What is NORAD's Role in Military Cyber Attack Warning?

By Randall DeGering

Abstract

For more than fifty years, North American Aerospace Defense Command (NORAD) has been responsible for conducting aerospace warning and control missions for the defense of North America. In accomplishing those operations, Commander NORAD is responsible for making the official warning to both the president of the United States and the prime minister of Canada if North America is suddenly under aerospace attack. Now, with the dramatic increase in worldwide cyberspace events, NORAD has begun examining its own potential role within this new domain. Would involving NORAD in the military cyber attack warning process, leveraging its unique and proven binational structure, provide any advantages to both nations?

To analyze this question, this essay traces NORAD's warning mission history, discusses the basic concepts involved with "cyber attacks," identifies key U.S. and Canadian military cyber organizations, and examines significant U.S. and Canadian cyberspace government policies. It then proposes three potential new courses of action for NORAD, identifying advantages, disadvantages, and proposed solutions to implementation. The essay ends by recommending that NORAD advocate for unrestricted cyberspace national event conference participation. This would be a realistic, achievable first step offering significant improvement in both NORAD's cyber attack situational awareness, as well as improving overall operational responsiveness.

Introduction

For more than fifty years, North American Aerospace Defense Command (NORAD) has been responsible for conducting aerospace warning and aerospace control for North America. These two aerospace missions involve the combined efforts of military forces of both the U.S. and Canada to detect airborne threats approaching or flying within North America (aerospace warning) and then taking appropriate actions to determine the aircraft of interest's actual intentions (aerospace control). The commander of NORAD is responsible for making an official assessment to the president and the Canadian prime minister if it is believed North America is under aerospace attack.

Similarly, U.S. Cyber Command (USCYBERCOM) is responsible for defending the U.S. military's cyberspace enterprise. The commander of USCYBERCOM is responsible for making an official assessment to the president if the U.S. military is under cyber attack. Would involving NORAD, with its unique and proven binational structure, in the military cyber attack assessment process provide any advantages?

With cyber attacks by nation-states on the increase, the question arises as to whether there is an advantage to involving a binational military command in the assessment of military cyber attacks. Potential advantages include operational efficiencies, improved cyberspace defense readiness, and/or enhanced situational awareness of a precursor cyberspace attack before any kinetic attack upon North America. Disadvantages involve the difficulties in sharing cyberspace defense information between U.S. and Canadian cyberspace defense agencies, or the potential lessening of operational effectiveness of USCYBERCOM cyberspace operations themselves.

Using existing national policy and guidance, as well as dialogue with Headquarters NORAD and USNORTHCOM, USCYBERCOM, and Canadian military cyberspace practitioners, this essay proposes three courses of action that NORAD might consider, outlines the advantages and disadvantages of each, and concludes with a recommendation.

Historical Background

With the beginning of the Cold War during the late 1940s, American defense experts began planning a new, comprehensive air defense strategy they believed was critical for defending the U.S. against attacks by long-range Soviet Union strategic bombers. Led by the U.S. Air Force's newly established "Air Defense Command" (created in 1948), regional commands were charged with protecting various areas of the U.S. from bomber attacks.[1]

In August 1949, the Soviet Union detonated its first atomic bomb under project "First Lightning."[2] The test shocked the Western powers, as the American intelligence community had previously estimated the Soviets would not develop an atomic weapon until 1953, at the very earliest.[3] It was now predicted the Soviet Union would soon have the means to drop atomic weapons on the U.S. using long-range strategic bombers.

As concerns about Soviet nuclear capabilities became dire, in 1954 the Department of Defense formed a new, multi-service command called "Continental Air Defense Command" (CONAD) involving Army, Naval, and Air Force personnel. As their service contribution, the Air Force provided interceptor fighter aircraft and agreed to operate an extensive array of arctic distant early warning radar sites which would act as a "trip wire" against any surprise Soviet bomber attack being launched over the North Pole (the shortest attack route from Russia.)

In addition, the U.S. and Canada had begun mutual defense negotiations, centering on building three series of long-range ground radar warning sites across Canada—the southern "Pinetree Line," the "Mid-Canada Line," and the famous northern "Distant Early Warning (DEW) Line."

Based upon the remarkable success of these joint United States-Canadian radar construction efforts, in 1958 the U.S. and Canada then jointly agreed to create an innovative "North American Air Defense Command" (NORAD), merging the operational control of both United States and Canadian air defense forces under a new, combined binational military command.

Adding to the continental defense challenge, Soviet engineers soon developed new intercontinental ballistic missiles (ICBM) capable of delivering small, newly developed hydrogen bomb warheads. Thus, long range missile attacks now became a new, critical defense problem, as NORAD's vast line of arctic air defense radar sites could now "not only [be] outflanked, but literally jumped over."[4]

In response to this growing Soviet ICBM threat, beginning in 1959, NORAD developed the Ballistic Missile Early Warning System (BMEWS). Consisting of huge 165 feet high by 400 feet long radars, BMEWS became the first operational ballistic missile detection and warning system, designed to provide 15–25 minutes critical warning of a Soviet missile attack launched directly over the North Pole.

Later, because of growing concerns these BMEWS radars were unable to observe actual Soviet launches occurring far beyond the Earth's horizon, the U.S. began developing its own missile technology to orbit successive generations of early warning satellites capable of immediately detecting any ICBM launch occurring around the globe.

Space-based early warning progressed from the nascent "Missile Defense Alarm System" (MIDAS) developed in the 1960s, to the more capable "Defense Support Program" (DSP) series of satellites employed during the 1970s to 1990s, to the current "Space-Based Infrared System" (SBIRS) series of satellites first launched in the 2000s.

Operating from geostationary orbit over 22,000 miles above the earth, early warning satellite systems are designed to detect immediately any missile launches or nuclear explosions occurring across the globe. Using sensitive on-board sensors designed to detect infrared emissions from intense heat sources, these early warning satellites then send an immediate message to NORAD warning of a possible ICBM launch.[5]

Thus, an evolving Soviet threat caused NORAD to adapt its warning missions to include both aircraft and missile attacks on North America. Reflecting that evolution, the 1981 NORAD Agreement officially changed the command's name to the North American "Aerospace" Defense Command.

