NATO OTAN

RESEARCH PAPER

Research Division - NATO Defense College, Rome - No. 62 – November 2010

Cyber war and cyber power
Issues for NATO doctrine

by Jeffrey Hunker[1]

Contents

Research Paper
ISSN 2076 - 0949
(Res. Div. NATO Def. Coll., Print)
ISSN 2076 - 0957
(Res. Div. NATO Def. Coll., Online)

NATO Defense College
Research Division
Via Giorgio Pelosi, 1
00143 Rome – Italy
web site: www.ndc.nato.int
e-mail: research@ndc.nato.int

Imprimerie Deltamedia Roma
Via Iberia 19/a 00183 Roma
www.deltamediagroup.it

"Cyber war" is now the subject of considerable attention in the US, both in the popular media and in policy realms (together with its companions, cyber threats, cyber attacks, cyber terrorism, and cyber weapons). For those in NATO it is important to understand what cyber war and related terms mean, why they are the subject of US focus, and what the implications for NATO are. That is the purpose of this paper.

The combination of extensive dependence on cyber systems and the pervasive security vulnerabilities in these systems is the foundation for the growing concern about cyber war and other cyber threats. Unfortunately, one challenge of discussing cyber war is that there are few, if any, commonly shared definitions or clear cut distinctions between key concepts. When is a cyber attack an act of war or a crime? Indeed, when is an unauthorized penetration of a cyber system a cyber attack? What are cyber weapons? How would the attacked know where a cyber attack originated from, or even that they are being attacked, and what degree of confidence is required to respond? What responses are legal, or appropriate? And, from the adversary's perspective, how does the attacker know if a cyber attack will be successful?

This paper first explains the basis for concern about threats to cyber systems, and distinguishes between the different types of cyber threats and attacks. I define cyber attack and other key concepts, fully aware that there are many alternative definitions, and then review the history of events that relate to cyber war. In doing so, I will introduce the concept of cyber power.

A key conclusion of this paper is that, for NATO, cyber war as the focus of concern is a misnomer; the real or potential use of cyber power by nations or terrorist groups should be the principle focus. Cyber war is just one outcome of the exercise of cyber power between nations. The central part of the paper will outline some of the special characteristics that distinguish cyber power from the other elements of national power, and point to some of the challenges that these special characteristics present in developing a doctrine of cyber power.

1 Jeffrey Hunker is Principal of Jeffrey Hunker Associates LLC, Pittsburgh Pennsylvania, USA. hunker@jeffreyhunker.com. He is author of Creeping Failure: How We Broke the Internet and What We Can Do to Fix It, McClelland and Stewart, 2010. The views expressed in this paper are the responsibility of the author and should not be attributed to the NATO Defense College or the North Atlantic Treaty Organization.

I will then briefly review NATO and US policy relating to cyber power, and point to the need by NATO and NATO members to develop a cyber power doctrine, supported by coherent foreign policies.

I. DEPENDENCE AND VULNERABILITIES IN CYBER SPACE

Cyber space is the notional environment in which digitized information is stored or communicated over information systems and networks. Largely because of the Internet, in a very short time – less than twenty years – much of what goes on in advanced countries depends on cyber space. Critical infrastructures like pipelines and many industrial processes now run on Supervisory Control and Data Acquisition (SCADA) systems, many of which are connected through the Internet[2]. Whether a phone call is on Skype, cellular or normal phones, much of long distance telecommunications is routed either on the Internet or through the same fiber optic cables carrying Internet traffic.

Cyber space is rife with vulnerabilities – ways in which malicious actors can cause cyber systems to behave in manners in which they were not intended to behave. Vulnerabilities may be due to design error, or inherent in the design of the systems, and may overlap with 'bugs', which are defects that may also cause accidents. Vulnerabilities exist at the system level, e.g. in desktop software. Vulnerabilities also occur at the network level. The Internet, for instance, depends on the Domain Name Service (DNS) to look up network addresses; the DNS ultimately runs on 13 computers which, if malfunctioning, would disrupt, albeit slowly, the workings of the Internet. Distributed denial of service (DDOS) attacks rely on massive floods of incoming data packets[3] to prevent users from accessing systems, without actually harming the systems affected directly. Despite much attention to reducing vulnerabilities, cyber space will remain exposed to malicious attacks.

II. EXPLOITING VULNERABILITIES: DEFINING TYPES OF CYBER ATTACKS

There are many ways of exploiting vulnerabilities – from the attacker on another continent remotely inserting malicious software into a system to a co-worker stealing a password. However done, the act of exploiting or attempting to exploit a vulnerability without authorization is a cyber attack (this is my definition; there is no consistent terminology here). Since there are so many ways of exploiting vulnerabilities – i.e. launching a cyber attack – the term 'cyber weapon' is meaningless in general usage.

The goal of a cyber attack can be to either:

• copy and then remove data without disrupting the systems or data - a *passive cyber attack*[4] - or

• disrupt cyber space systems by corrupting or changing data, affecting system or network service, or denying or preventing use of systems or networks - a *disruptive cyber attack*[5].

A passive cyber attack could either be a cyber crime, e.g. theft of passwords or credit card data, or cyber espionage or intelligence collection if done by a state. Cyber crimes could also be committed by terrorists, as for example committing cyber theft in order to raise funds for operations.

A disruptive cyber attack could be a cyber crime committed for greed, vandalism, revenge or extortion, or could be an act by terrorists, non-state actors or a state.

