A FRAMEWORK FOR THINKING ABOUT CYBER CONFLICT AND CYBER DETERRENCE, WITH POSSIBLE DECLARATORY POLICIES FOR THESE DOMAINS

Stephen J. Lukasik

Center for International Strategy, Technology, and Policy
The Sam Nunn School of International Affairs
Georgia Institute of Technology, Atlanta, Georgia

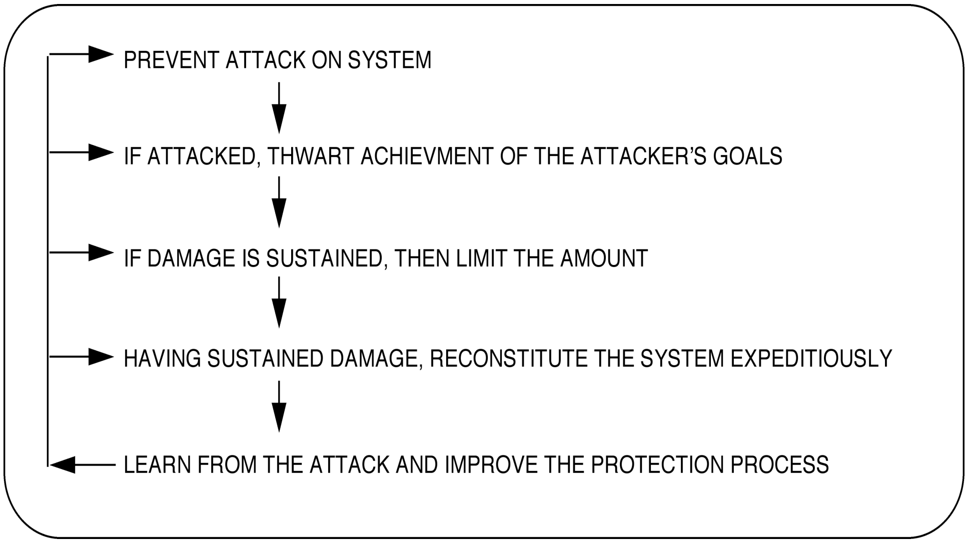
July 22, 2010

OUTLINE

A. Deterring Cyber Attacks

THE ROLE OF DETERRENCE IN DEFENSE AGAINST CYBER ATTACKS

Defending against attacks includes actions during three periods. The pre-attack period is perhaps the most important, for it is here that deterrence can be effective. The trans-attack period is one where actions can be taken to thwart an attacker, assuming one has real-time systems for sensing events and undertaking responses. The post-attack period is one of reconstitution and learning from the attack to improve the protection process to forestall or blunt future attacks. Schematically:


PREVENT ATTACK ON SYSTEM
IF ATTACKED, THWART ACHIEVMENT OF THE ATTACKER'S GOALS
IF DAMAGE IS SUSTAINED, THEN LIMIT THE AMOUNT
HAVING SUSTAINED DAMAGE, RECONSTITUTE THE SYSTEM EXPEDITIOUSLY
LEARN FROM THE ATTACK AND IMPROVE THE PROTECTION PROCESS

The first line describes the pre-attack period; the next two describe the trans-attack period; and the last two describe the post-attack period. All must be addressed when considering declaratory policy.

The most attractive are those which dissuade an adversary from attacking. In practice this includes to deter, to thwart early on in the preparations for the attack, to preempt attackers before they can launch an attack, and to harden oneself to reduce vulnerabilities.

Thwarting an attack deflects the attack rendering it ineffective. Hardening can serve either to deter, when hardening is highly effective, or to reduce the effectiveness of the attack. Distributing facilities, thus increasing the number of aim-points, creating virtual facilities behind which real facilities are hidden, adding redundancy, and deception can also serve to thwart.

When these fail, one seeks to limit the amount of damage in real-time to a minimum. This is also a time for the cyber equivalent of civil defense, making users aware of an

attack so they can take individual protective actions beyond the direct control of central authorities.
Disconnection, either to disconnect the defender from an on-going attack or to disconnect the attacker can be useful though difficult to implement on a national scale currently.

Post-attack the defender reconstitutes what was destroyed and undertakes analyses to understand how the attack succeeded, what warning signs were present that were disregarded, and how the defense can be strengthened to reduce the likelihood or effectiveness of a future attack.[1]

Defense is a combination of all these, selected according to the technical capability of the defender, the value of assets to be protected, the costs to defend them, and the anticipated threat. All are part of total picture. Deterrence, while attractive if one can pull it off, is not the only option open to a defender. The policy declarations proposed later address the full range of cyber defenses.

