

An OpenSource Research and Analysis On

CYBER WEAPONS PROLIFERATION AND DETERRENCE

By: Angel T. Redoble,
Senior Consultant, Indra Sistemas, Spain
Associate Director, International Society of Cyber Security Professionals
Masters in Information Security Management, Certified Ethical Hacker, Computer Hacking
Forensic Investigator, ISMS Lead Auditor

The internet which is also referred to as the cyber space has evolved from a means to communicate for personal and business purposes to a dimension to commit crimes, cyber espionage and cyber war. The same security audit tools used by external and internal organization security auditors are now branded as cyber weapons and being used to; attack critical infrastructures, commit financial fraud, conduct cyber espionage, steal sensitive and confidential information, vandalism, propagate global jihad and disrupt services that is provided by private and public organizations to the consumers.

Considering the recent surveys and studies conducted by different entities, the number and financial impacts of cyber attacks have increased at a rate faster than ever even though cyber security measures are improving and getting more sophisticated. This could only mean one thing, that the people behind these attacks are always one step ahead of those who develop cyber security measures. The imminent danger such as cyber terrorists, hostile nations, and others will launch attacks that could possibly cause catastrophic damage, potentially leading to loss of life or widespread economic failure have been the basis as to why there is a need to implement an effective control on the proliferation of cyber weapons, and address the broader issue of cyber warfare.

There is no middle ground in cyber warfare; you can either be a victim or a pawn to be used as an attack point to attack other nations or infrastructures to hide the identity and source of the attacker. These things make it all the more important for all nations to address cyber threats from an international perspective down to the national level.

Developing cyber weapons are far cheaper than developing nuclear weapons, it is therefore perceived that terrorists, criminal organizations and hostile nations could freely and easily develop these weapons anytime and anywhere or acquire them at a very cheap cost. In the presentation provided by Mr. Kevin Coleman of Technolytics entitled "Preparing for eDay" it mentioned that between the year 2006 and 2007 there was a substantial increase in the number of countries pursuing cyber weapons and that in 2008 there are over 140 countries with cyber weapons program. Among these nations are China, Iran, Pakistan, India, Russia, Japan and North Korea.

The complexity of cyber weapons and cyber warfare issues makes it more difficult as to how to control the development of cyber weapons and at the same time deter cyber security threats. The challenge now is whether an international cyber weapons control might diminish the criminal and national security threats, while promoting greater cyber peace. Such a control might pertain to the development, distribution, and deployment of cyber weapons, or it might apply only to their use. It might relate primarily to criminal law, or it might govern the conduct of nation states in the domain of international law.

This information and technology-dependent world provides opportunities for spectacular gains and serious losses for individuals, corporations, and states. It is within this cyber world that the state-sponsored hackers and cyber-terrorist will operate. In the same manner that terrorists and enemy states have exploited widely accepted traditional warfare technology such as bombs, airplane hijacking and traditional espionage, they may exploit as well the tools of the cyber era for a country to obtain supremacy over their adversary, and for the terrorist to bring their case before the citizens of the world. The world must prepare itself to counter this threat in an age of a new and borderless warfare, the cyber warfare age. To defend against a cyber threat, one must understand its critical elements and the anatomy of cyber attacks. Cyber warfare, like a conventional warfare, will strive to cripple the capabilities of an enemy nation to survive by successfully attacking its critical infrastructures and bring down its economic superiority. However, cyber warfare may utilize a different means to this end. A cyber warrior will strive, not to disrupt physical reality directly (as an exploding bomb would) but rather to disrupt the normal functioning of technologies and other information systems to prevent all vital services. This cyberspace disruption would cause a disruption in the physical world. The violence that is normally associated with traditional warfare may shift into cyberspace where bits and bytes, not people, are attacked.

All these threats have one common denominator, the unrestricted and cheap cost in the proliferation of cyber weapons. Any individual or group with malicious intent can download or develop cyber weapons and use it without the fear of getting caught as it is very difficult to identify and trace the source of a cyber attack. A rogue nation can conduct cyber espionage against an adversary by just sitting on his chair located somewhere else using a laptop. A terrorist can propagate his agenda as well as provide attack strategies and targets globally without having the trouble and the risk of exposing himself physically to the real world. A cyber war may be launched against any country without the possibility of identifying the true source of the attack as well as the real intent of the attacker and still provide the same catastrophic outcome as a traditional warfare would. The cyber space with the existing cyber weapons provide a perfect environment for terrorists, criminals and state-sponsored attackers to easily and rapidly execute malicious activities and stay anonymous at the same time.

