.[43] He attempts to show how the US has adopted a more hard power approach to cyber through actions such as Presidential Decision Directive 20 which allows: "the US military the authority to conduct more aggressive cyber operations to thwart cyber-attacks against US systems."[44] This in contrast to Europe, where the EU has established a Cyber Security Strategy which: "is based on promoting norms in cyberspace, encouraging dialogue between nations, enhancing technical capacity and resilience, and fighting cybercrime."[45]

While this divide could threaten to prevent the adoption of an offensive capacity it must be mentioned that several European countries are actively pursuing offensive tools, namely the UK, France and Germany.[46] This divide adds further strength to the argument that the most effective way for NATO to move into the offensive cyber realm is to allow member states to conduct the research and development of the weapons, with an agreement that they will be shared with NATO, when needed.

CYBER TARGETING

While the nuclear model may provide a structure for the deployment of an offensive weapon, national governments, and NATO commanders, are going to have far more to consider than just the resources invested in the weapon. If a decision is made to initiate a cyber-attack, who is going to be targeted and exactly what targets are valid?

[43] Burton, *NATO's Cyber Defence…*310.
[44] *Ibid.*, 311.
[45] *Ibid.*, 312
[46] *Ibid*.

To answer these questions the first consideration is attribution. The nature of the cyber realm is such that borders are meaningless and anonymity is paramount, thus demonstrating who designed and choreographed a cyber-attack is incredibly complicated. Confounding the situation further, hackers can make an attack appear to come from anyplace in the world. Such was the case in Estonia, where the hackers who launched the DDOS attack commandeered computers from around the world, creating a global network of botnets.[47] Therefore, how is NATO, or an individual member, to prove who initiated an attack, to the degree required to satisfy a request to invoke Article 5? Furthermore, assuming it is possible to prove from which country the attack originated, is it possible to demonstrate who within the country designed and initiated the attack? Was it the state, or the actions of a non-state actor?

There are means of conducing cyber forensics. When a hacker launches an attack the code becomes available for everyone to see. This code can be dissected and analyzed looking for the cyber equivalent of fingerprints; every hacker, or group, tends to write code in a specific manner which may assist in identifying its origins.[48] However, this can take a great deal of time and likely will not entirely answer the question of who was responsible. A more likely scenario for NATO would see a cyber-attack as just one component of a larger campaign. Again, the attacks on Estonia are a good example. While the cyber-attacks were key in the larger campaign, the incitement of the Russian minority in Estonia, along with violent protests in Moscow, provided the circumstantial evidence that Russia, or at least Russian supported proxies, were responsible for the attacks.

The proxy situation further complicates the issue, while an attack may be attributable to a specific country, what if the evidence shows that the state had little to no knowledge and the

[47] Blank, *Web War I…*230.

[48] David Glance, "How We Trace the Hackers Behind a Cyber Attack," *The Conversation*, 3 December 2015, http://theconversation.com/how-we-trace-the-hackers-behind-a-cyber-attack-51731.

attack was perpetrated by a non-state actor. Or asked another way, what is the responsibility of the state in regards to non-state actors operating from within their territory?

Michael Schmitt, the Senior Fellow for the CCDCOE and the director of the Tallinn Manual project, through his writings on how cyber intersects with International Humanitarian Laws (IHL), makes a strong case that, at least to a certain degree, states have an obligation to prevent, or disrupt, offensive cyber operations launched from its territory.[49] Failure to do this may be considered a breach of trust by the state and may open the state to a proportional response, up to and including physical attack.[50] The *Tallinn Manual* continues this thought through the application of Rules 5 and 7.

Rule 5 states that: "A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other states."[51] In the expanded text on Rule 5 it is clear that this is directed at states that know an attack is planned, or ongoing, and fails to take the appropriate actions to prevent or disrupt that attack. An important aspect is the knowledge of a planned or ongoing attack, there must be evidence that the state knew:

> A State will be regarded as having actual knowledge if, for example, State organs such as intelligence agencies have detected a cyber-attack originating from its territory or if the State has received credible information (perhaps from the victim State) that a cyber-attack is underway from its territory.[52]

It is also important to note that actions to prevent or disrupt must be reasonable: "The nature, scale, and scope of the (potential) harm to both States must be assessed to determine whether this remedial measure is required. The test in such circumstances is one of

[49] Michael Schmitt and Liis Vihul, "Proxy Wars in Cyberspace," *Fletcher Security Review*, Vol I, Issue II (Spring 2014), 62.

[50] *Ibid*., 58.