Disruptive cyber attacks could have potentially serious physical consequences with social and economic implications; for instance, electrical power systems and rail lines are managed through cyber space. US policy names eighteen economic sectors as critical infrastructures whose functioning is essential for security, economic and social welfare; most of these critical infrastructures, including information technology, telecommunications, electric power and oil and gas depend in large part on cyber systems for their operation. A recent US government inquiry into the cyber security of one large electric utility found significant vulnerabilities that left it open to cyber attack. US policy makers are concerned about the vulnerability of military systems too: in 1997 the Eligible Receiver exercise aimed at testing the Pentagon's cyber security; within two days attack teams had penetrated the classified command network and were in a position to issue bogus orders.

With valuable information and key services dependent on cyber systems, not surprisingly cyber crime in all forms has grown rapidly

[2] The Stuxnet Worm first observed in September 2010 is reported in the press to have been intended to target and disable the SCADA systems of Iran's first nuclear power plant. This is the first (?) high profile example of a cyber attack specifically against SCADA systems.
[3] The Internet transmits messages/information by breaking the message into many discrete data packets, each of which may be sent across the Internet using different paths to arrive at the final destination, where the Internet Protocol reassembles the packets to reform the original message.
[4] The US DOD uses the terminology "computer network exploitation" and "computer network attack" for passive and disruptive cyber attack; attacks need not involve networks (although they usually do), and 'exploitation' is less clear than the intended effect, which is to be passive, leaving the system undisturbed.
[5] A fuller definition of nation-state disruptive cyber attack: the unauthorized penetration, use, or denial of use by a nation-state (or its proxies) of another nation's cyber systems (whether government or private) for the purpose of causing the disruption of or damage to these systems or their use, or the systems

and is now the province of sophisticated criminal organizations operating globally. Total cyber-related business losses in 2009 are estimated to be US$ 42 billion for the United States, and US$ 140 billion globally[6].

Cyber espionage, too, is a major threat. US counter-intelligence officials estimate that 140 different foreign intelligence agencies regularly attempt to hack into US commercial and government computers. Note that cyber espionage sometimes occupies a grey area between passive and disruptive forms of cyber attack. While traditional espionage per se does not appear to violate international law, many of the technical means of conducting cyber espionage (e.g. by implanting malicious software into the target systems) are close to or almost identical with the technical means of mounting a disruptive attack on the same system. Also, the amount of data that can be obtained and the speed of cyber espionage can be of a different order of magnitude from that of more traditional espionage operations. In April 2009 someone illicitly downloaded terabytes of information from US national security computers related to the development of the F-35. With a high degree of certainty, these officials believe that the intrusion can be traced back to an Internet address in China and that the signature of the attack implicates Chinese government involvement[7].

In parallel with cyber espionage capabilities, reportedly many nations have been developing disruptive cyber attack capabilities. China is a sophisticated cyber state, having recently surpassed the US in the number of Internet users. China talks of "winning informationised wars by the mid-21st century" and is according to US analysis developing "an advanced information warfare capability, the stated goal of which is to establish control on an adversary's information flow and maintain dominance in cyberspace." In April 2009 the Wall Street Journal reported that China had planted logic bombs[8] in the US electric grid. Many other countries are building up disruptive cyber attack capability, among them Russia, Israel, and North Korea[9].

III. INCIDENTS OF CYBER WAR?

Almost certainly, we have already seen disruptive cyber attacks by one nation against another nation, though I am unaware of any cases of terrorist groups launching disruptive cyber attacks. Some of these events have been described as cyber war. The following are select instances:

In May 1999, following the accidental bombing of the Chinese embassy in Belgrade, Chinese hackers targeted US government web sites; the White House shut down www.whitehouse.gov for three days because of security concerns stemming from the non-stop DDOS attacks.

In 2007, during a period of tension with Russia, Estonian government, commercial and private organizations, notably banks, were the subject of three weeks of DDOS attacks. Other DDOS attacks occurred against Georgia in 2009, prior to kinetic military action with Russia, and against Kyrgyzstan in 2009. In all cases, the likely governments – China and Russia respectively – denied any involvement; the cyber attacks against Georgia were orchestrated from a control computer in Brooklyn, New York City.

Reportedly, also in 2007, Israeli jets bombed a complex in eastern Syria. Under construction with a North Koran labor force, the complex was to have been a North Korean-designed nuclear weapons plant. Israeli jets were able to penetrate Syrian air space without detection, having somehow evaded or subverted sophisticated air defense networks (provided by the Russians) through a cyber attack[10].

To summarize, the combination of dependence on and vulnerabilities in cyber space, together with a growing record of cyber attacks exploiting these vulnerabilities, supports the perception that cyber space is a realm where national interests – military, diplomatic, economic and social – are now at risk.

(including physical infrastructures) which these systems control. This definition is mine, but is based on elements of other definitions.

[6] Estimated losses due to cyber crime are highly unreliable; many businesses prefer not to report cyber crime. Cyber crime has exploded since 2000 and has become a form of organized crime. D.C. Blair, *"Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence"*, Washington, Director of National Intelligence, 2009, http://intelligence.senate.gov/090212/blair.pdf (accessed 27 September 2010).

[7] Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do about It, New York, HarperCollins, 2010, 233.

[8] A logic bomb is a piece of software intentionally and maliciously inserted into a software system (e.g. a computer) that will damage or destroy the system's functionality when a specific condition occurs (e.g. a certain date is reached) or by command.

[9] A thorough recent discussion of Chinese capabilities is Steve DeWeese et al., *"Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation"*, Report prepared by Northrop Grumman Corp. for the US-China Economic and Security Review Commission, Washington, 17 February 2010, www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_Final_Approved Report_16Oct2009.pdf (accessed 27 September 2010). See also "War in the Fifth Dimension: Briefing on Cyber war", *The Economist*, 3 July 2010, 25-28.

[10] Clarke op. cit. (who provides no citations to support his material).