New Warning Missions for NORAD

In the aftermath of the 9/11 attacks, Canada and the U.S. created a Binational Planning Group (BPG) in 2004 to work on numerous proposals for creating wider cooperation between U.S. and Canadian military plans and protocols, and to look for common mission areas in which the two countries could share information. One area of mutual interest was improving awareness of maritime threat routes which surround the North American continent.[6]

In a letter to the Chairman of the Joint Chiefs of Staff, Commander NORAD supported the concept of NORAD being tasked with a new maritime surveillance, warning, and information sharing mission.[7] After lengthy staffing actions between military headquarters, the U.S. and Canada signed a renewed NORAD Agreement (effective May 2006) assigning NORAD its new Maritime Warning mission, consisting of "…processing, assessing, and disseminating intelligence and information related to the respective maritime areas and internal waterways of, and the maritime approaches to, the U.S. and Canada, and warning of maritime threats to, or attacks against North America utilizing mutual support arrangements with other commands and agencies, to enable identification, validation, and response by national commands and agencies responsible for maritime defense and security."[8]

Six years later, in 2012, both the U.S. Chairman of the Joint Chiefs of Staff (CJCS) and the Canadian Chief of Defense Staff (CDS) jointly directed Commander NORAD to conduct a "NORAD Strategic Review" to address the following specific issues:

- Review current and potential future roles, missions, and command relationships
- Inform and support analysis of need for investment in NORAD capabilities
- Recommend linkages to align respective national research and development, planning, programming and budgeting processes related to NORAD requirements
- Recommend ways to align readiness reporting processes.[9]

When asked about the pending NORAD Strategic Review, General Charles Jacoby (then-Commander NORAD) replied,

> [w]e are deliberately moving out on a review that looks at the threat assessment, readiness assessment and program assessment processes that we need to put in place or revitalize, as the case may be, to ensure that we're staying ahead of the threat. The threat to North America is changing and increasing as time goes by, *and that includes cyber threats*, threats to space, changing in the extremist threat to North America, changing in some of the more conventional threats and making sure that NORAD is positioned to keep faith with the agreement. (Emphasis added.)[10]

Completed in November 2014, the Strategic Review identified the emergence of new threats and capabilities which have the potential to affect NORAD"s ability to deter, detect, and defeat threats to Canada and the U.S. Specifically addressing cyberspace, the Review stated,

> NORAD must be aware of current and emerging cyberspace threats and the means by which NORAD's systems will be protected in order to meet their mission requirements. Therefore, NORAD must develop agreements and processes with trusted organizations and agencies to better analyze, characterize, assess, and share the impact of cyberspace events on NORAD operations, and the steps taken to defend NORAD networks against cyberspace-attacks.[11] Improvement of information sharing processes with cyberspace organizations and examination of new relationships can fill operational gaps to enhance NORAD mission assurance. (Canada's Department of National Defence) and (U.S.' Department of Defense) *should examine NORAD's potential roles and responsibilities in providing binational cyberspace warning for North America*. (Emphasis added.)[12]

Thus, since 1958, NORAD has a proven history of adapting and evolving to meet changing military defense challenges using new technology—from its early years providing

ground-based radar warning of approaching Soviet bombers, to ground-based radar warning of in-bound Soviet ICBMS, to satellite-based warning of any missile launch occurring around the world, to extended radar warning of approaching cruise missiles, to the warning of suspect maritime vessels approaching North America.

NORAD has sole responsibility for receiving early warnings from numerous space-based and ground-based sensors and developing an integrated North American attack assessment. And because all of the sensors feeding into NORAD travel across the broader "information superhighway," there exists a genuine risk of potentially hostile nations conducting damaging cyberspace operations against NORAD (to include blinding NORAD to actual threats, or feeding the Command false information for incorrect action.) With the recent increase in world-wide cyberspace events, NORAD thus has begun examining its own potential role in this new operational domain.

Growing Military Cyberspace Threats

In his testimony to the Senate Select Committee on Intelligence on January 29, 2014, James Clapper (Director of National Intelligence) provided an overview of the various international cyber threat actors currently challenging the U.S., stating "[w]e assess that computer network *exploitation* and *disruption* activities such as denial-of-service attacks will continue. Further, we assess that the likelihood of a *destructive* attack that deletes information or renders systems inoperable will increase as malware and attack tradecraft proliferate."[13]

First, Director Clapper highlighted his growing concerns regarding the evolving Russian cyber threat:

> Russia presents a range of challenges to U.S. cyber policy and network security. Russia seeks changes to the international system for Internet governance that would compromise U.S. interests and values. Its Ministry of Defense (MOD) is establishing its own cyber command, according to senior MOD officials, which will seek to perform many of the functions similar to those of the U.S. Cyber Command.[14]

As an example, the FireEye network security company stated they had reason to believe an "advanced persistent threat" (APT) from Russia had been operating since at least 2007, and was engaged in espionage against political and military targets. The report outlined how it was believed Russian hackers had targeted the Georgian Ministry of Defense; interfered with the Bulgarian, Polish and Hungarian governments; targeted Baltic military forces supporting U.S. Army training; and targeted several North Atlantic Treaty Organization (NATO) organizations.[15]

Director Clapper then explained to the Select Committee how China was also becoming a serious cyberspace threat to the nation, stating,

> China's cyber operations reflect its leadership's priorities of economic growth, domestic political stability, and military preparedness… Internationally, China also seeks to revise the multi-stakeholder model of Internet governance while continuing its expansive worldwide program of network exploitation and intellectual property theft.[16]

Underscoring this threat, in May of 2014, the U.S. Department of Justice indicted five members of the Chinese People's Liberation Army (PLA), charging these individuals with hacking into computer networks owned by the U.S. Steel Corporation, Westinghouse Electric, and other major corporations. The Justice Department indictment specifically focused on "Unit 61398," acknowledged as being the Shanghai-based cyber unit of the PLA. While acknowledging that countries conduct espionage for national security purposes, the indictment charged it was illegal for China to employ national intelligence assets to steal U.S. corporate secrets in order to gain an economic advantage.[17]

Director Clapper also warned the Select Committee about two other serious cyber threat actors. He argued that "Iran and North Korea are unpredictable actors in the international arena. Their development of cyber espionage

or attack capabilities might be used in an attempt to either provoke or destabilize the U.S. or its partners."[18] Regarding Iran, U.S. Representative Peter Hoekstra (R-Michigan) stated, "Iran has boosted its cyber capabilities in a surprisingly short amount of time and possesses the ability to launch successful cyber attacks on American financial markets and its infrastructure."[19] Finally, North Korea has expended enormous resources to develop its cyber warfare cell called "Bureau 121" under the General Bureau of Reconnaissance, a spy agency run by the North Korean military.[20] South Korean intelligence contends that Bureau 121 has repeatedly conducted cyber attacks against numerous South Korean businesses, to include incidents in 2010 and 2012 targeting banks and media organizations. Pyongyang rejects these charges.[21]

Thus, one can clearly see the Intelligence Community's increasing concern about the cyberspace threat posed by several potentially hostile nations, and the general consensus that these global threats are indeed serious and not abating.

What should be considered a "Cyber Attack"?

In their article "Cyber-Weapons," Thomas Rid and Peter McBurney state there is no internationally agreed-upon definition of a cyber weapon. Therefore, they proposed the following definition: "[a] cyber weapon is seen as a subset of weapons, more generally as computer code that is used, or designed to be used, with the aim of threatening or causing *physical, functional, or mental harm* to structures, systems, or living beings." (Emphasis added.)[22] Expanding upon this proposed definition, in his book *Cyberattack,* Paul Day proposed four levels of cyber weapons.[23]

- Level 1. "Dual use" software tools provided with a computer's organic operating system, such as network monitoring tools, which can be converted into hacking tools and used to exploit security vulnerabilities.
- Level 2. Software tools that can be downloaded for computer security purposes that are then abused to compromise networks and computers. This software is specifically designed to allow skilled operators to test and penetrate system security, but in the wrong hands can subvert a network.
- Level 3. Malware designed only to exploit and infect other computers. Examples include RAT, spyware, and botnet clients. Again, these programs are widely available on the Internet.
- Level 4. Purposely built cyber weapons covertly developed by nation states with the expressed intention of waging cyber warfare. The most famous example is the "Stuxnet" worm discovered in 2010. (This level would match cyber weapon attacks as outlined by Rid and McBurney.)