As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk. Hackers can steal information, issue phony commands to information systems to cause them to malfunction, and inject phony information to lead men and machines to reach false conclusions and make bad (or no) decisions.

This document will try to analyze and layout the challenges for implementing a cyber weapons control and will assess whether the traditional methods of deterrence used against traditional warfare weapons would be sufficient enough to deter the proliferation and acquisition of cyber weapons. This document will address cyber attacks and the cyber weapons used in those attacks. These cyber weapons or hacking tools include software and methods for sabotaging systems, stealing confidential state information, causing public panic and chaos, international and local financial fraud and for launching computer viruses, worms, and denial-of-service attacks.

The focus on cyber security is growing all over the world. Nations are now seriously considering cyber security threat as a national security issue. A threat that if realized could possibly affect a nation's very reason of existence. A threat that could easily be exploited by cyber criminals, cyber terrorists and rogue nations who are continuously seeking to take down another nation that is considered to be an adversary. Recent events of cyber espionage, cyber terrorism and state-sponsored cyber attacks have forced concerned nations together with the United Nations to come up a strategy to deter these persistent and growing cyber threats. Military officials from 1st world countries insisted time and again that cyber security threats

have the same catastrophic outcome as those of traditional warfare threats and therefore must be integrated to military operations. Some nations have started developing cyber warfare programs to protect their cyberspace and to be able to launch a counter cyber attack if possible.

In 2007, Estonia experienced a cyber attack that targeted government, media, and economic systems. The attack was insidious, rapid, and difficult to trace, and it denied service to information users for three weeks. The incident in Estonia signaled a change in the international security environment for cyberspace. Cyber infiltrators routinely attempt to penetrate Department of Defense, government, economic, and industrial networks to gain access to information that could be vital for activities in each of these arenas. The advantages that such adversaries gain through cyberspace afford them the ability to pose serious, if not fatal, threats to a nation's national security.

China who is perceived to be having a state-sponsored hacking group designed to infiltrate networks and systems of other countries to obtain confidential information has always denied such accusations, ignoring the numerous and reliable existence of such hacking group as well as incidents that are directly connected to them. These proves the difficulty to positively identify the perpetrators as it is possible to attack an infrastructure of one nation using the network of another nation thus providing the attacker a very strong means of anonymity.

When the world started moving into cyber age many years ago, information, technology, communication and its control are rapidly becoming the most important considerations for the advancing societies of the world, we have seen a corresponding shift by terrorists, criminals and rogue nations to using cyber warfare weapons and techniques to advance their cause, and we have seen the effects brought by cyber attacks perpetrated by common criminals to state-sponsored hacking activities.

The possibility of an all out cyber war prompted the United Nations to draft a document in 2009 that creates a framework of International cooperation and support for investigation acts of cyber aggression. The ink has not dried on the rules of cyber engagement and response. The rules of engagement are in their infancy, unclear and differ significantly country to country. However it still remains unclear what acts of cyber aggression exactly constitutes an act of cyber war.

The development of cyber weapons requires little infrastructure, information that is readily available, and technical skills that are common. These factors combine to make the identification and detection of cyber weapons development efforts extremely difficult, thus making deterrence efforts relatively complex and easier said than done.

- The only difference between cyber weapons and security testing tools is the intent of those behind their development and use.
- Many fear that any action to control the proliferation of cyber weapons will be the first step in a series of controls put in place by governments to clamp down on the freedom of expressions the Internet was founded on and known for.
- The continued escalation of acts of cyber aggression has military and government leaders concerned that an all out cyber war could be a reality.
- Chinese strategists have warned, "There is no means which cannot be used in war and there is no territory or method which cannot be used in combination."
- During the first week of general conflict in Iraq back in 2003, over 20,000 web site attacks were recorded on pro- and anti-Iraqi war sites.