IV. THE CONCEPT OF CYBER POWER

The focus of NATO concern should not just be cyber war per se but rather the direct or threatened exercise of ***cyber power*** through computer network attacks. While attractive in the media, cyber war is a special form of disruptive cyber attack[11]:

• *Cyber warfare* is a serious form of disruptive cyber attack by a nation on another nation's cyber space, crossing the line into being considered a use of force. Issues of the Law of War come into play.

Note that an act of cyber war is only one outcome of a nation launching a disruptive cyber attack. Cyber power as a concept covers more completely aspects of concern to NATO:

• *Cyber power* is the use, threatened use, or effect by the knowledge of its potential use, of disruptive cyber attack capabilities by a state[12].

It is worth pointing out that most discussions of 'cyber war' reference instances of disruptive cyber attack where the parties neither enter into nor are already in a state of armed hostilities; the Georgian attack is an exception. In other words, most discussions are not about war but about the use of power.

Nations may project cyber power in many ways – in concert with other kinetic military operations, masked and with no clear link to the attacker, as part of a complex military-diplomatic escalation, or in indirect manners to exert influence or advance national goals. Note that passive cyber attacks – meaning mostly espionage – are not elements of cyber power, just as non-cyber espionage is not an element of national power as usually defined. Massive cyber espionage programs, or the technical means of conducting cyber espionage that could be perceived by the target as tools of disruptive cyber attack, are "grey areas" for how cyber espionage might be regarded.

Cyber power has some unique characteristics which shape its effective use:

Cyber space is a wide and dynamic environment. The pace at which change occurs far exceeds that of almost all physical systems. Change is not just in technological innovations; transformations are ongoing in network and system configurations, uses, and social/organizational interactions. Detailed maps of cyber space, if any existed, would almost immediately become obsolete.

Cyber weapons, once used, often lose their effectiveness: many cyber attacks depend on exploiting vulnerabilities unknown or unpatched – i.e. not fixed – by the target. Once a particular vulnerability has been exploited, especially in a noteworthy cyber attack, most likely that vulnerability will be patched, and the particular cyber weapon will lose its effectiveness. This is not universally true; for example DDOS attacks do not depend on vulnerabilities in the target system, and in effect there are no good defenses against these types of attacks.

Offensive operations dominate in cyber space: the challenge to defense is to patch all vulnerabilities; the attacker's opportunity lies in finding only a single key vulnerability in complex systems. There is no indication that this inherent attacker advantage will change in the foreseeable future.

Cyber operations can occur at the speed of light: physical constraints related to the use of kinetic weapons do not apply to cyber attacks.

Cyber attacks have global dimensions: almost by definition, given the topology of cyber networks, cyber attacks will transit nations other than just the attacker and targ et. This can create challenges (discussed later) in identifying the true source of an attack – a cyber trail may grow cold at an intermediate location with no resolution as to the true attack source. Or, cyber attacks can be mounted from cyber systems located in countries other than the attacker – with or without the knowledge of the other state or system owner). The physical and technical resources required for an attack are not necessarily large enough to generate special notice, even if operating in another country.

---

[11] Military doctrine categorizes the four elements of national power under the acronym "DIME" – Diplomatic, Information, Military and Economic. "Information" as an element of national power describes a grab bag; for the US Defense Department "information operations" include electronic warfare, psychological operations, military deception, operations security and computer network operations. Computer Network Operations –the topic of this paper – is further divided into computer network attack, computer network defense and related computer network exploitation enabling operations to be conducted. I would argue that the special characteristics of cyber power and cyber space (to be discussed shortly) support cyber power as a fifth element of national power. Cyber space is neither a physical realm (where military operations have historically taken place) nor a perceptual sphere (e.g. that of "psych ops"). The closest historical analogy to disruptive cyber attack might be, for example, the scrambling or distortion of adversary radio communications. The potential scope and impact of cyber attacks is so much greater than what might be seen in historical analogies to again argue that cyber should be considered a fifth element of national power.

[12] See also Franklin D. Kramer et al., *Cyberpower and National Security*, Washington, Center for Technology and National Security Policy, National Defense University Press, Potomac Books, 2009, 48.

V. DISRUPTIVE CYBER ATTACK IN COMBINATION WITH OTHER ATTACK MODES

I would further argue that disruptive cyber attacks conducted without any kinetic accompaniment do not make much sense in large-scale warfare. Disruptive cyber attacks can destroy important data and disrupt communications, and perhaps seriously affect physical operations like transportation and the management of large scale networks like electric power. But even now major electric blackouts, or communications systems failures, are not unknown, and yet advanced countries manage to carry on. While the impact of cyber attacks may be hard to gauge in advance (see discussion below), the effect of disruptive cyber attacks is to throw sand into the gears.

For a rational player, the benefit of pure cyber attacks is in the demonstration of power, as in situations of escalating state-to-state tension or in limited war. Alternatively, cyber might be employed through proxy actors. In either case, though, its effectiveness as a stand-alone projection of power will be limited.

More attention needs to be given to the combination of cyber with physical attacks in any future conflict. For instance, occasionally major telecommunications blackouts in the US, including disruptions to civilian air traffic control, have occurred because a cable was accidentally dug up somewhere. If the intent were to disrupt select critical infrastructures, physical damage – like a dozen or so rented mechanical diggers, each accidentally cutting a cable on a select day – combined with cyber disruptions might be very effective. A physical attack could damage transmission nodes, for instance, while cyber attacks disrupt the damage assessment and response functions. Combined attack modes might be far more complex and difficult than single mode attacks to assess and prevent. Combined attacks might be particularly difficult to recover from if specialized equipment with few backups were destroyed; for instance, reportedly there are very few spare SS7 switches, the key switches in managing telecommunications backbones[13].