[51] Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* 1st Edition (UK: Cambridge University Press, 2013), 26.

[52] *Ibid*., 28

reasonableness."[53] Thus it may not be reasonable to expect the state in question to pull its entire network down to prevent an attack; unless the outcome from that attack is believed to be so heinous as to demand such a drastic measure.

The counterpoint to Rule 5 is Rule 7, which, to some degree, delinks the actions of the non-state actor from the state:

> The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to the state, but it is an indication that the state in question is associated with the operation.[54]

Thus just because the attacks on Estonia were believed to have originated in Russia does not mean the Russian government was responsible for the actions of the Nashi Youth Group.[55] However, it does link the Russian government, hence the importance of Rule 5. What knowledge did the Russian government have on the cyber operations of the Nashi group? What actions did the government then take to disrupt the attack? Based on the answers to these questions, the Estonian government may have had grounds to retaliate against Russia.

Within the legal arguments for the use of cyber operations, there are grounds that would allow NATO to launch cyber counter-attacks, whether the attack originated from a state or a non-state actor. Therefore if NATO were to decide to launch a retaliatory strike, or even a pre-emptively strike, to prevent an attack on a member state, it must ensure that it strikes a valid target. This raises further difficult questions for NATO commanders, what is a valid cyber target and how is collateral damage assessed in the cyber realm.

The full legalities of cyber targeting are highly complicated, and again, beyond the scope of this paper; however there are three distinct points to be raised. First of all, generally speaking

[53] *Ibid.*, 27.
[54] *Ibid.*, 34.
[55] Schmitt, *Proxy Wars in Cyberspace*…56.

cyber warfare is no different than other forms of war, target selection must be distinct and the effect must be proportional.[56] This first consideration is incredibly difficult, especially considering the dual-use aspect of the cyber realm. There are few aspects of cyber infrastructure that is not used by both military and civilian means. In most nations, military emails share the same infrastructure as civilian; military air traffic control networks are integrated to ensure seamless control of both civilian and military aircraft. For this reason, being able to identify and affect a purely military target is incredibly difficult.

The follow-on to distinction is collateral damage, what affect will the strike on a legitimate military target have on the civilian infrastructure surrounding it. Within the cyber realm this analysis of collateral damage is problematic. While it is easy to determine blast patterns and likely probability of damage to civilian infrastructure when dropping a bomb; it is far more difficult to determine the second or third order effects of a cyber weapon. For example, what is the effect of taking a nations air traffic control system offline? That nation's ability to launch and coordinate military aircraft will be reduced, but what is the impact on civilian aircraft? Will this result in civilian aircraft crashing or colliding; if the system is forced offline long enough will it have a longer term effect on that nation's economy? These are all effects that must be considered, and as per IHL, precautionary measures taken to minimize the harm to civilians.[57]

A more interesting point, however, is the impact of cyber operations on other more kinetic options. Under IHL there is a: "requirement to consider alternative weapons, tactics and targets in order to minimize civilian incidental harm."[58] Thus if NATO were to get involved in

[56] Michael Schmitt, "The Law of Cyber Targeting," *CCDCOE Tallinn Paper*, No 7 (2015), 7-9.
[57] *Ibid.*, 17.
[58] *Ibid.*, 18.

another large scale operation against a state with a modern IADS an offensive cyber operation against the heart of the system may be more appropriate, minimizing potential collateral damage.

Cyber targeting is a field which will need considerably more research and guidance before NATO is ready to fully exploit an offensive capability. Though, on achieving this capability NATO forces may become more efficient and less likely to cause unintended harm to civilians. In order to create an effective cyber targeting tool NATO could look to adopt the rules and guidelines laid out in the *Tallinn Manual on the International Law Applicable to Cyber Warfare.* This was a project sponsored by the CCDCOE and authored by twenty international law experts. It effectively lays out the *jus ad bellum* and the *jus in bello* for cyber warfare. As a product of NATO aligned experts its adoption should not be difficult.

STABILIZING CYBER RELATIONS

Based on the issues listed above, both organizational and legal, it will not be easy for NATO to adopt a balanced defensive and offensive cyber posture. However, as this paper has intended to show, this hybrid posture, over the longer term, will prove more beneficial to the relationship between NATO and non-NATO states. There is a stability formed when all understand the nature of the game. As things currently stand there is no understood response to a cyber-attack on a NATO member; according to Lewis, Russia believes that: “NATO’s new cyber doctrine is destabilizing as it threatens to use conventional or even nuclear responses.”[59]

NATO could level the playing field by declaring that it has broadened its mandate to include offensive cyber operations. It has already been announced that a cyber-attack on NATO may result in some form of response; by declaring an offensive capability it makes it more likely that the response will be cyber in nature, not physical. This may result in a reanalysis by all non-NATO states to consider their actions against NATO networks.