In order to discuss the merits of any proposed cyber attack warning policy, it would be helpful to have a clear definition of what specifically defines a "cyber attack."

Media Definitions

While the news media repeatedly warn us about "cyber attacks,"[24] there currently are no uniformly agreed-upon terms to describe cybersecurity activities. Typical cyber actions are often publically described as:[25]

- "Cyber-vandalism" or "hacktivism" (defacing or otherwise temporarily interfering with public access websites)
- "Cyber-crime" or "cyber-theft" (defrauding individuals to obtain their personal identification data, or actual theft of funds from financial accounts)
- "Cyber-espionage" (covertly stealing sensitive or proprietary information)
- "Cyber-warfare" (conducting military operations using cyber means).

Popular cyber terms used in the media include "breach," "compromise," "intrusion," "exploit," "hack," "incident," and "attack."[26] So what is the difference between these various terms? Specifically, from a military viewpoint, what should be meant by a "cyber attack"?

NATO Definition

We begin by defining an "act of aggression" as being "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[27] Examples of acts of aggression outlined by the United Nations in its resolution include:

- The invasion or attack by the armed forces of a State into the territory of another State
- Bombardment by the armed forces of a State against the territory of another State, or the use of any weapons by a State against the territory of another state
- The blockade of the ports or coasts of a State
- An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State.[28]

Given this general definition of an act of aggression, what does it mean to conduct a "cyber attack?" To answer this question, beginning in 2009, NATO undertook a three-year project to identify the international laws applicable to cyber warfare, with a goal of defining specific rules governing such conflicts. Working with twenty international law scholars and cyber practitioners, this working group eventually published their *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013.

First, the Tallinn group developed a general definition of the "use of force" for cyber operations: "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[29]

The group found focusing on the "scale and effects" of a cyber operation was a useful approach when attempting to distinguish between cyber acts which unmistakably qualify as use of force (e.g., such as acts that injure people or damage property) and cyber acts which do not cause physical harm. Used this way, "scale and effects" effectively captures the qualitative factors to be considered in evaluating whether a cyber operation reached the level of other kinetic actions analogous to a use of force.[30]

The group next developed a set of eight specific factors to consider in judging whether a specific cyber operation actually constituted the "use of force." As stated in the *Tallinn Manual*, these include:

- **Severity** Consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force…the scope, duration, and intensity of the event will have great bearing on the appraisal of their severity
- **Immediacy** The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects
- **Directness** Cyber operations in which the cause and effect are clearly linked are more likely to be characterized as uses of force
- **Invasiveness** As a rule, the more secure a targeted cyber system, the greater the concern as to its penetration. For example, cyber operations targeting State domain names (e.g., ".mil" or ".gov") could be considered more invasive than cyber operations directed at non-State domain names (e.g., ".com" or ".net.")
- **Measurability of Effects** The more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of a use of force
- **Military Character** The closer the connection between the cyber operation and military operations, the more likely it will be deemed a use of force

- **State Involvement** The clearer and closer a nexus between a State and cyber operations is, the more likely it is that other States will characterize them as uses of force by that State

- **Presumptive Legality** Finally, the group clarified that acts not forbidden by international law are permitted and are presumptively legal. Propaganda, psychological operations, espionage, economic pressure, etc., are all actions allowed by international law. Thus, cyber operations falling into these internationally legal categories will be less likely to be considered by States as uses of force.[31]

Using these specific factors, the Tallinn group then developed a definition of the "threat of force" under cyber operations: "[a] cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force."[32] Finally, linking all previous definitions into a coherent concept, the Tallinn group developed an authoritative definition of what constitutes a genuine "cyber attack":

> "[a] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[33]

Thus, after considerable legal deliberations and debate, the Tallinn group developed a definition of "cyber attack" useful in policy development, military strategies, and international affairs. It excludes non-lethal activities (such as cyber-crime and cyber-espionage) and allows for both state and non-state actors.

More importantly, the NATO definition clearly provides a logical connection between the legal concepts of "an act of aggression," "use of force," "threat of force," "armed attack," and "self-defense." And it provides useful factors for consideration in determining whether the "scale and effects" of a specific cyber operation constitutes an actual armed attack upon a State.

Expressing similar concerns about growing worldwide cyberspace threats, NATO endorsed a new "Enhanced Cyber Defence Policy" during its 2014 North Atlantic Council Summit. In its published Declaration, NATO stated:

> [t]he policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks…Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance.[34]

Alternative Definition

Interestingly, in January 2015, Admiral James Stavridis (NATO Commander from 2009–2013) disagreed with this specific NATO definition. He stated the *Tallinn Manual* definition of cyber attack was "far too simplistic to account for the nuances of cyberwarfare. It sets a dangerously high threshold for a domain with comparatively low barriers to entry."[35] Stavridis proposed there are three elements to "cyberforce": intelligence (understanding the target environment), cyberweapons (the actual computer code, usually target-specific with a short shelf life), and intent (a calculated human decision). He then proposed that it is specifically the cyberweapon which defines whether cyberforce approaches the level of a genuine armed attack.[36]

For example, Stavridis outlines the 2012 "Shamoon" virus that infected Saudi Aramco, the world's largest State-owned oil company. This cyber operation erased data from computer memories which the company could not reconstitute. Also, company systems were down for two weeks, resulting in adverse global economic affects. Finally, more than 30,000 workstations were replaced to rid the corporation network of malware. This action "is a far better measure of cyberforce than simply concentrated personal injury or physical damage. Yet, according to the *Tallinn Manual*,

Shamoon was not a cyber attack."[37] Therefore, Stavridis offers his own alternative cyber attack definition:

> [a] cyber attack is the deliberate projection of cyberforce resulting in kinetic or nonkinetic consequences that threaten or otherwise destabilize national security, harm economic interests, create political or cultural instability; or hurt individuals, devices or systems."[38]

This alternative definition may in fact become a more useful one for future military planners, as it broadens threats from cyberspace operations to include those actions which inflict economic harm or national security instability.