Importantly, NATO military systems rely heavily on information systems, many of which transport data over commercial networks. If a combined cyber-kinetic attack actually did succeed in disrupting commercial communications systems for hours or days, the potential to cripple military command and control (C2) systems might be a serious concern. Also, many weapons platforms rely on networked data transmissions, and these systems may have their own unique vulnerabilities to combined cyber-physical attacks.

Because of the limited impact of disruptive cyber attacks, cyber terrorism is probably an oxymoron. Cyber attacks conducted by terrorist organizations, for instance as criminal activities to finance their efforts, are likely in the future if not already taking place. Terrorist organizations routinely use the Internet for communications and other purposes, just like any organization. But disruptive cyber attack is not an effective means of inducing terror in target populations. Even when, not if, terrorist organizations acquire the ability to launch sophisticated cyber attacks, these incidents largely will be shaped by the same considerations affecting state action. Most likely, terrorist attacks using cyber will also simultaneously employ kinetic means.

VI. THE USE OF CYBER POWER

Since everything associated with cyberspace is new – the very term "cyber space" dates back only to 1982 – not surprisingly the use of cyber power presents a number of challenges. Effective cyber power doctrine will have to address the following:

Technical attribution of the source of the attack is difficult

Electrons do not bear national markings. Because the Internet's creators never envisioned the need, the Internet has no reliable means for tracing where a message comes from. Furthermore, the Internet model was not designed to withstand malicious alteration of the transmission packets[14] ; it is easy for attackers to forge the source address – the sender's address – of a packet in a one-way communication. Usually network attack techniques employ a series of stepping stones, using compromised intermediate hosts to "launder" packets sent. These packets can be changed in transmission hops between hosts, and so attempting to trace attacks by correlating similar packets will not work against a sophisticated attacker. Some of the best though inadequate means of attribution require "hacking back" through intermediate systems. A hack back may itself result in significant violations of the Law of War.

[13] SS7 stands for Signaling System No. 7, and is the name for the switches and supporting protocols that operate the major (trunk) telephone lines.
[14] See also Footnote 2. Each Internet packet has along with its small portion of the message an address header that directs the packet through intermediate to its final destination (think of a router as a postman sorting mail based on the packet's address heading). The address header also contains the address of the sender; it is easy for a malicious hacker to alter this header information to make it appear that the message is actually coming from a different person, not the one who actually sent it.

Therefore, the potential – perhaps great potential – exists for misattributing the source of cyber attack. This risk is compounded by the speed at which cyber power can be exercised.

There is no standard for how much evidence for the attribution of the attack is required for a particular type of response by the state attacked. The open question is whether a target state can lawfully act against the proximate or likely source of the attack, even though the target is by no means certain that the attack originated there.

Even if a nation acknowledges that an attack came from computers on its territory, the government could claim that the attack was from anonymous (or "patriotic") citizens, as in the case of the Estonian and Georgian attacks, and the attacks against the US originating in China. The possible cooperation of non-state actors in a state-sponsored cyber attack further complicates attribution. Since the technical skills required for cyber attack are similar or equivalent to those of sophisticated cyber criminals and hackers, it may be that cyber attacks, though sanctioned or supported by the attacking state, use cyber criminal or hacker resources in part or whole. Hence, the challenge of attribution may extend not just to identifying the actual location of the cyber systems used in the attack but also to tracing the organizational linkages.

Alternatively, an attack could be traced back to a nation that claims that its systems were merely intermediate points from another state or actor, or unknowingly served as the launching point for a cyber attack. The circumstances in which lawful action can be taken by a target state against this intermediate nation are still being defined by legal experts and will be discussed later

The effects of a cyber Attack can be highly uncertain or unexpected

Since some attack tools, like worms and viruses, can spread globally, there is a real risk of collateral damage as these agents spread uncontrollably. The original worm, the Morris worm of November 1988, caused extensive damage to the nascent Internet, though that was certainly not the intent of its creator, a student from Cornell.

Also, cyber attacks seek directly to change the performance of highly complex cyber systems, which in turn may affect the behavior of other highly complex physical systems like infrastructures. The behavior of complex systems is, in general, not well understood; for instance, the actual causes of some widespread (accidental) electric power outages have never been satisfactorily explained. It seems likely that unanticipated system behavior may cause outcomes other than those intended by the attacker.

Finally, cyber attackers may not know with certainty the extent to which the target has significantly improved its defenses, or has back-up, perhaps non-cyber systems, to support critical functions.

These uncertainties can have serious implications. On legal and humanitarian grounds, unexpected collateral damage could be viewed as indiscriminate attack. If the unplanned impacts of a cyber attack include cutting off the target's command structure from component forces, then even more serious military and diplomatic problems could arise.

For the target it may be difficult to distinguish intent

If the target state sees only the technical details of a particular cyber attack, their decision makers may find it almost impossible to determine whether the attack was launched by a nation or by terrorists, criminals or vandals. Information from sources other than a technical analysis of what happened to the cyber systems attacked may be needed to attribute the source of the attack. Even if the source of the attack is known, it may be difficult to ascertain what the intent was. A passive attack, such as an act of cyber espionage, can have technical details very similar to an intentionally disruptive attack. Unlike physical attacks, the true damage resulting from a cyber attack may be difficult to assess quickly. The target decision makers may be uncertain of the 'true' impact of the attack for a period of time, and therefore assume the worst until further information is available; if target decision makers fear that the operational effectiveness of their command and control structure has been compromised, this period of uncertainty may be further extended. Although waiting "to see" what course an observed cyber intrusion takes may be the only effective way to determine its intended effect, waiting may not be a viable option for target decision makers who fear that a disruptive attack is underway.

Furthermore, some cyber attacks may have impacts that build up slowly and gradually, as in the case, for instance, of an attack against a financial system designed to corrupt data incrementally. The knowledge that such an attack has taken place presents the target decision makers with a potentially complicated set of choices about matters such as defense and response.