- The current asymmetric threats we face requires a uncommon interaction between the military, the government and the private sector business and technology communities.
- The United States has come under attack from computers and computer networks situated in China and Russia (Titan Rain and Moonlight Maze)
- In Kosovo back in 1999, Yugoslav President Slobodan Milosevic organized a systematic “ping bombardment” of the NATO server that went on for nearly two weeks.
- On August 14 2003, the US Eastern grid massive blackout affected millions of Americans in eight states as well as millions of Canadians.
- In 2007, the United States government suffered an "an espionage Pearl Harbor" in which an "unknown foreign power...broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information.
- On May 17, 2007 Estonia came under cyber attack. The Estonian parliament, ministries, banks, and media were targeted. The attackers went after their financial systems
- On 14 December 2007 the website of the Kyrgyz Central Election Commission was defaced during its election. The message left on the website read "This site has been hacked by Dream of Estonian organization". During the election campaigns and riots preceding the election, there were cases of Denial-of-service attacks against the Kyrgyz ISPs.
- In Myanmar, on September 23, 2008, in anticipation of the first anniversary of the Saffron Uprising, The government launched DDoS attacks against three websites that support the monks: The Irrawaddy, the Oslo-based Democratic Voice of Burma (DVB), and the New Era in Bangkok.
- Georgian and Azerbaijani sites were attacked by hackers during the 2008 South Ossetia War, for the first time coupling a kinetic and a cyber attack prior to a military invasion.
- On the July 4, 2009, weekend and continuing into the following week, a DDoS attack took down U.S. and South Korean government and commercial websites for indeterminate periods of time. The South Koreans believed the government of the Democratic People’s Republic of Korea (DPRK) or its agent as responsible, whereas no formal opinion as to attribution was expressed by any U.S. officials.
- In June 2009, the president of Tatarstan’s website was knocked offline and Internet access was lost in an attack that he attributes to the Russian Federal Security Service (FSB).
- On January 18, 2009, a DDoS attack shuttered two to three of Kyrgyzstan’s four ISPs for several days, denying Internet access to most of the population during a time of growing political unrest.
- On March 28, 2009, a cyber spy network, dubbed GhostNet, using servers mainly based in China has tapped into classified documents from government and private organizations in 103 countries, including the computers of Tibetan exiles, but China denies the claim.
- In July 2009, there were a series of coordinated cyber attacks against major government, news media, and financial websites in South Korea and the United States.

- In December 2009, a cyber attack, dubbed Operation Aurora, was launched from China against Google and over 20 other companies.

Nations face a multitude of threats in cyber space. One such threat is that of malicious code being embedded in firmware of computer or application software from foreign suppliers. This is a threat that is perceived to be so hard to detect. To ensure that a certain software or hardware acquired from different suppliers developed by any nation do not contain an embedded code or chip that can be activated anytime would be a huge challenge for everyone. These cyber weapons are often available for download from the internet; some are free while some are not.

Among the countries perceived and reported to be developing cyber warfare capabilities is China. In the report entitled **“Report on the Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation”** provided by NorthropGrumman, it mentioned:

*“The government of the People’s Republic of China (PRC) is a decade into a sweeping military modernization program that has fundamentally transformed its ability to fight high tech wars. The Chinese military, using increasingly networked forces capable of communicating across service arms and among all echelons of command, is pushing beyond its traditional missions focused on Taiwan and toward a more regional defense posture. This modernization effort, known as **informationization**, is guided by the doctrine of fighting **“Local War Under Informationized Conditions,”** which refers to the PLA’s ongoing effort to develop a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum.”*

*The Chinese have adopted a formal IW strategy called **“Integrated Network Electronic Warfare” (INEW)** that consolidates the offensive mission for both computer network attack (CNA) and EW under PLA General Staff Department’s (GSD) 4th Department (Electronic Countermeasures) while the computer network defense (CND) and intelligence gathering responsibilities likely belong to the GSD 3rd Department (Signals Intelligence), and possibly a variety of the PLA’s specialized IW militia units.*

The PLA is training and equipping its force to use a variety of IW tools for intelligence gathering and to establish information dominance over its adversaries during a conflict. PLA campaign doctrine identifies the early establishment of information dominance over an enemy as one of the highest operational priorities in a conflict; INEW appears designed to support this objective.

Below are some of the widely known threats and weapons in cyber security:

Advanced Persistent Threat Attacks (APT)

The APT attack is targeted and persistent and the approach often follows the common methodology & anatomy of attack. However, a major difference resides in the concept of time. The initial inability to backtrack the attack has been the continuous point of contention. In addition the ROI is not a major concern and attackers approach is stick and move on if the victim is well defended. Time is on their side and it must be conveyed that they will be back.

The intruders responsible for the APT attacks target the Defense Industrial Base (DIB), financial industry, manufacturing industry, and research industry. The main differentiator is the APT intruder’s perseverance and resources. They have malicious code (malware) that circumvents common safeguards such as anti-virus and they tend to generate more activity than wanton “drive by hacks” on the Internet. The intruders also escalate their tools and techniques as a victim firm’s capability to respond improves.

Computer Virus Attacks (CVA)

A virus is a harmful software program that is secretly introduced into a system with the characteristic feature of being able to generate and distribute multiple copies of it, and thereby spread throughout the computer system. Each virus has a destructive payload that is activated under certain conditions. When activated a virus can corrupt, alter, or destroy data, generate bogus transactions, and even transfer information.