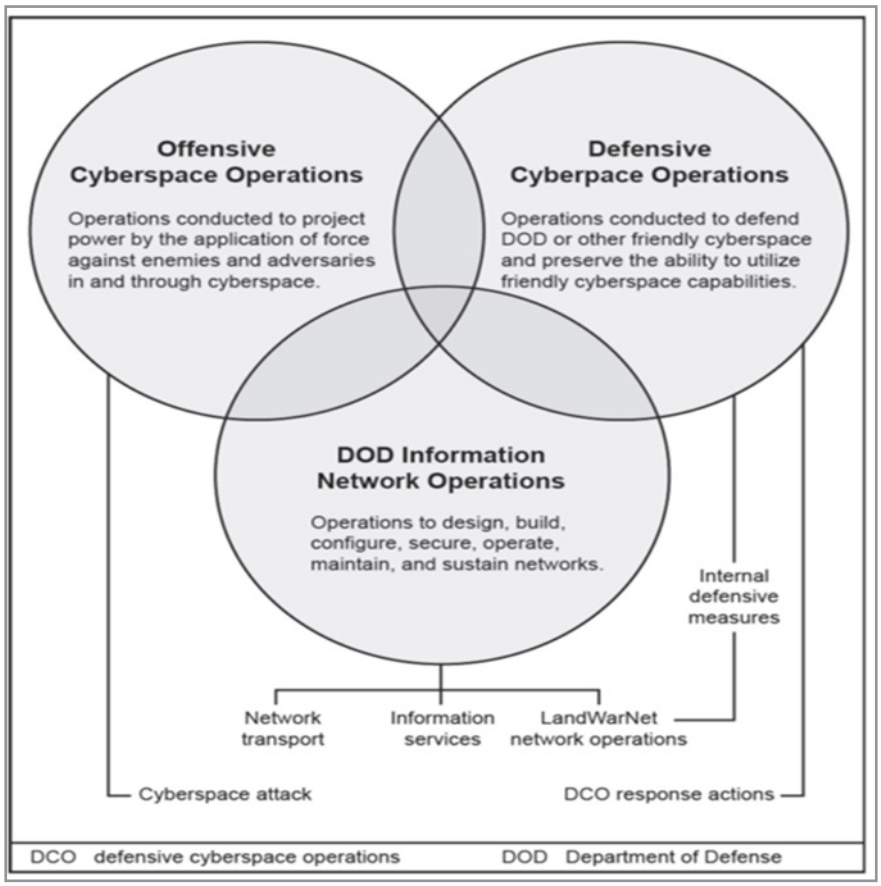

Figure 1. DOD Cyberspace Operations.[39]

What Constitutes "Cyberspace Operations"?

From a Department of Defense (DOD) perspective, military cyberspace missions can be characterized using several overlapping definitions and relationships (see Figure 1):

Department of Defense Information Networks (DODIN)

These are described by the Department of the Army as "[t]he globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems."[40]

DODIN Operations

These are described by the Department of the Army as "[o]perations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks."[41] DODIN operations are the traditional methods we all think of to preserve data availability, integrity, confidentiality, and user authentication. These operations include configuration control and system patches, user training, physical security, firewalls, and data encryption. Many DODIN activities are conducted through regularly scheduled events and updates.

Defensive Cyberspace Operations (DCO)

These are operations which respond to unauthorized activity or alert/threat information which threaten the DODIN. DCO can be both "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."[42] "Internal defense measures" are conducted within the DODIN. These are defined as being "defensive tools and techniques [which] are designed to find, fix and finish anomalous network activity using rule, signature and behavioral-based techniques."[43] By comparison, "DCO-Response Actions" or DCO-RA are defensive measures taken outside the defended network to protect DOD cyberspace capabilities. Once sources of a cyber attack are identified, response actions (such as custom-made computer code) may be employed to defend friendly cyberspace systems.[44]

Offensive Cyberspace Operations (OCO)

These are "operations intended to project power by the application of force in and through cyberspace."[45] OCO focuses effects in cyberspace to influence or degrade enemy weapon systems, command and control processes, critical infrastructures, etc.

Cyberspace Attack

As defined by DOD, cyber attacks are activities that deny (by degrading, disrupting or destroying access to, operation of, or availability of a target) or that manipulate (by controlling or changing an adversary's information or networks.)[46]

As can be seen, the topic of "cyber attack" involves not only various potential definitions of what a cyber attack actually entails, but also what means are available to respond either defensively or offensively to such an attack.

While cyberspace definitions remain fluid, they all help establish the essential conceptual foundation to allow military and civilian policy makers to consider how "cyber attack warning" might be specifically implemented by NORAD.

Military Cyber Event Conferences

In order to provide rapid command and control, the U.S. Chairman of the Joint Chiefs of Staff (CJCS) has established emergency conferencing procedures that allow military commands around the world to simultaneously connect and discuss urgent military events at various classification levels.[47] USCYBERCOM specifically manages two important cyberspace-related worldwide conferences (see Figure 2):

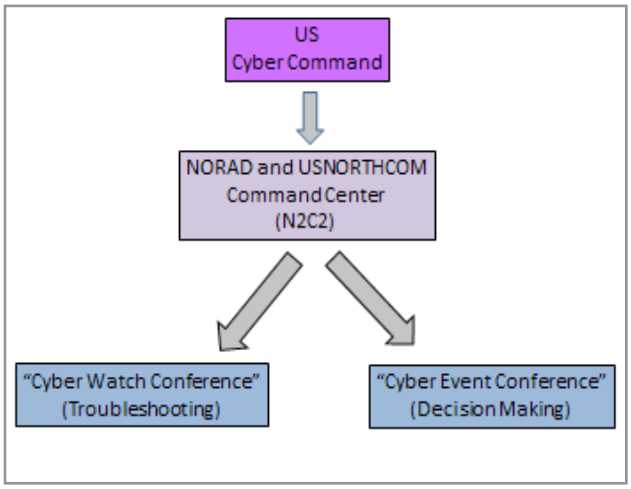

Figure 2. Cyber Event Conferences.

- "Cyber Watch Conferences" provide a specialized, technical forum for operational watch centers around the world to identify and troubleshoot anomalous cyberspace indications, conduct checks to verify circuits are serviceable, communication encryption devices are functioning, satellite relay systems are operative, etc.
- "Cyber Event Conferences" allow senior decision-makers to discuss securely potential operational impacts with each other, and to deliberate what follow-on cyberspace actions might be required.

Another, more senior-level conference (managed by the Pentagon) is entitled the "National Event Conference" or NEC. Using this conference, government and military agencies and commands worldwide are brought together for situational awareness regarding an urgent national event.

One significant situation that can trigger a NEC is a "cyberspace event," defined as "… any significant loss or serious threat of loss of networks or data (e.g., critical cyberspace links or nodes, cyberspace mission data providing assets etc.) that threatens U.S. national security or interests."[48] During a cyber NEC, Commander USCYBERCOM is required to make an official "Cyberspace Attack Assessment" to U.S. (but not currently Canadian) national leadership using formally-defined assessment criteria (see Figure 3.)[49]

UNCLASSIFIED	
YES	In the judgment of CDRUSCYBERCOM, a verified cyberspace attack has occurred, is occurring, or is imminent.
CONCERN	In the judgment of CDRUSCYBERCOM, a cyberspace attack may be in progress or is imminent. The situation is still under assessment and may warrant implementation of appropriate measures and/or plans to enhance cyberspace responsiveness and inter-agency awareness.
NO	In the judgment of CDRUSCYBERCOM, a verified cyberspace attack has not occurred, nor is one in progress.
PENDING	The judgment of CDRUSCYBERCOM will be provided as soon as possible. No assessment is available at this time. There is inadequate information available to assess whether a cyberspace attack is or may be occurring or is imminent.
	UNCLASSIFIED

Figure 3. Cyberspace Attack Assessment Criteria.[50]

NORAD participates in these worldwide conferences via the NORAD and USNORTHCOM Command Center (N2C2), which acts as the central point of contact and coordinator for participation in all national conferences for both Commands (see Figure 4.)