DEFENDING WHAT AGAINST WHOM

Defenders must deal with three kinds of attackers. *Nuclear state*s because they are cyber-capable as well, have global agendas, and may see the U.S. as either an obstacle or a military or economic threat to their agendas. *Non-nuclear states* are likely to see cyber weapons as an attractive counterbalance to U.S. conventional and nuclear capabilities. Cyber weapons are inexpensive, widely available, relatively easy to master, and a cyber attack can be cost-free as long as attackers can remain anonymous. The attacker tier below states is that of *sub-state groups*. They consist of terrorists and other criminal and extremist groups. The lowest level of attackers are *individuals*, the cyber equivalent of the Unibomber, but also including a wide range of frivolous ankle-biters. The latter appear frequently in discussions of cyber defense although the threats they pose are not of a worrisome magnitude. Some will, however, turn professional and thus can be viewed as apprentice attackers.

Cyber technology has resulted in an active cyber underground and commercial malware industry. Virus production has been automated and there is a malware market for goods and services to support spamming, phishing, and other potentially dangerous activities. A recent report notes:

> “Half (52 percent) of new malware strains only stick around for 24 hours or less. The prevalence of short lived variants reflects a tactic by miscreants aimed at overloading security firms so that more damaging strains of malware remain undetected for longer, according to a study by Panda Security. The security firm, based in Bilbao, Spain, detects an average of 37,000 new viruses, worms, Trojans and other security threats per day. Around an average of 19,240 spread and try to infect users for just 24 hours, after which they become inactive as they are

[1] Stephen J. Lukasik, Seymour Goodman, and David Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack*, Adelphi Paper 359, International Institute for Strategic Studies, London (2003).

> replaced by other, new variants. Virus writers — increasingly motivated by profit — try to ensure their creations go unnoticed by users and stay under the radar of firms. It has now become common practice for VXers to review detection rates and modify viral code after 24 hours. The practice goes towards explaining the growing malware production rate. The amount of catalogued malware by Panda was 18 million in the 20 years from the firm's foundation until the end of 2008. This figure increased 60 percent in just seven months to reach 30 million by 31 July 2009."[2]

State actors pose the greatest existential threat. They have resources, discipline, and can recruit and train numbers of personnel and manage large planned attacks. They have sovereign power to provide potential target intelligence and the means to acquire vulnerability information. They can have clear reasons for attacking other states. But against these advantages one must have a realistic assessment of their strategies for the use of force to achieve their objectives and the role cyber force is likely to play.

Sub-state groups pose a very different threat. They have more limited agendas than do states and must operate under everyone's radar. The fluid nature of their organizations, leadership, numbers, goals, and rapid changes in technology complicates assessing the threats posed by such groups. They may, in their totality, represent the larger part of cyber threats to the U.S.

Cyber attacks are usually defined as software attacks, seen as arising from "outside" and to use the Internet or other network facilities to deliver attacker cyber force to the target. The attacker is seen as anonymous. The attack consists of transmitting software or data to the target such as to cause a computer to malfunction, or to enable the attacker to insert, destroy, copy, or modify data files contained therein. The modification can consist of encrypting the files so the attacker can hold them hostage for ransom. A network attacker can be part of the production and distribution supply chain for software and hardware as well, where the attack software is delivered "shrink-wrapped."

One can interrupt computer-enabled operations by attacking circuit board power supply logic, causing soft and hard failures. The target computer or system can be attacked by disabling the support systems on which operators depend: building security, fire protection, system power, and the like. One can induce soft or hard failures through electromagnetic pulse technology. Attacks on computer systems using physical force are attractive because, even in distributed systems, efficiency requires concentrations of hardware: system control centers, server farms, and specialized facilities for manufacturing, maintaining, and distributing subsystems and components.

There are two kinds of targets to defend: the economy and people, either groups or individuals. Attacks can large or small, and repeated frequently or infrequently.The people-directed attacks have results that are similar to those of psychological operations,

[2] See <http://www.theregister.co.uk/2009/08/13/malware_arms_race/>.

producing soft damage that is less easy to measure but is as central to warfare as physical damage.

