NATO & Cyber Conflict: Background & Challenges

Dr. Sean Lawson
Department of Communication
University of Utah

[Full citation: Lawson, Sean. (2012) "NATO & Cyber Conflict: Background & Challenges." Presented at The Shadow NATO Summit III. 14-15 May. George Washington University. Washington, D.C.]

Introduction

The goal of this paper is to provide a broad overview of cyber conflict with an eye towards the challenges that NATO faces in trying to address it. I will begin with a typology of cyber conflict. Second, I will provide a brief, historical overview of four instances in which NATO has experienced cyber conflict of one form or another. Third, I will provide a brief overview of NATO's current stance in relation to cyber conflict, including relevant organizations, principles, and activities. Finally, I will end by highlighting just a few of the challenges that NATO faces in its attempts to respond to the advent of cyber conflict.

Typology of Cyber Conflict

I will begin with a typology of cyber conflict. I will present these in the order of least to most damaging or dangerous. This also happens to be the order of most common to least common.

Cyberspace has become a domain for political activity. It allows activists to collect and publish information, to engage in dialogue, to coordinate their actions, and to lobby those in power. We see this most recently in the important use that Occupy Wall Street activists have made of the Internet for all of these purposes.

Though the Anonymous hacker collective has engaged in actions on behalf of the Occupy movement, the vast majority of Occupy's use of the Internet has not involved hacking. But the relationship between Anonymous and Occupy does remind us that the lines between these categories are blurry.

Next is hacktivism. Dorothy Denning defines hacktivism as "the convergence of hacking with activism, where 'hacking' is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software" (Denning 2001: 263).

Hacktivist methods include distributed denial of service (DDoS) attacks, website defacements, breaking into websites and stealing personal information, and use of malware like viruses and trojans.

The most well-known recent examples include the exploits of Anonymous and LulzSec. These groups are generally against the state, of course. But there are "patriot hackers" as well. In the United States, this includes one hacker who calls himself Th3J35t3r. He uses various techniques to take down jihadist web forums. He has also used targeted malware against the mobile phones of those that he believes are sympathetic to Anonymous and the Occupy movement, which he sees as anti-American.

Cyber crime is the use of the various hacking tools and techniques for criminal purposes, including theft and extortion. For example, organized crime groups often use DDoS to carry out online protection rackets against e-commerce sites. Fake antivirus scams are used to steal victims' money and personal identities. Email spam and so-called phishing attacks are used for similar purposes.

The fact that the tools and techniques used for criminal purposes are the same as those used for political purposes by hacktivists is another way in which the boundaries are blurry between these categories.

Cyber espionage includes the use of many of the same techniques mentioned above, especially website break-ins, targeted phishing attacks (called spear phishing), social engineering, and targeted use of malware to surreptitiously collect information on an adversary or competitor.

There are two types of cyber espionage: economic and political-military. In economic espionage, we see competing corporations, often from different countries, who engage in espionage against one another online. It is believed that countries like China and Russia encourage their own patriotic hackers to engage in this kind of activity.

Political-military espionage is the traditional, state-vs-state espionage we typically think about when we think about espionage. This includes attempts to steal national security information.

Again, the boundaries are blurry between the categories. States like China and Russia will enlist the help of cyber crime syndicates and patriotic hacktivists for the purposes of cyber espionage.

Dorothy Denning (2000) defines "cyberterrorism" as

> *attack[s] against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*

Were it to occur, non-state actors would carry out cyberterrorism. However, most observers, including Denning, concede that we have not yet seen real-world examples of cyberterrorism.

Cyberwar is the use of computer network attack by one state against another where such attacks cause damage to military capabilities or civilian critical infrastructure. Like cyberterrorism, to be considered a stand-alone armed attack, such attacks should result in injury, death, damage, or destruction of people and property (Schmitt 1999; Dunlap 2011).

Many tools and techniques of cyber conflict might be used in the context of traditional warfare as supporting capabilities. We saw this in the cyberattacks that accompanied the Russian invasion of Georgia in 2008. However, that does not make these tools or techniques cyberwar if they are used outside the context of wider warfare.