Figure 4. NORAD-USNORTHCOM Command Center.[51]

The N2C2 effectively integrates all missile warning, air warning, maritime warning, land operations and cyberspace operations, thus bringing the two Commands' multiple missions together to create greater synergy. However, due to current U.S. information classification policy restrictions, NORAD Canadian personnel must exit any national event conference once specific "U.S.-only" classified cyberspace topics are being discussed.

Key U.S. and Canadian Cyber Policy Guidance

Cyberspace warning is influenced by a host of international, governmental and military policies and guidance. Both the U.S. and Canadian governments have published many documents providing guidance to military commands at the strategic, operational, and tactical levels.

In an effort to establish his own administration's guidance regarding cyberspace, in 2009 President Obama directed a Cyberspace Policy Review as a "clean slate" review assessing U.S. cybersecurity policies.[52] The results established

> ...strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, *international engagement*, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (Emphasis added.)[53]

As a near-term accomplishment, the report specifically recommended the Nation should "develop U.S. Government positions *for an international cybersecurity policy framework and strengthen our international partnerships* to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity." (Emphasis added.)[54]

The executive branch prepares and updates the U.S. National Security Strategy (NSS) to outline the key national security concerns of the United States, and how the current administration plans specifically to address those concerns. The current NSS, developed in 2010, states:

> [n]either government nor the private sector nor individual citizens can meet this challenge alone—we will expand the ways we work together. *We will also strengthen our international partnerships* on a range of issues, including the development of norms for acceptable conduct in cyberspace; laws concerning cybercrime; data preservation, protection, and privacy; *and approaches for network defense and response to cyber attacks*. We will work with all the key players—including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents. Just as we do for natural disasters, we have to have plans and resources in place beforehand." (Emphasis added.)[55]

Drafted in 2011, the U.S. International Strategy for Cyberspace serves as the U.S.' first, comprehensive International Strategy for Cyberspace. Regarding military initiatives, the Strategy outlines the following:

> Build and enhance existing military alliances to confront potential threats in cyberspace**.** Cybersecurity cannot be achieved by any one nation alone, and greater levels of international cooperation are needed to confront those actors who would seek to disrupt or exploit our networks. This effort begins by acknowledging that the interconnected nature of networked systems of our closest allies, *such as those of NATO and its member states*, creates opportunities and new risks. Moving forward, the United States will continue to work with the militaries and civilian counterparts of our allies and partners *to expand situational awareness and shared warning systems, enhance our ability to work together in times of peace and crisis, and develop the means and method of collective self-defense in cyberspace*. Such military alliances and partnerships will bolster our collective deterrence capabilities and strengthen our ability to defend the U.S. against state and non-state actors. (Emphasis added.)[56]

Overall, the International Strategy for Cyberspace establishes a roadmap allowing U.S. governments and agencies to better coordinate cyberspace policy with our partner nations. It also establishes an invitation to other nations to join in a common vision of innovation, interoperability, reliability and security.

The National Military Strategy (NMS), also drafted in 2011, serves as the means for the CJCS to provide the "best military advice"[57] to the Nation's leadership, and outlines the ways and means by which the U.S. military advances the Nation's enduring national interests.

This strategy outlines three broad themes:

> [f]irst, in supporting national efforts to address complex security challenges, the Joint Force's leadership approach is often as important as the military capabilities we provide. Second, the changing security environment requires the Joint Force to *deepen security relationships with our allies and create opportunities for partnerships with new and diverse groups of actors*. And third, our Joint Force must prepare for an increasingly dynamic and uncertain future in which a full spectrum of military capabilities and attributes will be required to prevent and win our Nation's wars. Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains. Strategic Command and Cyber Command will collaborate with U.S. government agencies, nongovernment entities, industry, *and international actors* to develop new cyber norms, capabilities, organizations, and skills. Should a large-scale cyber intrusion or debilitating cyber attack occur, we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable. (Emphasis added.)[58]

Finally, "[j]oint Forces will secure the '.mil' domain, requiring a resilient DOD cyberspace enterprise that employs detection, deterrence, denial, and multi-layered defense."[59] Thus, DOD is chartered to focus on the ".mil" domain, while DHS focuses on the broader ".gov" domain.

Similarly, Canada drafted its own Cyber Security Strategy in 2010. This strategy is the Canadian government's plan for meeting the cyberspace threat, and delivers on the government's commitment to implement a

cyberspace strategy to protect Canada's digital infrastructure. It acts as a cornerstone of the government's commitment to keep Canada, and its cyberspace, safe, secure, and prosperous.

Further, Canada's "Action Plan 2010-2015" then outlines the Canadian government's plan to implement the Cyber Security Strategy and meet the ultimate goal of securing Canada's cyberspace for the benefit of Canadians and their economy. The Action Plan outlines thirty specific actions to take, the required deliverables, and the lead agencies involved, all coordinated to meet the three pillars outlined in the Cyber Security Strategy.

Finally, the Canadian Forces Cyber Operations Primer, drafted in 2014, describes Cyber Operations from a Canadian Armed Forces (CAF) perspective, and outlines the operational functions in the Cyber environment, those being Command, Sense, Act, Shield, and Sustain. Under the "Sustain" function, the Primer states, "[s]ustaining the Force requires the CAF to engage in a wide range of multi-national political/military alliances and arrangements (i.e., Five-Eyes, NATO, *NORAD*.)" (Emphasis added.)[60]

As can be seen, U.S. and Canadian strategic cyberspace guidance documents all propose a closer working arrangement between each country as both deal with growing cyberspace threats. These documents significantly inform the discussion regarding NORAD's potential new role in cyberspace threat information and attack assessment.

Three Proposed Courses of Action for NORAD Consideration

Informed from extensive dialogue with NORAD, USCYBERCOM, and Canadian military cyberspace practitioners, I propose three potential courses of action (COAs) for NORAD consideration regarding possible roles the Command might play in future military cyber attack warnings. Each of these three COAs met all five validity criteria used by the DOD: [61]

- **Adequate** Can accomplish the mission within the commander's guidance
- **Feasible** Can accomplish the mission within the established time, space, and resource limitations
- **Acceptable** Must balance cost and risk with advantage gained
- **Distinguishable** Must be sufficiently different from other COAs
- **Complete** Does it answer who, what, where, when, how and why?

I have arranged these three COAs sequentially by increasing levels of responsibility being placed upon NORAD, and I have examined them for their specific advantages, disadvantages, and levels of difficulty in their implementation.

COA #1. Full NORAD Cyber Conference Participation

Under this COA, NORAD's role would be to fully participate in all cyberspace event conferences in order to increase the Command's internal situational awareness regarding in-progress, military-related cyber events.

NORAD currently participates in "Cyber Watch Conferences" which provide cyber technicians a standardized venue to discuss and troubleshoot detected system anomalies. However, during advanced "Cyber Event Conferences" and "National Event Conferences," practitioners report Canadian participation is denied approximately 50 percent of the time due to discussions involving non-releasable (US-only) classified cyberspace compartmented information. This COA proposes U.S. classification policy be changed by DOD to allow NORAD Canadians to participate fully in those cyberspace conferences.