[59] Lewis, *The Role of Offensive Cyber Operations*…6.

There is a concern that by going down this road NATO is opening itself up to a cyber arms race, akin to the nuclear race from the Cold War.[60] It must be noted, however, that the nuclear arms race ultimately created its own sense of stability. Mutually Assured Destruction meant that NATO and the USSR knew exactly what would happen if either attempted a nuclear first strike. While this analogy does not align perfectly with the cyber warfare model, it does demonstrate that matching offensive capabilities can provide stability.

In the end however, to achieve this stability this posture change must be made clear to all. As per Ilai Saltzman's writings on how cyber can affect the offense-defense balance: "For [offensive] cyber capabilities to actually influence calculations and decisions in matters of war and peace, leaders and policymakers must be aware of these technologically advanced capabilities and acknowledge their strategic advantages."[61] Thus not only must NATO decide to adopt an offensive and defensive posture but it must ensure that all understand their desire to use the offensive aspect.

CONCLUSION

This paper has attempted to lay out a case for NATO to declare an offensive cyber posture, in conjunction with its current defensive capabilities. Several issues have been addressed: the birth of the current NATO Enhanced Cyber Defense Policy. The expected difficulties in establishing an offensive capability, namely a process that would allow the few NATO states who maintain a credible cyber offensive capacity to support NATO, while still maintaining command and control of their weapons. The legal considerations in launching a cyber-attack, especially how NATO can determine who was responsible for an attack and what could legitimately be targeted in a counter-attack. How the Tallinn Manual could be considered a

[60] Geers, *Strategic Cyber security*…121.
[61] Saltzman, *Cyber Posturing and the Offense-Defense Balance*...44.

template to be used by NATO for guiding the offensive use of cyber weapons. Finally, the potential for improving stability between NATO and non-NATO states, most importantly Russia, through a declared offensive cyber posture.

NATO received a wakeup call in Estonia; however it decided that the best response was to adopt a purely defensive model. Further actions by Russia in Georgia and Ukraine have highlighted Russia's cyber capabilities and their willingness to use them.[62] Therefore as NATO deploys forces in support of EFP it must put itself in a position where it is capable of not only defending its forces against Russia's cyber techniques, but is also capable of striking back against state and non-state actors. By maintaining a purely defensive posture the alliance has artificially hamstrung itself, has placed its commanders on an unequal footing, and in the end destabilized relations with non-NATO states.

[62] Lewis, *The Role of Offensive Cyber Operations*…5.

BIBLIOGRAPHY

Blank, Stephen. “Web War I: Is Europe’s First Information War a New Kind of War?” *Comparative Strategy*, Vol 27, No 3 (May 2008): 227-247.

Burton, Joe. “NATO’s Cyber Defence: Strategic Challenges and Institutional Adaptation.” *Defence Studies*, Vol 15, No 4 (2015): 297-319.

Czosseck, Christian, Rain Ottis and Anna-Maria Taliharm. “Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security.” *International Conference on Information Warfare and Security* (Jul 2011): 57-64.

Daugirdas, Kristina and Julian Davis Mortenson. “NATO Affirms that Cyber Attacks May Trigger Collective Defense Obligations.” *The American Journal of International Law*, Vol 109, No 1 (Jan 2015): 211-213.

Farwell, James and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival*, Vol 53, No 1 (2011): 23-40.

Geers, Kenneth. *Strategic Cyber Security*. Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2011.

Glance, David. “How We Trace the Hackers Behind a Cyber Attack. *The Conversation*, 3 December 2015. http://theconversation.com/how-we-trace-the-hackers-behind-a-cyber-attack-51731.

Gunneriusson, Hakan and Rain Ottis. “Cyberspace from the Hybrid Threat Perspective.” *European Conference on Information Warfare and Security* (Jul 2013): 98-105.

Lewis, James. “The Role of Offensive Cyber Operations in NATO’s Collective Defence.” *CCDCOE Tallinn Paper*, No. 8 (2015).

Lynn, William III. “Defending a New Domain.” *Foreign Affairs*, Vol. 89, Issue 5 (Sep/Oct 2010): 97-108.

Mishory, Jordana. “Vershbow: NATO Needs to Invest in Offensive Cyber Capability.” *Inside the Pentagon*, Vol 32, No 51 (22 Dec 2016).