Like cyberterrorism, we have seen few if any stand-alone acts of cyberwar to date. The Stuxnet worm that damaged Iranian nuclear facilities might be an exception, however, which is why it is so significant.

NATO & Cyber Conflict

The 1999 Kosovo operation served as NATO's first experience with cyber conflict. During that conflict, activists and belligerents on all sides used the web to spread and/or counter propaganda. There were also a number of notable website break-ins and defacements, again usually for propaganda and protest purposes. In some cases, hacktivists sent virus-laden attachments. Beyond the immediate parties to the conflict, hackers from China became involved after the accidental U.S. bombing of the Chinese Embassy in Belgrade (Denning 2001).

The 2007 cyber attack against Estonia is the most well-known, NATO-related incident of cyber conflict. After a Soviet war memorial was moved, ethnic Russians in Estonia took to the streets in protest. The protest spread online and resulted in denial of service attacks against government, news, and bank websites. Rain Ottis (2010: 72) of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn reports that "the immediate effects to people in Estonia were minimal, and in many cases nonexistent" and that "[n]o critical services were permanently affected." Nonetheless, the attacks were a "wake-up call" for both Estonia and NATO, leading to changes in policy for both, including the creation of the CCDCOE by NATO.

In April 2011, The Cyber Security Forum Initiative, which provides cyberwar information and advice to the U.S. and NATO, published its *Project Cyber Dawn: Libya* report that assessed Libyan vulnerabilities to cyber attacks.[1] The report came to light as a result of the hacktivist group LulzSec's breach of a defense contractor's (Unveillance) servers and theft of internal emails. The report described several possibilities for cyber

[1] More information about the organization can be found at http://www.csfi.us/.

attack against Libya. The *New York Times* and *Washington Post* reported that the U.S. did consider cyber attacks against Libyan air defense systems to clear the way for the NATO mission to protect civilians from Muammar Qaddafi's forces. The U.S. rejected the use of these capabilities because of doubts about the ability to deploy them in a timely and effective manner (Schmitt & Shanker 2011; Nakashima 2011).

The revelation of *Project Cyber Dawn: Libya* was not NATO's only encounter with hacktivists in 2011. In July of that year, the hacktivist group Anonymous claimed to have hacked NATO servers and stolen 1 GB of sensitive information. Of that information, the group only released three PDFs. The hack was in part a response to a Spring 2011 NATO report that had listed hacktivism as a growing threat to national security.[2]

NATO Cyber Policy

NATO has further developed its cyber defense policies and capabilities in response to each of these incidents. It's most recent cyber defense policy statement highlights a number of principles and goals for NATO's cyber defense efforts.[3]

The primary focus of the policy remains the defense of NATO's own networks and systems. Actions in this area include centralizing the defense of NATO networks and systems. But it also includes identifying critical dependencies on national networks and systems of member states and developing minimum cyber defense standards for these national systems that intersect with NATO networks.

Though recognizing the inevitability of cyber attacks, NATO policy emphasizes the need to prevent attacks where possible and build resilience to rapidly recover from attacks when they do occur.

Finally, NATO retains the option to assist member nations that ask for assistance in the face of a cyber attack. To maintain flexibility, however, NATO cyber defense policy states that response will not be automatic or predefined in terms of its actions and scope. The policy seeks to maintain "strategic ambiguity."

Implementing these principles and achieving these goals involve a number of activities that are being addressed by several organizations within NATO. The North Atlantic Council provides political oversight to the development and implementation of policy and also plays a crucial role in decision making about responses to cyber attacks on NATO or its members. The Defence Policy and Planning Committee provides advice to member nations in their efforts to develop their own strategies and to meet NATO minimum standards. The Cyber Defence Management Board works to coordinate cyber initiatives within the NATO organization. Finally, the Computer Incident Response

[2] That report be Lord Joplin, "Information and National Security," can be found at http://www.nato-pa.int/default.asp?SHORTCUT=2443.
[3] See *Defending the Networks: The NATO Policy on Cyber Defence*, available from http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

Capability works at the technical end of things to respond to incidents affecting NATO networks and systems.[4]

Because NATO is partly dependent upon the networks and systems of its members, it has created Rapid Reaction Teams that can be dispatched to assist members who are the victim of cyber attack.