Implementing this COA eliminates those restrictions, makes classified cyber event information fully available to appropriate Canadian military personnel, and improves NORAD's own cyberspace situational awareness and ability to gauge any associated mission impacts.

Advantages of COA #1 include:

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Does not change existing relationships with USCYBERCOM.
- Does not require a change in the NORAD Agreement and/or Terms of Reference negotiated between the U.S. and Canada.

Disadvantages to COA #1 (and proposed alternative solutions) include:

- Some classified cyberspace threat information and technical "tactics, techniques, and procedures" (TTPs) are not currently releasable to Canadian personnel. (Change DOD classification guidance to allow Canadians full access to cyberspace threat information and TTPs.)
- NORAD regional headquarters currently must drop off threat conferences during classified discussions. (Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.)
- Modifies existing conference checklist procedures. (Modify cyberspace conference checklists to reflect full NORAD participation.)

COA #2. NORAD All-Domain Warning Production

Under this COA, NORAD's role would be to fuse applicable North America military-related cyber event information with current NORAD aerospace and maritime operational information to produce all-domain warnings to the U.S. and Canadian governments.

Assuming the issue of releasing classified cyber event information to NORAD Canadians is successfully resolved (proposed in COA #1), COA #2 directs NORAD to fuse military cyber event information with current aerospace and maritime warning information to produce timely all-domain warnings to the U.S. and Canadian governments using existing NORAD binational military relationships and established warning processes.

This COA would allow Canadian cyber forces to become involved in the NORAD notification process. As technical cyber event information would initially be analyzed by USCYBERCOM, then provided to NORAD for further amalgamation, there would be no change to the existing relationships between the two commands.

Advantages of COA #2 include:

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Does not change existing relationships with USCYBERCOM.
- Directs NORAD to fuse military cyber event information with current aerospace and maritime warning information to produce an all-domain characterization.
- Uses proven, legacy NORAD binational relationships and procedures to provide immediate all-domain warning updates to both U.S. and Canadian military command structures.

Disadvantages to COA #2 (and proposed alternative solutions) include:

- Some classified cyberspace threat information and technical TTPs are not currently releasable to Canadian personnel. (Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.)
- NORAD regional headquarters currently must drop off threat conferences during classified SCI discussions. (Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.)
- Modifies existing conference checklist procedures. (Modify cyberspace conference checklists to reflect NORAD fusing and dissemination of all-domain warning updates to both the U.S. and Canada.)
- Requires training NORAD personnel to fuse and disseminate all-domain warning updates. (Build new training program for NORAD personnel to fuse and disseminate all-domain warning updates.)
- Requires negotiating new cyberspace defense and response policies between the U.S. and Canada. (Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.)
- Requires a change in NORAD Agreement and/or Terms of Reference between both Governments. (Negotiate change to NORAD Agreement and/or Terms of Reference between the U.S. and Canada, if required.)

COA #3. Joint NORAD + USCYBERCOM Cyber Attack Assessment

Under this COA, NORAD's role would involve CDRNORAD and CDRUSCYBERCOM to conducting a combined formal cyber attack assessment, if such an attack was believed to be in progress.

Again, assuming the releasability of classified cyber event information (proposed in COA #1) is successfully accomplished, COA #3 would require joint concurrence regarding a cyber attack assessment. While CDRUSCYBERCOM understands the technical cyberspace issues involved during a cyber attack, CDRNORAD has the operational responsibility to provide aerospace and maritime attack warning for North America to the civilian military leadership of both Nations. Providing a joint cyber attack assessment would strengthen the validity of such an evaluation.

Advantages of COA #3 include:

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Leverages USCYBERCOM's global cyberspace visibility, technical infrastructure, and cyberspace expertise to accomplish an official cyber attack assessment.
- Leverages NORAD's visibility on current air defense operations and aerospace/maritime warning expertise to ascertain any effects on NORAD operations.

Disadvantages to COA #3 (and proposed alternative solutions) include:

- Some classified cyberspace threat information and technical TTPs are not currently releasable to Canadian personnel. (Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.)
- NORAD regional headquarters currently must drop off threat conferences during classified discussions. (Change DOD conference procedures to allow NORAD

regional headquarters to remain on cyber event conferences during classified discussions.)

- Modifies existing conference checklist procedures. (Modify cyberspace conference checklists to reflect joint CDRUSCYBERCOM/CDRNORAD cyber attack assessment.)
- Requires training NORAD General Officers for new cyber attack assessment coordination responsibility. (Build new training program for NORAD General Officer joint cyber attack assessment responsibility.)
- Changes existing relationships with USCYBERCOM. (Negotiate new command arrangements agreement between NORAD and USCYBERCOM.)
- Requires negotiating new cyberspace defense and response policies between the U.S. and Canada. (Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.)
- Requires changing the NORAD Agreement and/or Terms of Reference. (Negotiate change to NORAD Agreement and/or Terms of Reference, if required.)

Courses of Action Analysis and Results

Using inputs from numerous military cyberspace subject matter experts, I have weighted each COA's proposed implementation solutions using an increasing score:

- "1" (Routine; requires normal NORAD internal staff actions.)
- "2" (Challenging; requires detailed, U.S. government-wide staff actions.)
- "3" (Difficult; requires politically sensitive binational staff actions.)

I then summed all weighted solutions to present a total COA score for consideration. The COA which presented the greatest apparent advantages and the lowest disadvantages score was presumed to be the best COA for NORAD to pursue. (Figure 5 summarizes all three COAs, their proposed solutions and implementation weights, and their specific total scorings.)

Overall, this methodology (while not strictly scientific) still provides the reader a general measure of the relative cost of implementation for each proposed COA. (Before any COA might be adopted by NORAD, a formal military COA analysis should be conducted, to include surveys and/or interviews with cyberspace practitioners.)

		COA 1	COA 2	COA 3
Proposed Solutions	Weight	Full NORAD Cyber Conference Participation	NORAD All-Domain Warning Production	Joint NORAD + USCYBERCOM Cyber Attack Assessment
Modify cyberspace conference checklists to reflect full NORAD participation.	1	1		
Modify cyberspace conference checklists to reflect NORAD fusing and dissemination of all-domain warnings to both the U.S. and Canada.	1		1	

Modify cyberspace conference checklists to reflect joint CDRUSCYBERCOM / CDRNORAD cyber attack assessment.	1			1
Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.	2	2	2	2
Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.	2	2	2	2
Build new training program for NORAD personnel to fuse and disseminate all-domain warning updates.	2		2	
Build new training program for NORAD General Officer joint cyber attack assessment responsibility.	2			2
Negotiate new command arrangements agreement between NORAD and USCYBERCOM.	2			2
Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.	3		3	3
Change NORAD Agreement and/or Terms of Reference, if required.	3		3	3
SCORES		**5**	**13**	**15**

Figure 5. COA Analysis Summary.