Accidents can happen

Even with proper command and controls in place, accidental cyber attacks can occur. As can happen when accidentally sending an e-mail, the wrong code could be relayed to a target; or a logic bomb or other software already implanted in the target system could be accidentally triggered by the network operators or a hacker.

Threatening the 'use of force' in cyber space can be problematic

There may be a limited range of circumstances in which a threat to launch disruptive cyber attack will be regarded as credible by either the target state or the community of nations. A DDOS attack can be credibly threatened; there are no effective short term defenses, and the attack can be terminated at will. Cyber criminals routinely use the threat of DDOS attacks in extortion against on-line businesses. In other cases, however, the threatened use of cyber power, like the threat of force, which is prohibited by Article 2(4) of the UN Charter, may be less convincing. With exceptions like DDOS attacks, most disruptive cyber attacks are based on one-time use techniques, so that a demonstration attack may actually work to the detriment of the attacker. It seems therefore that the threatened use of cyber power will remain problematic. In other words, for diplomacy and cyber power to work in concert new ideas may have to be developed.

Consequently, deterrence in cyber space remains an undeveloped concept. The lessons of nuclear deterrence are not uniformly applicable to cyber power. Nuclear deterrence was based on a common understanding of the effects of nuclear devices and a certain confidence in the impact of promised deterrent actions. With cyber weapons, however, the same degree of confidence cannot be placed in their performance on demand. Furthermore, it is difficult to stage effective demonstrations of cyber power without reducing the very effectiveness of the cyber arsenal. Basing deterrence on other modes of response, e.g., kinetic responses, may further worsen a situation and certainly raises its own legal and diplomatical issues. Cyber space deterrence may thus have to rely on new formulations, just as nuclear deterrence evolved from concepts different from those common to conventional military power.

Command structure and definition of combatants need clarification

In the US at least, authority relating to the use of cyber power appears fragmented both across the national security community and between the government and private sector. The intelligence community uses tools very similar to those used by the military, but for very different purposes, and reports through different command structures. NATO appears to be addressing the challenges of cyber war in its forthcoming Strategic Concept, while in the US a sub-unified military cyber command has been created (see below). Nonetheless there remains some potential for multiple authorities to direct less than perfectly coordinated operations, particularly given the nascent state of cyber operations overall. Furthermore, in the US government, responsibility for cyber security is divided between the Departments of Defense (DOD) and Homeland Security (DHS).

Deciding whether and how to incorporate private sector network management and control into a command structure may be even more challenging than coordination within governments and across Alliance members. Coordination across private networks and with the government depends on decisions made by civilian network managers of privately owned critical infrastructures. While better in some sectors, notably telecommunications, overall coordination is voluntary and seems haphazard.

A second major issue, affecting military, non-military government, and private sector networks alike, is the role of civilians in supporting or operating cyber systems used in disruptive cyber attack. In this context the difference between combatants and non-combatants, traditionally fundamental in kinetic war, is far more nebulous. Given the principle of distinction, must the person who physically presses the 'send' button launching a cyber attack be viewed as a combatant? It would be easy to envision circumstances in which major parts of actually performing the functions of cyber power (e.g., software development, network management) were outsourced to the private sector, including international companies resident in NATO countries.

Cyber attack is a developing area under the law[15]

A key question in the deployment of cyber power is under what circumstances a cyber attack or continuous series of cyber attack can constitute an armed attack, thus triggering the target states' right to respond forcefully through a legitimate exercise of self-defense. The Law of Armed Conflict provides the primary legal framework for understanding when it is legal for one nation to use force against another (jus ad bellum) and the rules that govern the behavior of combatants who are engaged in armed conflict (jus in bello). In cyber attack, these considerations are important both for a target nation formulating appropriate and effective responses, and for the state contemplating cyber attack prior to the outbreak of hostilities but without intending to give cause for the outbreak of general hostilities.

---

[15] For a much more detailed discussion, and many references, see "Cybersecurity Symposium – National Leadership, Individual Responsibility", *Journal of National Security Law and Policy 4*, No. 1, 2010. http://jnslp.com/ (accessed 27 September 2010).

The UN Charter prohibits a state from either threatening or using force against another state in the international community, excepting actions authorized by the Security Council, or acts of self-defense. Appropriate self-defense must reflect the principles of both "necessity" and "proportionality".

Legal scholars conclude that a considerable body of international law does apply to the use of force in cyber space. Some states, including the US, and the UN General Assembly have specifically identified cyber attacks as a threat to international peace and security. However, given their relative newness, there is no legal precedent as to how offensive cyber operations should be regarded. In defining when cyber attacks constitute a use of force, an "effects based approach" focuses not so much on whether a cyber attack qua cyber attack constitutes a use of force, but whether a cyber attack with a specific effect constitutes a use of force. The US appears to have adopted this perspective. For example, in using this approach a disruptive cyber attack on the financial system, significantly disrupting commerce, would result in damage to the state's economic well-being equated with an armed attack. A question is how to regard the placement, but not actual use, of logic bombs or other disruptive cyber attack software in target systems. Do these constitute hostile intent? Are they the cyber analogy of placing a large explosive device under a target military installation? Or are they more like 'sleeper agents', as remembered from the Cold War?

Three other issues relate to the definition of use of force. Although traditionally espionage has not been regarded as a use of force, there is some belief that cyber espionage, conducted over an extended time period and in large volume, as might be the case for the F-35 incident, constitutes a demonstration of hostile intent. Do such passive cyber attacks justify responses beyond taking additional passive defense measures? Such responses might include conducting counter-probes of the adversary networks from which the intrusions are originating, and even attacking these networks to neutralize the probes. These responses are sometimes called an "active defense", and we will return to the implications of this approach when discussing NATO cyber defense policy. Finally, cyber operations affecting economic functions also fall into the ambiguities inherent in international law between the use of economic sanctions (which is legal), and blockades, which constitute an act of war.