Distributed Denial of Service Attacks (DDoS)

DDoS attack is launched from as many remote computer systems as a hacker can compromise. When DDoS are launched, the attacks are hard to stop because the data flood originates from many computers from multiple locations. Typically, systems managers are unaware that their machines are attacking other systems. In this type of attack, websites are suddenly overloaded with traffic (sometimes tens of thousands of bogus hits), jamming and disabling websites by overloading the bandwidth of the site or processing capabilities of the servers running the sites. These attacks can and often are launched from computers that have been compromised all over the world.

Cyber Espionage

Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.

Directed Energy Weapons (DEWs)

This class of cyber weapon is capable of disabling enemy computer systems without the use of explosives. DEWs include high energy microwaves (HEWs), high power microwave (HPWs) and transient electromagnetic devices (TEDs). This class of weapons operates by using pulses or beams of electromagnetic energy to disrupt or destroy electronic components in a computer, missile, tank, or any smart weapons that has not been properly hardened against this type attack.

In the report provided by the Institute for Security Technology Studies entitled “Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States”, it provided a realistic assessment of the capabilities, means, and motivations of selected nation-states to conduct a remote, computer-to-computer attack either against the United States or against regional adversaries. The report took as a given that there is no such thing as “perfect” IT security. For example, hackers seem always able to keep one step ahead of the latest software security patch, and some secure portions of the U.S. Department of Defense computer systems (pertaining to procurement and logistics) are connected to the public-switched network. The consequences of an attack “through the wires,” and the degree of potential disruption, will often hinge on the pervasiveness (and therefore importance) of the network impaired by the attack: national versus regional, local, or municipal in scope.

China

Within the framework of an integrated national plan, the People’s Liberation Army (PLA) has formulated an official cyber warfare doctrine, implemented appropriate training for its officers, and conducted cyber warfare simulations and military exercises. Beijing’s intelligence services continue to collect science and technology information to support the government’s goals, while Chinese industry gives priority to domestically manufactured products to meet its technology needs. The PLA maintains close ties with

its Russian counterpart, but there is significant evidence that Beijing seeks to develop its own unique model for waging cyber warfare.

India

Cyber attacks pose more than a theoretical challenge to the Indian government's day-to-day national security agenda due to the intrusions and web defacements experienced after New Delhi's nuclear weapons test and in the confrontation with Pakistan over Kashmir. The Indian authorities announced a shift in military doctrine in 1998 to embrace electronic warfare and information operations. An IT roadmap, enumerating a comprehensive ten year plan, was published. In the framework of the roadmap, the government has granted permission for closer government/industry cooperation to leverage the output of India's world-class IT software industry. In addition, a new National Defense University and Defense Intelligence Agency (DIA) have been established. According to journalistic accounts, the armed forces plan to establish an information warfare agency within the DIA with responsibility for cyber war, psychological operations, and electromagnetic and sound wave technologies.

Iran

U.S. national security experts have included Iran on a published list of countries said to be training elements of the population in cyber warfare. The leadership in Tehran is known to sponsor terrorist groups and for many years has chafed in the face of perceived Iranian inadequacy in the conduct of modern information warfare. Although the rhetoric of the clerical regime has been more prudent in recent years (at least until recently), the government nevertheless continues to accord economic and political priority to extending the technological threshold of its defense sector. This is illustrated in two ways: first, the armed forces and technical universities have joined in an effort to create independent cyber R & D centers and train personnel in IT skills; and second, Tehran actively seeks to buy IT and military related technical assistance and training from both Russia and India. Overall, we assess that Iran is leveraging its resources in the non-conventional weapons and IT sector as a "force multiplier" to gain greater influence in Central Asia.

North Korea

Although U.S. national security officials include North Korea on a published list of countries believed to be developing information warfare units either in the military or the intelligence services, the open literature contains no North Korean military doctrinal or policy statement to that effect. South Korea's defense community alleges cyber reconnaissance or network hacks sponsored by Pyongyang, but such charges may only represent "disinformation." Due to the closed, Stalinist make-up of the North Korean regime and society, concrete evidence is difficult to obtain. There are few credible first-hand sources. We believe it is possible North Korea is experimenting with offensive cyber attack capabilities, based on Pyongyang's track record of priority resource allocations to the military, its evident endowment of scientists and engineers, and its documented achievements in missile and related military technologies.