COA #1 is a promising first step. Overall, this would seem to be a realistic, achievable COA that offers significant improvement in NORAD cyber attack situational awareness and operational effectiveness at a cost of only an administrative change in DOD information classification policy. Releasing classified cyberspace information to all NORAD personnel, and allowing NORAD regional headquarters to remain on cyber event conferences, also mirrors current U.S. national policies which repeatedly highlight the need for greater U.S. cooperation and information sharing with our international allies.

Under COA #1, existing classified cyber event conferences would continue as normal. However, updated internal NORAD operational checklists would be required to fully capitalize on new cyber attack warning information now being made available to NORAD personnel from such cyberspace conference attendance.

After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted implementation score of "5" would seem to indicate few major roadblocks to overcome.

Overall, while requiring several "challenging" staff actions through DOD to accomplish the desired releasability goal, this COA would enable greater information exchange between allies, would provide greater cyberspace situational awareness to NORAD, and would help Commander NORAD make more knowledgeable assessments regarding any potential attack upon North America.

By comparison, COA #2 proposes a much more active role for NORAD, assuming the issue regarding the releasability of classified cyber event information to Canadian personnel (proposed under COA #1) has been successfully resolved. It directs the Command to fuse military cyber event information with existing aerospace and maritime warning information to produce timely, all-domain warnings to U.S. and Canadian national civilian leadership using current NORAD binational military relationships and established warning processes.

While USCYBERCOM currently provides specific cyber event updates directly to military command centers, having NORAD produce broader all-domain warning products to both the U.S. and Canada would help both nations have a better appreciation for the effect a cyber event might have had on North American defenses.

Under COA #2, existing classified cyber event conferences continue as normal and capitalize on information now being fully available to all NORAD personnel. Updated internal operational checklists would be required to reflect NORAD fusing and dissemination of all-domain warnings to both nations. Also, a new training program would have to be built to train NORAD personnel on producing and disseminating all-domain warning products.

As cyber event information would initially be analyzed by USCYBERCOM, then provided to NORAD for further consideration, there would be no change to the existing relationships between the two commands.

Also, because this would be a major change to NORAD's legacy missions and processes, the U.S. and Canada might have to negotiate new cyberspace defense and response policies to ensure NORAD has the correct mission authority. Following such binational negotiations, The U.S. and Canada would also need to update the NORAD Agreement and / or Terms of Reference through international staffing channels.

After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted implementation score of "13" would seem to indicate several major roadblocks to overcome, mostly in the need to negotiate new international agreements between the U.S. and Canada.

Overall, while requiring both "challenging" and "difficult" staff actions both within DOD and internationally with Canada, this COA harnesses proven NORAD binational relationships and warning procedures to provide all-domain warning updates to both nations.

Finally, COA #3 is the most active NORAD option. Again, assuming the release of classified cyber event information to Canadian personnel (proposed under COA #1) has been successfully accomplished, this COA proposes a major change in current U.S. cyber attack assessment procedures.

While USCYBERCOM has strong technical understanding and global visibility of cyberspace activities, they often lack detailed insight into current operations being conducted by global combatant commands. Under COA #3, this deficit would be alleviated for North American air defense operations by directing NORAD to jointly participate in all North American-related cyber attack assessments. Commander NORAD would bring an awareness of on-going continental air defense operations, would provide essential operational expertise when adjudicating proposed cyberspace attack assessments, and could evaluate what effects any proposed follow-on cyberspace actions might have on current NORAD operations.

Some staffs have argued COA #3 is not required, as Commander USNORTHCOM (dual-hatted as Commander NORAD) already has the authority to declare a "Domestic Attack Assessment" if he judges the U.S. is under attack. Already having this authority would seem to obviate the need for him to assume an additional cyber attack assessment responsibility. However, his role as Commander USNORTHCOM does not specifically involve cyberspace operations, only involves U.S. military responsibilities, and does not involve notifications to the Canadian government which automatically occur within the binational NORAD structure.

Another concern voiced regards allowing another commander to participate in the cyber attack assessment process. One could argue if Commander NORAD needs to participate in North American-related cyber events, then should not Commander European Command participate in European-related cyber events, or Commander Pacific Command participate in cyber events occurring in Asia? Once the USCYBERCOM assessment process is opened to other geographic combatant commanders, does not this become a very slippery slope?

Under COA #3, existing classified cyber event conferences continue as normal. Updated internal NORAD operational checklists would be required to reflect joint CDRCYBERCOM and CDRNORAD participation in all cyber attack assessments. Also, a new training program would have to be built to train NORAD General Officers on their new joint assessment responsibility.

Additionally, if this COA were to be implemented, a new "Command Arrangements Agreement" between NORAD and USCYBERCOM would need to be negotiated to clearly outline the new cyber attack assessment responsibilities of each commander.

Further, because this would be a major change to NORAD's legacy missions and processes, the U.S. and Canada might have to negotiate new cyberspace defense and response policies to ensure NORAD has the correct mission authority. Following such binational negotiations, the NORAD Agreement and /or Terms of Reference would also need updating through international staffing channels.

After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted implementation score of "15" would seem to indicate several major roadblocks to overcome, mostly in the need to negotiate international agreements between the U.S. and Canada, and new command agreements between NORAD and USCYBERCOM.

Overall, while requiring both "challenging" and "difficult" staff actions both within DOD and internationally with Canada, this COA combines the advantages which both NORAD and USCYBERCOM offer to the cyber attack assessment process.

Recommendation

As the COAs were being developed, it became apparent they were not mutually exclusive, but in fact all three COAs could potentially be adopted sequentially over the course of several years.

COA #1 offers a major improvement in cyber situational awareness at little implementation cost. The difficulty will be in convincing DOD the need to change its administrative policies regarding the sharing of classified cyberspace operational information with Canadian military personnel. This would not be a trivial endeavor. However, numerous strategic policies emphasize the need to share this type of information with international partners,

and NORAD Canadians are clearly one of the longest and most enduring allies to the U.S. Overall, this COA would seem to be the easiest to implement while significantly improving NORAD's cyber situational awareness.

Later, as cyberspace information sharing with Canadians becomes routine, NORAD could reevaluate whether it is militarily desirable to pursue COA #2. This would be a subjective evaluation by the NORAD, USCYBERCOM, and other cyberspace information users to determine if there was value added in NORAD producing all-domain fused warnings. While COA analysis shows this to involve both "challenging" and "difficult" staff actions, a broader question might be "is there a real customer need?"

Finally, COA #3 may be militarily undesirable. Having Commander NORAD directly involved with North American cyber attack assessments seemed reasonable, but COA analysis showed many roadblocks to success. Further, the "challenging" task of negotiating new Command Arrangements Agreements between NORAD and USCYBERCOM might then generate the need to develop similar CAAs between USCYBERCOM and USEUCOM, USPACOM, etc. This greatly expands the overall impact of this COA, probably making this policy option "a bridge too far."

In conclusion, with global cyber attacks on the rise, it seems reasonable NORAD should explore potential new roles for cyber attack warning. Hopefully these three proposed COAs might serve as a beneficial roadmap for future NORAD consideration.