A second set of questions relates to the nature of appropriate response and when can and should non-cyber responses (e.g., kinetic means) be employed in response to cyber attacks. This issue, relevant also to a concept of cyber space deterrence, remains unclear; there is to date no precedent. Such use might violate Law of War jus ad bellum considerations.

Also at issue legally is the perceived requirement that the target state must conclusively attribute a cyber attack to another state or its agents. Nations following this dictum historically have chosen to respond to cross-border cyber attacks as they would to criminal acts. However, in the case where a nation claims that non-state actors are at fault, over the past twenty years new thinking has emerged as to assigning state responsibility – as a sanctuary state – for the actions of non-state actors. Under the concept of "indirect responsibility" a state has an established duty to prevent its territory from being used as a launching pad for attacks. In the International Law Commission's Draft Articles on the Responsibility of States for Wrongful Acts (2001), and as recognized by the UN General Assembly, the state is said to have breached its duty of responsibility when it consistently fails to undertake specifically identified measures designed to prevent attacks, such as the passage of legislation criminalizing cyber attacks and the corresponding cooperation in investigation and prosecution of those engaging in cyber attacks. In that case, it becomes a sanctuary state and is vulnerable to a legitimate use of force by the victim state.

VII. NATO AND US POSTURE RE CYBER WAR

NATO

NATO documents usually reference cyber defense rather than cyber war or cyber power. Operationally NATO cyber defense activities are centered in three groups:

• The NATO Computer Incident Response Capability (NCIRC), created in 2002, handles and reports cyber security incidents and disseminates important incident-related information to systems/security management and users. NCRIC is part of the NATO Communications and Information Services Agency.

• The Cooperative Cyber Defence Center of Excellence (CCDCOE) was established in 2003, and accredited as a NATO Center of Excellence (COE) in 2008. It conducts research and training on cyberwarfare. Currently sponsoring Alliance members are Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, and Spain, with the US, Turkey, and Hungary joining. Its activities are also supported by the NATO Science Programme.

• The Cyber Defence Management Authority (CDMA) has sole responsibility for coordinating cyber defense across the

Alliance. CDMA is overseen by the NATO Consultation, Control and Command (NC3) Board. Also, in August 2010 the Emerging Security Challenges Division (ESCD) was created within the NATO International Staff to address non-traditional risks and challenges, including cyber defense.

NATO's attention to cyber defense dates back at least to 2002, when implementation of a Cyber Defence Programme – "a comprehensive plan to improve the Alliance's ability to defend against cyber attacks by improving NATO's capabilities" – was approved by the North Atlantic Council[16]. This Programme also supports the Prague Capabilities Commitment (June 2002), which identified deployable and secure command, control and communications as one of eight fields for improvement. Further commitments to the Cyber Defence Programme were made in the 2006 Comprehensive Political Guidance and at the 2006 Riga Summit.

The cyber attacks on Estonia in April-May 2007 transformed the scope of NATO cyber defense activities. Prior to then, NATO efforts were primarily concentrated on protecting the communications systems owned and operated by the Alliance. During the DDOS attacks against Estonia, responding to a historic request by a NATO member in defense of its digital assets, NATO members, including the US, provided technical assistance. As a result of the Estonian attacks, NATO has developed more formal guidance for supporting Allied nations if they need to counter cyber attacks. "This implies that NATO has developed mechanisms for assisting those Allies who seek NATO support… including through the dispatch of Rapid Reinforcement Teams" – although, as will be discussed shortly, further work in this area appears to be needed. In parallel, supporting refinements or new initiatives have been made in three areas: NATO cyber defense policy, NATO cyber defense military concept, and measures to accelerate the hardening of NATO's own information systems against cyber attack.

"Practical cooperation on cyber defence" with NATO partners is being developed in accordance with the "Council Guidelines for Cooperation on Cyber Defence with Partners and International Organizations" (August 2008) and the "Framework for Cooperation on Cyber Defence between NATO and Partner Countries" (April 2009). Estonia, Slovakia, Turkey, the UK and the US have signed agreements with NATO to facilitate cooperation in the event of a cyber attack [17].

[NATO is now in the process of updating the NATO Strategic Concept, last revised in 1999.] The language of the Group of Experts' Report informing this process may suggest elements of NATO's new cyber defense posture [18]:

The threat: "The most probable threat to Allies in the coming decade are unconventional….The next significant attack on the Alliance may well come down a fiber optic cable."

The gap: "…there persist serious gaps in NATO's cyber defence capabilities. The Strategic Concept should place a high priority on addressing these vulnerabilities, which are both unacceptable and increasingly dangerous."

The need: "The danger posed by unconventional threats has obvious implications for NATO preparedness, including its definition of security, its strategies for deterrence, its need for military transformation, its ability to make decisions rapidly, and its reliance for help on countries and organizations from outside the Alliance."

The recommendations: "NATO must accelerate efforts to respond to the dangers of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."

The Report recommends that "to guard against these threats [including cyber attacks], which may or may not reach the level of an Article 5 attack, NATO must update its approach to the defense of Alliance territory while also enhancing its ability to prevail in military operations and broader security missions beyond its borders".

The Group of Experts report further specifically recommends five actions:

• Increase the monitoring of NATO's critical network and assess and furnish remedies to any vulnerabilities that are identified.

• The CCDCOE should do more, through training, to help members improve their cyber defense programs.