Pakistan

Well-documented hacker activity in Pakistan and possible ties between the hacker community and Pakistani intelligence services indicate that Pakistan appears to possess a cyber attack capability. However, the published evidence is lacking concerning the exact nature of the capability; it is quite possible that the government of Pakistan has made only a minimal investment in its cyber warfare program. The available evidence

suggests that the main target of Pakistan's offensive capability is India—Islamabad's rival on the sub-Continent and adversary in the Kashmir dispute. Pakistan's developed IT industry, well-educated computer programmers, and supportive government that is concerned with security in Kashmir and parity with India provides circumstantial evidence suggesting a cyber warfare program.

Russia

Russia's armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia's cyber warfare doctrine have disclosed discussions and debates concerning Moscow's official policy. "Information weaponry," i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine. Moscow also has a track record of offensive hacking into Chechen websites. Although we assess it likely that Moscow will continue to scout U.S. military and private sector networks and websites, available evidence is inadequate to predict whether Russia's intelligence services or armed forces would attack U.S. networks, especially after taking into account present-day political and economic ties between the two nations.

Considering the traditional methods of deterrence applied to nuclear weapons and other weapons of mass destruction, they may not be as effective when applied to cyber deterrence. The success of these methods on the field of deterring national security threats on the traditional warfare will have very little impact on the growing proliferation of cyber weapons and the arena of cyber warfare. The ambiguities of cyber deterrence contrast with the clarities of nuclear deterrence. In the Cold War nuclear realm, attribution of attack was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first; counterforce was possible; there were no third parties to worry about; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose. Although the threat of retaliation may dissuade cyber attackers, the difficulties and risks suggest the perils of making threats to respond, at least in kind. Indeed, an explicit deterrence posture that encounters a cyber attack with obvious effect but non-obvious source creates a painful dilemma: respond and maybe get it wrong, or refrain and see other deterrence postures lose credibility. The case for cyber deterrence generally rests on the assumption that cyber attacks are cheap and that cyber defense is expensive. If cyber attacks can be conducted with impunity, the attacker has little reason to stop. Besides, nuclear deterrence prevented the outbreak of nuclear conflict during the Cold War. What is there about cyberspace that would prevent a similar posture from working similarly well?

In the report published by RAND Corporations entitled "Project Air Force", it laid out the very important questions that simply do not crop up with nuclear or even conventional deterrence matter in cyberspace whenever the target of an attack contemplates retaliation:

Will we know who did it? Cyber attacks can be launched from literally anywhere, including cybercafés, open Wi-Fi nodes, and suborned third-party computers. They do not require expensive or rare machinery. They leave next to no unique physical trace. Thus, attribution is often guesswork. True, ironclad attribution is not necessary for deterrence as long as attackers can be persuaded that their actions may provoke retaliation. Yet some proof may be necessary given: (1) that the attacker may believe it can shake the retaliator's belief that it got attribution right by doing nothing different ("who, me?") in response to retaliation, (2) that mistaken attribution makes new enemies, and (3) that neutral observers may need to be convinced that retaliation is not aggression.

Can retaliators hold assets at risk? It is possible to understand the target's architecture and test attack software in vivo and still not know how the target will respond under attack. Systems vary by the microsecond. Undiscovered system processes may detect and override errant operations or alert human operators. How long a system malfunctions (and thus how costly the attack is) will depend on how well its administrators understand what went wrong and can respond to the problem. Furthermore, there is no guarantee that attackers in cyberspace will have assets that can be put at risk through cyberspace.

Can they do so repeatedly? It is difficult to imagine an act of cyber retaliation that is prospectively so awesome that no potential attacker would run the risk of being hit (a crucial feature of nuclear retaliation). Repeated application may be necessary but is not necessarily possible. Even successful retaliation may not be convincing if the attacker tells itself it will be less vulnerable the next time around.

Can cyber attacks disarm cyber attackers? In a world of cheap computing, ubiquitous networking, and hackers who could be anywhere, the answer is no.

Will third parties stay out of the way? Cyber attack tools are widely available. If non-state actors jump into such confrontations, they could complicate attribution or determining whether retaliation made the original attackers back off.

Might retaliation send the wrong message? Most of the critical U.S. infrastructure is private. An explicit deterrence policy may frame cyber attacks as acts of war, which would indemnify infrastructure owners from third-party liability, thereby reducing their incentive to invest in cyber security.

Can states set thresholds for response? Unless a state declares that all cyber attacks, no matter how minor, merit retaliation, it needs to define an actionable threshold. Proving that any one attack crossed it, however, may be tricky.

Can escalation be avoided? Even if retaliation is in kind, counter retaliation may not be. A fight that begins in cyberspace may spill over into the real world with grievous consequences.