About the Author

Randall DeGering *is a retired USAF officer with broad experience in NORAD and USNORTHCOM air operations and joint military headquarters staff planning. A career Air Battle Manager, he's flown over 2700 hours aboard the E-3 AWACS conducting real-world theater air control operations around the world. With growing concerns posed by international cyberspace threats, he focused his thesis research on an emerging operational issue relevant to his current employment in NORAD. He may be reached at randall.r.degering.civ@mail.mil.*

Disclaimer

The views expressed in this essay are the author's alone.

Notes

1. NORAD History Office, Brief History of NORAD, (Colorado Springs, CO: 30 Dec 2012).

2. Carey Sublette, "The Soviet Nuclear Weapons Program," *The Nuclear Weapons Archive*, last modified 12 December 2007, http://nuclearweaponarchive.org/Russia/Sovwpnprog.html.

3. Ibid.

4. *Brief History of NORAD*, 6.

5. U.S. Air Force Factsheet, "Infrared Satellites," accessed 19 Dec 2014, http://www.losangeles.af.mil/About-Us/Fact-Sheets/Article/343740/infrared-space-systems-directorate.

6. "2014: Piracy, Terrorism and Direct Maritime Threats," *The Maritime Executive*, 14 Mar 2014, accessed 20 Apr 2015, http://www.maritime-executive.com/article/2014-Piracy-Terrorism--Diverse-Maritime-Threats-2014-03-14.

7. NORAD History Office, Letter from CDRNORAD to CJCS, dated 15 Jul 2004.

8. NORAD History Office, *NORAD Agreement*, 28 Apr 2006.

9. NORAD and USNORTHCOM, *NORAD Strategic Review*, 3 Dec 2014. (Note: Only unclassified paragraphs were quoted.)

10. Marcus Weisgerber, "Interview: General Charles Jacoby," *Defense News*, 19 Jul 2014.

11. Ibid., 22.

12. Ibid., 23.

13. U.S. Senate, Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community, 24 Jan 2014," accessed on 20 Apr 2015, https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf.

14. "Russia Preparing New Cyber Warfare Branch, Military Officials Say," *Softpedia*, accessed 17 Dec 2014, http://news.softpedia.com/news/Russia-Preparing-New-Cyber-Warfare-Branch-Military-Official-Says-376807.shtml.

15. Pierluigi Paganini, "APT28: Fireeye Uncovered a Russian Cyber Espionage Campaign," Security Affairs, 29 Oct 2014, accessed 17 Dec 2014, http://securityaffairs.co/wordpress/29683/intelligence/apt28-fireeye-russian-espionage.html.

16. U.S. Senate, Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community, 24 Jan 2014."

17. Michael Schmidt and David Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times*, 19 May 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0.

18. U.S. Senate, Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community, 24 Jan 2014."

19. U.S. House Committee on Foreign Affairs, Joint Subcommittee Hearing, "Iran's Support for Terrorism Worldwide," 4 Mar 2014, accessed on 4 Apr 2015, http://docs.house.gov/meetings/FA/FA13/20140304/101832/HHRG-113-FA13-20140304-SD001.pdf.

20. Ju-min Park and James Pearson "In North Korea, Hackers Are a Handpicked, Pampered Elite," *Reuters*, 5 Dec 2014, http://www.reuters.com/article/2014/12/05/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205.

21. Kyung Lah and Greg Botelho, "Watch Out World: North Korea Deep Into Cyber Warfare, Defector Says,"*Cable News Network*, 18 Dec 2014, http://www.cnn.com/2014/12/18/world/asia/north-korea-hacker-network/index.html.

22. Thomas Rid and Peter McBurney"Cyber-Weapons," *The Rusi Journal*, Feb/Mar 2012, 6–13, accessed 21 Apr 2015, http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354.

23. Paul Day, *Cyberattack* (London, UK: Carlton Publishing Group, 2013), 120–122.

24. "Cyber Attacks on South Korean Nuclear Power Operator Continue," *The Guardian*, 28 Dec 2014, accessed 21 Apr 2015, http://www.theguardian.com/world/2014/dec/28/cyber attacks-south-korean-nuclear-power-operator.

25. "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," *National Academy of Science*, 2014, vii, accessed 17 Dec 2014, http://www.nap.edu/openbook.php?record_id=18749.

26. Ibid., 30.

27. United Nations General Assembly Resolution 3314 (XXIX), "Definition of Aggression," Article 1 (Dec 14, 1974), accessed 18 May 2014, http://www.un-documents.net/a29r3314.htm.

28. Ibid., Article 3.

29. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge, UK: University Press, 2013.) (Note: Tallinn is the capital of Estonia, where the first modern cyber attack occurred, where the NATO Cooperative Cyber Defense Center of Excellence is now located, and where this manual was eventually developed.)

30. Ibid., 48.

31. Ibid., 48–51.

32. Ibid., 52.

33. Ibid., 106.

34. NATO Wales Summit Declaration, 5 Sep 2014, paras 72–73, accessed 17 Dec 2014, http://www.cfr.org/nato/wales-summit-declaration/p33394.

35. Adm James Stavridis, "Incoming: What is a Cyber Attack?" *Signals*, 1 Jan 2015, accessed 21 Apr 2015, http://www.afcea.org/content/?q=node/13832.

36. Ibid.

37. Ibid.

38. Ibid.

39. Ibid., 3–2.

40. Department of the Army, Field Manual 3–38, "Cyber Electromagnetic Activities," 3–7 Feb 2014, accessed 21 Apr 2015, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf.

41. Ibid., 3–7.

42. Ibid., 3–6.

43. Ibid., 3–6.

44. Ibid., 3–6.

45. Ibid., 3–2.

46. Ibid., 3–3.

47. U.S. Department of Defense, "Emergency Action Procedures of the Chairman of the Joint Chiefs of Staff, Volume VI, Emergency Conferences (U)," 14 Sep 2012, (Note: Information presented are from unclassified paragraphs.)

48. Ibid., II-14.

49. Ibid., II-14.

50. Ibid., II-14.

51. Lockheed Martin, "Integrated Space Command & Control (ISC2)," accessed 13 Jan 2015, http://www.lockheedmartin.com/us/products/isc2.html.

52. U.S. Department of Homeland Security, "Cyberspace Policy Review," 2009, iii, accessed 6 Feb 2014, http://www.dhs.gov/publication/2009-cyberspace-policy-review.

53. Ibid., 2.

54. Ibid., vi.

55. The White House, "National Security Strategy," 2010, accessed 4 Feb 2014, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

56. The White House, "Launching the U.S. International Strategy for Cyberspace," 2011, accessed 11 Feb 2014, http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace.

57. U.S. Department of Defense, "Chairman's Corner: 2011 National Military Strategy," accessed 13 Jan 2015, http://www.defense.gov/Portals/1/Documents/pubs/2011-National-Military-Strategy.pdf.

58. Ibid., 10.

59. Ibid., 19.

60. Canadian Department of National Defence, "Canadian Armed Forces Cyber Operations Primer," Feb 2014, 6.

61. U.S. Department of Defense, Joint Publication 5–0, "Joint Operation Planning," 11 Aug 2011, IV-24 through IV-36, accessed 21 Apr 2015, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.