North Atlantic Treaty Organization. “Boosting NATO’s Presence in the East and Souteast.” Last modified 15 Mar 2017. http://www.nato.int/cps/en/natohq/topics_136388.htm?selectedLocale=en.

North Atlantic Treaty Organization. “Cyber Defence: Evolution.” Last modified 17 Feb 2017. http://www.nato.int/cps/en/natohq/topics_78170.htm.

North Atlantic Treaty Organization. “Cyber Defence: Principle Cyber Defence Activities.” Last modified 17 Feb 2017. http://www.nato.int/cps/en/natohq/topics_78170.htm.

North Atlantic Treaty Organization. “Operations and Missions: Past and Present: From 1949 to the early 1990s.” Last modified 21 Dec 2016. http://www.nato.int/cps/en/natohq/ topics_52060.htm.

North Atlantic Treaty Organization. “Press Conference by NATO Secretary General Jens Stoltenberg.” Last modified 14 Jun 2016. http://www.nato.int/cps/en/natohq/opinions_ 132349.htm?selectedLocale=en

North Atlantic Treaty Organization. “NATO Opens New Centre of Excellence on Cyber Defence.” Last modified 14 May 2008. http://www.nato.int/docu/update/2008/05-may/e0514a.html.

North Atlantic Treaty Organization. *Riga Summit Declaration*, 2006. Last modified 29 Nov 2016. http://www.nato.int/cps/en/natohq/official_texts_37920.htm.

North Atlantic Treaty Organization. *The North Atlantic Treaty*. Brussels: NATO, 1949. http://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty _en_light_2009.pdf.

North Atlantic Treaty Organization. *The Prague Summit and NATO’s Transformation*: *a Reader’s Guide.* Brussels: NATO, 2003. http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf

North Atlantic Treaty Organization. “Warsaw Summit Communique.” Last modified 9 Jul 2016. http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

North Atlantic Treaty Organization. “Wales Summit Declaration.” Para 72 (2014). Last modified 26 Sep 2016. http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber

North Atlantic Treaty Organization, Cooperative Cyber Defence Centre of Excellence. “About Us.” Last accessed 11 Apr 2017. https://ccdcoe.org/about-us.html.

North Atlantic Treaty Organization, Cooperative Cyber Defence Centre of Excellence. “Resources: Cyber Definitions.” Accessed 18 Apr 2017. https://ccdcoe.org/cyber-definitions.html

North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.” Accessed 11 Apr 2017. https://ccdcoe.org/sites/ default/files/documents/CCDCOE_Tallinn_Manual_ Onepager_web.pdf.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies*, Vol 35, No 1 (2012): 5-32.

Saltzman, Ilai. “Cyber Posturing and the Offense-Defense Balance.” *Contemporary Security Policy*, 34:1 (2013): 40-63.

Schmitt, Michael. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 1st Edition. UK: Cambridge University Press, 2013.

Schmitt, Michael. “The Law of Cyber Targeting.” *CCDCOE Tallinn Paper*, No 7 (2015).

Schmitt, Michael and Liis Vihul. “Proxy Wars in Cyber Space: The Evolving International Law of Attribution.” *Fletcher Security Review*, Vol I, Issue II (Spring 2014): 55-73.

Schmitt, Michael and Liis Vihul. “The Nature of International Law and Cyber Norms.” *CCDCOE Tallinn Paper*, No 5 (2014).

Shafqat, Narmeen and Ashraf Masood. “Comparative Analysis of Various National Cyber Security Strategies.” *International Journal of Computer Science and Information Security*, Vol. 14 No. 1, January (2016): 129-136.

Tigner, Brooks. “NATO Unveils New Cyber Policy.” *Jane’s Defence Weekly* (10 Jun 2011).

Tigner, Brooks. “Polish Think-Tank Advocates Offensive Cyber Stance for NATO.” *Jane’s Defence Weekly*, Vol. 53, Issue 43 (2016).

United States. Joint Chiefs of Staff. *Cyberspace Operations*. JP 3-12. Washington, DC: Joint Chiefs of Staff, 2013.

Van Epps, Geoff. “Common Ground: US and NATO Engagement with Russia in the Cyber Domain.” *Connections: The Quarterly Journal*, Vol 12, No 4 (Fall 2013): 15-50.

Veenendaal, Matthijs, Kadri Kaska, and Pascal Brangetto. *Is NATO Ready to Cross the Rubicon on Cyber Defence?* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Zetter, Kim. “Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target.” *Wired*. Last modified 23 September 2010. https://www.wired.com/2010/09/stuxnet-2.