On January 30, 2010 in Davos, Switzerland, International Telecommunications Union Secretary General Hamadoun Toure warned the world needs a treaty to prevent cyber attacks becoming an all out war. He went on saying that the risk of cyber conflict between two nations is growing every year. And that the outcome would be worse than a tsunami, it would be catastrophic.

In 2001, Dorothy Denning of Georgetown University wrote a document entitled "Obstacles and Options in Cyber Arms Control". The document addresses obstacles and options for implementing a cyber arms control treaty and it is concerned mainly with computer network attacks and the cyber weapons ("hacking" tools and methods) deployed in those attacks. She arrived to a conclusion that a treaty that pertains to criminal law and law enforcement is preferable to one that pertains to the conduct of nation states under international law, in particular the law of war. A secondary conclusion is that controls should apply mainly to the use of cyber weapons to commit illegal acts. The production, distribution, and possession of cyber weapons should not be controlled except when the intent is to use the weapons to commit crimes. Although this document and the arguments presented can be considered old with regards to its date of publication, but the content pertaining to the obstacles in implementing cyber control is still very valid until now. The following are the presented obstacles and the reason why it would be very difficult to implement in an effective manner a control on the proliferation of cyber weapons and thus makes it more difficult to deter cyber security threats,

especially if the basis of such control is focused on the existing traditional methods of deterrence applied on nuclear weapons and other weapons of mass destruction:

Enforceability

Many attacks are never detected in the first place. When they are, finding the perpetrator is seldom easy, especially when the person has looped through numerous computers in different countries. An attack against computers in one country, for example, might appear to originate from government computers in another, all the while being perpetrated by teenage hackers in a third country who had gained control over the computers. Further, many countries do not have adequate cyber crime laws, making it difficult or impossible to prosecute persons in those countries who commit acts that are illegal in their victim's county. Even if their laws are good, their investigative capability may be inadequate, or they may not agree to cooperate in an international investigation.

A cyber arms control treaty could alleviate many of these problems by promoting greater harmony of national crime laws and greater cooperation among international law enforcement agencies. Enforcement would still be nontrivial, however, as it only takes a few non-compliant countries to complicate an investigation. Further, enforcement would be problematic as it relates to the actions of sovereign states, as it can be hard to know if an attack originated from a state or non-state actor. The United States government has yet to determine who is responsible for the ongoing Moonlight Maze intrusions into Department of Defense computers other than that they are coming out of Russia.

Currently, most crime laws do not prohibit the production, distribution, or possession of cyber weapons, at least when the tools are not used in conjunction with a crime. Given that many treaties and laws restrict these activities as they pertain to certain physical weapons, particularly chemical, biological, and nuclear weapons, it is reasonable to consider whether a cyber arms control treaty should extend such restrictions to cyber weapons.

Moreover, once produced, cyber weapons are easily copied and distributed on the Internet through electronic mail, websites, instant messaging, peer-to-peer sharing systems, and other mechanisms. Unlike many physical weapons, software weapons can be transmitted and stored without posing any physical danger to the parties involved. Thousands of copies can be produced and transmitted to other locations at virtually no cost.

Monitoring for treaty compliance would also be hard given the rapid changes in technology and in methods and tools of attack. New computer viruses, worms, Trojan horses, denial-of-service programs, exploit scripts, and other types of cyber weapons are continually being developed.

There are tools for detecting the presence of some cyber weapons, but they are not perfect, and cyber weapons often evolve in ways that foil detectors. Most anti-viral tools, for example, scan mainly for known viruses. Further, the presence and distribution of cyber weapons can be concealed with the use of encryption, anonymity, and other information hiding tools and methods.

Verification and monitoring for compliance would also require a level of intrusion that few if any people would find acceptable. It would be impossible to know if a government agency, for example, had access to prohibited cyber weapons without scanning all computers and storage devices owned by the agency, including all classified systems. No agency would agree to this. Scanning the personal computers of

citizens likewise would be unacceptable, as it would violate human rights (see also the section on privacy). The best that could be achieved would be to scan the public spaces of network servers for certain hacking tools. This might help keep the tools from some, but it would not keep them from determined individuals, who could swap them through private channels. Nor would it keep them from governments, who could develop them on their own.

Another issue is that even if the presence of a controlled cyber weapon is detected, it would be impossible to find and eliminate all copies, which might be stored on thousands of computers all over the world. Some of these servers could be located in places that are not party to a cyber arms control treaty or that operate safe havens, for example, the offshore Sealand platform, which is said to be the world's smallest sovereign territory. Hacking tools can be published through systems such as Publius that use encryption and distributed storage techniques to create an environment that is highly resistant to censorship.