---

[16] NATO, *"Defending Against Cyber Attacks"*, www.nato.int/cps/en/natolive/topics_49193.htm?selectedLocale=en (accessed 27 September 2010). Unless noted, material in this and following paragraphs is drawn from this report.

[17] NATO Newsroom, *"Interview with NATO Assistant Secretary General for Defence Investment Peter Flory"* 28 March 2008, www.nato.int/cps/en/natolive/opinions_7598.html (accessed 27 September 2010).

[18] NATO, *"NATO 2020: Assured Security, Dynamic Engagement; Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO"*, 17 May 2010, www.nato.int/cps/en/SID=F9F9C7EC-4E74993B/natolive/official_texts_63654.htm?selectedLocale=en (accessed 27 September 2010). Unless noted, material in this and following paragraphs is from this source.

• Allies should expand early warning capabilities in the form of a NATO-wide network of monitoring nodes and networks.

• The Alliance should be prepared to send an expert team to any member experiencing or threatened by a major cyber attack.

• Over time, NATO should plan to mount a fully adequate array of cyber defense capabilities, including passive and active elements (italics added).

These recommendations raise at least two challenging issues for NATO doctrine. Active cyber defense is a somewhat nebulous term of art. While passive defense includes commonly used practices such as firewalls, virus protection and network monitoring – steps taken by any responsible organization – active defense can include practices such as aggressive efforts to trace the source of incoming cyber attacks, or actions to disable the attack source. Active defense as a component of NATO doctrine will require careful definition. Such a definition is made even more challenging given the dynamic technological changes ever-present in the nature of cyber attack and defense.

It is also unclear on what Treaty basis NATO would act in the event of a cyber attack or threat of cyber attack against any member -- Article 4 or Article 5 of the North Atlantic Treaty? [19] The Group of Experts' Report notes that Article 4 consultations are "singularly well-suited to the review of unconventional dangers…". However, "there may well be doubts about whether an unconventional danger – such as a cyber attack… - triggers the collective mechanism of Article 5".

The United States

In the US, since 1998, when Presidential Decision Directive 56 called for a national policy to protect critical infrastructures, particularly cyber-based, defensive postures, cyber security has been the focus of continued government and private sector attention. In 2008, at the beginning of the Obama Administration, a quasi-official report noted that "The United States must treat cybersecurity as one of the most important national security challenges it faces… This is a strategic issue on par with weapons of mass destruction and global jihad." [20]

It is important to note that the US perceives itself as having a greater vulnerability to cyber attack than other nations, for several reasons. The US has a greater dependency on cyber-controlled systems than potential adversary nations. Few nations, and certainly no US adversaries, have more essential national systems in private hands; furthermore, cyber security for critical infrastructures is largely voluntary, and it is unclear how robust these infrastructures would be in the face of a sophisticated disruptive cyber attack. Finally, the US military perceives itself as being highly vulnerable to cyber attack. As noted by Defense Secretary Gates, 'With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DOD's vast information grid…" [21]

US defensive cyber policy is some ways dysfunctional. The two lead government agencies tasked to defend the United States are the DOD, responsible for defending national security systems, and the DHS, responsible for defending, in "public-private partnership", the eighteen designated critical infrastructures as well as other non-national security assets. A White House official, reporting both to the National Security Advisor and to the National Economic Advisor, is responsible for overall policy coordination. Under the 2003 "National Strategy to Secure Cyberspace", US policy has been to eschew regulations or mandates on privately owned critical infrastructures, including telecommunications and most facets of cyberspace, in favor of self-directed plans for protection, information sharing and response.

But beyond efforts to protect themselves against cyber crime, it is unclear how much the private sector is concerned (or should be concerned, on a voluntary basis) in defense against national-level cyber threats. Few, if any, observers regard this system as providing adequate direction or incentive for a national cyber defensive posture, if indeed this is possible. Defense of national security systems, however, has been a longstanding priority of the Defense Department. Use of national security assets to defend civilian cyber space is problematic; while reportedly the Defense Department has considered such a role, the DOD's National Security Agency (NSA), which has primary responsibility for supporting DOD's cyber security duties, is not authorized to assist private sector critical

---

[19] In the 1949 North Atlantic Treaty, Article 4: "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence, or security of any of the Parties is threatened."; Article 5: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed 27 September 2010).

[20] James A. Lewis et al., *"Securing Cyber space for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency"*, Washington, Center for Strategic and International Studies, 2008, 15, http://csis.org/files/media/csis/pubs/081208_securingcyberspace-44.pdf (accessed 27 September 2010).

[21] Secretary of Defense Robert M. Gates, *"Submitted Statement to the Senate Armed Services Committee"*, Washington, US Senate, 27 January, 2009, http://armed-services.senate.gov/statement/2009/January/Gates 01-27-09.pdf, (accessed 27 September 2010).

infrastructure systems directly [22].

More recently, cyber war, and implicitly the concept of cyber power, have received much attention in America. However, US offensive (disruptive cyber attack) policy and doctrine is inchoate at the present. In 2002, National Security Presidential Directive 16 called for a national policy on the rules of engagement for using cyber warfare as a weapon. A 2006 DOD Directive assigned baseline responsibilities for the conduct of 'information operations'. In the 2009 Quadrennial Roles and Mission Review Secretary Gates designated cyber space as one of the four focus areas, a reinforcement of tenets in the 2005 and 2008 National Defense Strategy. A recent commentator notes that the DOD strategy "is to establish the foundation for developing capable cyber forces; structure the forces, as well as their processes and procedures; and then employ these forces to achieve desired effects across the full range of military operations". [23]

The US Cyber Command (USCYBERCOM) is now standing up, with an initial operating capability scheduled for November 2009 now delayed. USCYBERCOM is a subunified command under the US Strategic Command (USSTRATCOM). USSTRATCOM is tasked under the Unified Command Plan to direct the defense of the Global Information Grid and synchronize cyberspace operations. However, a number of observers are critical of the current state of US policy and coordination; as one notes, the US 'has a military Cyber Command but not a cyber war strategy, not a major policy or program to defend the private sector, nothing to initiate international dialogue on cyber war'. [24] A close reading of the news suggests that there are numerous rivalries amomg the DHS, NSA and various other parts of the DOD over who controls what within the domains of cyber security and cyber war, with the US Congress weighing in with various proposed bills now under consideration.