The Co-operative Cyber Defence Centre of Excellence was established in 2008 to be a center of excellence for research and training. The center has hosted several international conferences and published a number of papers exploring the evolution of cyber conflict and challenges for strategy and international law.

Finally, NATO cyber defense policy recognizes that the larger interdependencies of the global cyber commons require cooperation with partners outside of NATO. There is no dedicated NATO cyber organization for this activity, however.

Challenges

NATO faces a number of challenges in its attempts to formulate and implement a cyber defense strategy. These are not challenges that are entirely unique to NATO. Each of its member states faces many of the same challenges.

First is whether or not cyber attacks should be identified as attacks that will trigger Article 5 commitments. So far, NATO has not taken this step. But there are some who have argued that it should. However, there are good reasons not to deal with all cyber attacks under Article 5. Because of difficulty with attribution in cyberspace, any deterrent benefit gained by making cyber attack an Article 5 issue would likely be low. What's more, most cyber attacks do not rise to the level of a military attack. NATO would be stretched thin if it were to respond in each instance of cyber attack on a member state. Finally, the most potentially devastating type of cyber attack (one with impacts approximating traditional armed attack) would already fall under Article 5. NATO should continue to resist the temptation to define all cyber attacks as falling under Article 5 (Dunn Cavelty 2011).

Second, developing and implementing a cyber defense strategy will be made more difficult by the fact that not all member states share the same perceptions of cyber threats. Though most of the states agree that cyber threats are on the rise and are of great concern, there is variation in the details of these threat perceptions, including in identification of the most important sources, objects, and impacts of these threats. These differences will inevitably pose a challenge and could limit the possible scope of NATO action (Brunner et al 2009).

Third, as mentioned above, aggregating all types of cyber attack into a generic category of cyber threat risks stretching NATO's ability to respond. Cyber conflict at the level of

[4] For more on the organizational aspects of NATO's response, see "NATO and Cyber Defence," available from http://www.nato.int/cps/en/SID-4526072A-533C7553/natolive/topics_78170.htm?.

hacktivism, crime, and economic espionage are daily occurrences. They cannot all be dealt with in the same way, and certainly not as an Article 5 issue. On the other hand, disaggregating these threats raises its own challenge, including the question of which organizations are best able to respond to the various types of threats in and through cyberspace. Private actors within member states own most critical infrastructures. It is often difficult enough for member states to deal effectively with cybersecurity within their own borders. This difficulty, the role of private actors, and differing threat perceptions, will all combine to make it difficult for NATO to do more than focus on securing its own networks (Dunn Cavelty 2011).

Finally, the case of U.S. reluctance to use offensive cyber attacks during the Libya campaign points to the challenge of deploying offensive cyber capabilities in a timely manner and with certainly of their effects. In turn, this points to potential legal challenges for deploying offensive cyber capabilities during conflict, in particular challenges of using these capabilities in accord with principles of discrimination and proportionality.

References

Brunner E et al. (2009) Cybersecurity - Recent Strategies and Policies: An Analysis. *CRN Reports* August.

Denning D (2000) Cyberterrorism. Presentation to Special Oversight Panel on Terrorism, Committee on Armed Services, House of Representatives. 23 May.

Denning D (2001) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Arquilla J, Ronfeldt D (eds) *Networks and Netwars: The Future of Terror, Crime, and Militancy.* 239-288.

Dunlap Jr (ret) MGCJ (2011) Perspectives for Cyber Strategists on Law for Cyberwar. *Strategic Studies Quarterly* 5(1): 81-99.

Dunn Cavelty M (2011) Cyber-Allies: Strengths and Weaknesses of Nato's Cyberdefense Posture. *IP Global Edition* 12(3): 11-15.

Nakashima E, (2011) U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses. *Washington Post,* 17 October, Available at: http://www.washingtonpost.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAETpssL_story.html.

Ottis R, (2010) The Vulnerability of the Information Society. *futureGOV Asia Pacific,* August-September, p. 70.

Schmitt E, Shanker T, (2011) U.S. Debated Cyberwarfare in Attack Plan on Libya. *New York Times,* 17 October, Available at: https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1.

Schmitt MN (1999) Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law* 37: 885-937.