Security

There is another argument against enacting cyber arms controls that prohibit the production and distribution of attack tools. Such controls would curtail research and publication in the area of computer security. It is not possible to build strong defenses without knowing what attacks are possible and what vulnerabilities might be exploited, so investigating methods and tools of attack is an important element of cyber security.

Indeed, it is frequently argued that “full disclosure,” which includes publishing information about system vulnerabilities and the tools that exploit them, contributes to security by making the information available to everyone and not just “the bad guys.” Researchers can build on each other’s work, thereby accelerating progress in information security. Further, it is argued, publication pushes the vendors to fix security flaws. While the merits of full disclosure, particularly the publication of the actual tools of attack, are debatable, it must be recognized that it is not just malicious hackers who support the concept.

System administrators and security consultants would also object if the controls prohibited them from using hacking tools to test their own systems or the systems of their clients for vulnerabilities. It is common to use many of the same types of tools used by hackers for this purpose, for example, scanners, password crackers, sniffers, and network monitoring tools. The difference lies in whether the tools are used for attack or defense.

Hacking tools are also used for “active defense,” that is, launching some sort of operation against the perpetrator to trace their location or abort their attack. Governments especially might object if they could not use hacking tools to adversaries that disable or penetrate systems and threaten national security.

Privacy

To investigate crimes in cyberspace, law enforcement agencies need the capability to search and seize digital evidence and to intercept network communications. To facilitate these operations, they have asked for hardware and software tools and, in some cases, additional legal authorities. In the United States, for example, the FBI developed Carnivore, now called DCS1000, to support court-authorized Internet wiretaps. When installed at a subject’s Internet Service Provider, DCS1000 intercepts particular message traffic belonging to the subject, for example, all e-mail messages sent to or from the subject, as specified in the court order. In the United Kingdom, the Regulation

of Investigatory Powers (RIP) bill has provisions that facilitate government monitoring of Internet traffic and provide access to encryption keys.⁴

These law enforcement advances have raised privacy concerns. Opponents of Carnivore argue that the tool could be misused in order to conduct mass surveillance or otherwise acquire evidence that was not legally permitted, although no evidence of abuse was put forth. Opponents of RIP argue that the ability of the government to demand encryption keys sets a dangerous precedent. My understanding, however, is that the British government cannot compel keys from parties who claim to have lost or forgotten them.

If a cyber arms control treaty prohibited certain cyber weapons, the process of policing the Internet for these weapons would raise additional privacy issues. Scanning the personal computers of citizens would violate the privacy laws of many nations.

Free Speech

Restrictions on cyber weapons, particularly source code and scripts, would raise significant legal issues in countries with laws protecting speech. In the United States, speech is protected under the First Amendment, and software is considered to be a type of speech. Not all forms of speech are given full legal protection, however. Defamatory speech, death threats, and child pornography, are examples.

In the domain of software, the Digital Millennium Copyright Act restricts the production, distribution, and use of software that circumvents copyright protection. The rationale is that such software harms copyright owners.

Treating cyber weapons in the form of software differently from more general information about cyber weapons is also problematic. For example, a programmer can translate a mathematical or English-language description of an algorithm into a working program. Should the program be restricted but not the description? Further, source code can be embedded in prose or poetry, as illustrated by a version of the DeCSS, with commentary, in haiku form. Professor David Touretzky of Carnegie Mellon University has over two dozen different versions of the DeCSS on his website, including the haiku version and a “dramatic reading” of the code. It would be extraordinarily difficult to draw a line between what could be published and what could not.

Corporate Responsibilities and Liabilities

A cyber arms control treaty could have a substantial impact on industry. Industry might be required to implement costly mechanisms to control the use or spread of cyber weapons or to investigate violations of arms control. They might also be held liable for actions taken on their network in violation of laws stemming from the treaty.

Companies, particularly service providers, are also concerned about being burdened with subpoenas and court orders originating in foreign countries. Many companies already spend considerable resources responding to requests relating to crimes in their own countries.

Foreign Policy

It will be impossible to establish meaningful cyber arms controls if nation states are opposed. In October 1998, Russia introduced and then tabled a resolution in the First Committee of the United Nations that attempted to get the United Nations to address the subject of arms controls with respect to information warfare. The resolution called for states to report their views regarding the “advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons.”