The US is already engaged in bilateral discussions concerning military use of cyber space. Russia supports forging an international treaty banning countries from engaging in cyber war, similar to past chemical warfare negotiations, and has made proposals for such a treaty in the United Nations. The US in turn has advocated improved cooperation among law enforcement agencies, the starting framework for which is already provided by the Council of Europe Cybercrime Convention, which the US has ratified, though many Alliance members have not.

VIII. AN AGENDA FOR THE FUTURE

Concerns about growing security threats in cyber space are valid. These concerns are grounded on the combination of growing national dependence on cyber systems, and the pervasive vulnerabilities in these systems.

Cyber attacks, both passive and disruptive, exploit these vulnerabilities; both criminals and nation states have effectively employed cyber attacks of both types. While some of these attacks have been called examples of cyber war, I believe that the term 'cyber war' is misleading. To draw an analogy from naval thinking, since the writings of Alfred Mahan [25] sea power rather than naval war has been the preferred strategic frame of reference for the projection of state power on the oceans. Like 'naval war', cyber war conjures up legal, policy, military, and diplomatic considerations that inappropriately narrow the scope of relevant issues. Cyber space is better thought of as a new theater for states to exercise cyber power and not just to conduct cyber war. In nuanced ways perhaps not yet seen, cyber power can involve both the projection of state power as well as the creative use of active defenses, all in concert with other military, diplomatic, information and economic tools. The projection of cyber power with both offensive and defensive elements must be a component of national and NATO security doctrine for the future.

The effective exercise of cyber power by NATO presents a number of new issues, including defining when a cyber attack constitutes the use of force, developing a theory of deterrence in cyber space, and clarifying the role of civilians operating cyber systems in a cyber conflict. A special issue for NATO will be to select the appropriate framework for providing assistance to Partners threatened by cyber attack. Should Article 4 be invoked, or Article 5? Furthermore, while NATO has made substantial progress in defining a cyber defense posture, it is clear that serious gaps in capability and doctrine remain. The forthcoming NATO Strategic Concept provides an opportunity for addressing these concerns.

---

[22] Some thought has been given to DOD defense of civilian networks; Ellen Nakashima, "Cyber-Command May Help Protect Civilian Networks," The Washington Post, 5 May, 2009.
[23] Jeffrey Caton,"What Do Senior Leaders Need to Know about Cyberspace?" in *Crosscutting Issues in International Transformation: Interactions and Innovations among People, Organizations, Processes and Technology*, ed. by Derik Neal et al., Washington, National Defense University, December 2009, 207.
[24] Clarke, 118.

In the future, disruptive cyber attacks launched by states will occur. Almost certainly we will see again what has already occurred – cyber attacks against significant civilian, government, and military systems of Alliance members without clear technical attribution of the source of the attacks. The likely attacker will claim plausible deniability. Effective means of defending against prolonged attacks will prove difficult, or an accidental disruptive cyber attack might occur. However, absent non-rational actors, I find it difficult to envision disruptive cyber attacks without kinetic accompaniment in any context other than limited warfare, escalations prior to the outbreak of hostilities, or accidents. An attempt at full-scale cyber war without kinetic attacks does not appear to make sense. While serious, the scope of damage from cyber attack is inherently limited compared with that achievable by conventional means. Over anything more than a short period of time (weeks or months) the effectiveness of cyber attacks likely will decline as alternatives to vulnerable systems are deployed or as cyber systems are hardened and therefore made less vulnerable.

Disruptive cyber attacks by terrorists are possible, even likely, but cyber qua cyber is not a weapon of terror. Cyber attacks could be viewed as a weapon of mass annoyance. Clearly, while cyber threats from non-state actors are not addressed in the same way as attacks from hostile states, the framework of issues shaping NATO doctrine and policy should for the most part be the same.

Given this future, there is need for the NATO alliance to develop a clear doctrine of cyber power, addressing issues of offensive use, defense, response and deterrence. This article has outlined key issues which doctrine must address.

Supporting foreign policy must accompany this doctrine[26]. Specifically, there is a need for an agenda to at least consider the development of bilateral and multilateral frameworks for defining the justification for and form of military action in cyber space, mediation of cyber conflicts and limitations on the exercise of cyber power. Given the complexities and newness of cyber attack as a tool for nations, it is unlikely that a nation seeking UN redress would see rapid action. NATO must be prepared to act.

Proposals for a cyber arms control regime are likely to be part of the future. Russia appears intent on pursuing this agenda. The development of arms control protocols is usually a long and complex process. The key point is that the foreign policy of NATO members should be consistent with the NATO doctrine of cyber power, and mutually supportive across member nations of agreed goals.

NATO doctrine for cyber war and cyber power will continue to evolve – rapid technological change alone ensures that. Cyber space represents a new environment for the projection of power –cyber power – and NATO needs to address this challenge on an on-going and committed basis.

[25] Alfred Thayer Mahan, *The Influence of Sea Power Upon History 1660-1783*, Twelfth Edition, Boston, Little, Brown and Company, 1890.
[26] Jeffrey Hunker,"U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away", *Journal of National Security Law and Policy 4*, No. 1, 2010. http:// jnslp.com (accessed 27 September 2010).