In November, the U.N. General Assembly adopted a revised resolution calling only for views and assessments regarding “(a) general appreciation of the issues of information security; (b) definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources; and (c) advisability of developing international principles that would enhance the security of global information and telecommunications and help combat information terrorism and criminality.” Mention of information weapons was removed. Russia offered another resolution in 1999. It met a similar fate.

Information warfare covers a much broader range of activity than computer network attacks, however. It also includes psychological operations and perception management, deception, electronic warfare, and intelligence collection. Many of these operations are used by governments during peacetime as well as during conflicts. It is, therefore, not surprising that any attempt to impose international restrictions on information warfare would meet with resistance.

In conclusion, given the arguments presented by various parties in different forums and levels, it is therefore very difficult to control the proliferation of cyber weapons using the existing traditional methods of deterrence, namely; Economic or trade sanctions, import export restrictions, Penalties and threat of retaliation. While these methods are not totally negligible, it will only have very little effect on the matter at hand. The skills required to develop cyber weapons is not as complicated and scarce compared to developing nuclear weapons or any WMD for that matter, not to mention the difficulty in determining the real intent of the person, the company or the country who are into developing these weapons, and given the fact that these so called cyber weapons are the same tools used to conduct penetration testing or ethical hacking projects to government agencies and private corporations. However deterring cyber threats is not as difficult as proliferation of cyber weapons. Deterrence can be effectively achieved on the national level or on the capacity of every Nation State.

While formulating a policy in relation to cyber space and threats on the international level would be helpful to lower down the possibility of an all out cyber warfare, the best approach would still rely on every nation state’s initiative. The current “Law On Armed Conflict” or LOAC does not provide nor include provisions on cyber warfare. Based on the legal lessons identified and learned from the past cyber attacks(Estonia 2007, Lithuania 2008, Georgia 2008), it seems that a contemporary “Eastern European” way of cyber-attacking a country is to use the “gray area” in law that does not invoke LOAC. Mostly, the perpetrators operate in a domain that triggers application of relevant provisions in criminal law, which is poorly developed in many countries and has an unsolid ground for cross-border cooperation. In the document released on November 2008 by Cooperative Cyber Defense Center of Excellence or CCDCE, it mentioned that it will take time to reach additional consensus on cyber defense legal aspects on the international level and that ratification of cyber crime convention even by all EU or NATO nations does not solve the practical problems related to cyber attacks. Those countries that have witnessed and experienced cyber attacks, have also recognized that there are significant restrictions as regards the applicability and usefulness of cyber crime provisions to such attacks; often the provisions are incomplete, the punishments are weak or the investigatory powers are insufficient.

In order to provide an effective legal remedy in cyber security, traditional LOAC principles must be developed to address the rapidly growing cyber attacks against nation states. It has been suggested that the Geneva Convention must be reviewed and must include in its definition the term Cyber warfare and what constitutes a cyber war. And that the new bloodless types of warfare make estimating the level of suffering difficult and the definition of an “attack” should not be strictly connected with established meanings of death, injury, damage and destruction.

Instead the definition of an attack should be consequence-based and bear in mind the final effect on the population. However, as current LOAC legislation is hardly applicable to cyber attacks scenarios, the best option to protect the cyber space of one nation still relies on the national level and its determination to implement a robust cyber security program on its own capacity. The complexity to formulate and implement international and criminal law usually results to the unwillingness of nation states to cooperate, and thus results to failure.

A strong relationship, cooperation and coordination between all government agencies together with the private sector would be a key factor in the success of deterring cyber threats. Cyber war cannot be won by merely calling in the military. While integrating cyber security issues to the military doctrine is a good idea, as well as formulating cooperation and coordination strategy internationally, the involvement of the private sector is still an integral part to effectively defend ones cyber space. Cyber attack targets do not involve military installations alone but also networks owned by private entities (small, medium, large) as well as individual and personal internet users. Compromising the private sector's network infrastructure could provide a catastrophic effect on a nation's capability to function economically and socially.

As what Admiral James G. Stavridis, the NATO's Supreme Allied Commander Europe (SACEUR) said in his statement at **Network Centric Warfare Europe 2010 Conference**, and I quote

“Our reliance on the global information grid as a distribution network for critical decision-making information creates a double-edged sword. On one hand, increased usage of electronic networks shortens the decision-making cycle and increases our technical means for critical analysis of complex systems and circumstances; on the other hand, heavy reliance on networks for information distribution and storage creates new and different vulnerabilities which require us to secure our networks and potentially delay our OODA (Observe, Orient, Decide and Act) loop. The challenge, therefore, is to strike the proper balance between authorized access to networks and denial of access to unauthorized personnel and entities.”