ECONOMY-ORIENTED CYBER ATTACKS	
Small attacks repeated frequently	1. Damage or bankrupt an economy 2. Defraud or extort parts of an economy
Large attacks repeated less frequently	3. Damage or destroy a single infrastructure 4. Exploit interdependencies among infrastructures
PEOPLE-ORIENTED CYBERATTACKS	
Attacks on a large number of people	5. Destroy trust within a population 6. Wear down resistance to policy change
Attacks on individuals or small groups	7. Attack reputations of leaders 8. Destroy confidence in elites

Military doctrine calls for controlling strategic territory. Despite the distributed nature of public networks that seems to deny such a possibility, there are cyber analogs. The essence of a network is its connectivity. Controlling network connectivity thus amounts to control of strategic territory.

International gateways will be central to such attacks. Control of the Internet is in part defined by control of the connectivity it enables. If an attacker seizes cyber control of these facilities, he would be in a position to disconnect parts of the network at will.

DETERRING CYBER ATTACKS BY STATES

Cyber conflict between states is very different from conflict involving conventional and nuclear force. Concepts of deterrence formalized in the Cold War are of limited utility. Dissuading the Soviet Union from launching an attack on the U.S. through fear of a certain and unacceptable response was the only plan that seemed to offer security early in the Cold War. Implicit was that both sides have comparable forces whose capabilities are known, that decapitating attacks can be made infeasible, that the survival of a retaliatory capability on each side is assured, and that firebreaks are fashioned so that escalation of the level of force in any conflict can be controlled. Deterrence had a psychological as well as a physical dimension.

But when an conflict involves computers against computers, the psychological aspect of the threat is missing. National leaders may not even have a clear idea of the vulnerabilities of their computer networks. Deterring cyber conflict requires expanding the concept of deterrence well beyond the framework of nuclear deterrence.

Beyond dissuading through fear of retaliation, dictionaries offer other synonyms for "deter." It can mean to discourage an attacker through effective defense or thwarting actions that make attacker success too uncertain. It can mean preventing by preemption. These broader meanings of deterrence suggest defense will play a larger role in cyber deterrence than in the nuclear case, where defenses were seen as destabilizing to the nuclear balance.

While the details of deterrence will be different, there are three aspects of deterrence that carry over. A defender's response must be seen as technically *feasible*. In the nuclear case, very visible weapon tests and well publicized images of nuclear detonations and measured global radioactive fallout provided convincing demonstrations of feasibility. Second the defender must be seen as *credible*, willing as well as able to respond. U.S. nuclear weapon use in WW II established that, and equivalent Soviet nuclear capabilities left little doubt what their response to a nuclear attack would be. Finally, defense through deterrence requires being *able* to respond, an offensive capability. While response to a cyber attack need not be a cyber counter-attack, international principles of armed conflict speak to proportionality of response and escalation control favors responding in kind. Thus cyber offense is a component of cyber defense, however much defense was seen as undesirable in the framework of nuclear deterrence.

DETERRING CYBER ATTACKS BY SUB-STATE GROUPS

Deterring sub-state groups from cyber attacks differs from deterring sovereign states. With fewer fixed assets, sub-state groups have greater flexibility, and their independence from sovereign commitments insulates them from many types of sanctions or punishment approaches to deterrence. Their strength is in their people and their commitment to an idea. Cyber weapons would seem to be attractive to them despite their the departure from the simpler forms of violence and intimidation they have employed to date. Nevertheless, the degree to which potential cyber capabilities are congruent with sub-state groups' operational code is relevant to U.S. planning.

To this end, it is useful to examine how one vocal sub-state group see the potential utility of cyber attacks. Jihadists, whose track record and declared antipathy to western values, makes them worth examining. Al-Qaeda, its affiliated terrorist groups, and its Jihadist supporters, like everyone else, use to the Internet. There are currently at least 5,000 Jihadist websites.[3] The most important, large forums that serve as hubs for the virtual Jihadist community and clearinghouses for terrorist propaganda and tactical materials, have tens of thousands of registered members.

In spite of the enthusiasm with which these individuals, active terrorists as well as sympathizers, have embraced the use of cyberspace, the bulk of their online activities are unrelated to "cyber terrorism" in the traditional sense of launching destructive attacks over the Internet. Instead, they use the Internet for coordinating various functions related to terrorism, including funding, recruitment, propaganda, dispersal of tradecraft, intelligence collection, and training.[4]

[3] MSNBC. "Pentagon Surfing 5,000 Jihadist Websites," May 4, 2006. See <http://www.msnbc.msn.com/id/12634238/>; Burleigh, Michael. "Some European Perspectives on Terrorism," Foreign Policy Research Institute, May 2008. See <http://www.fpri.org/enotes/200805.burleigh.europeanperspectivesterrorism.html>

[4] Kohlmann, Evan F. "The Real Online Terrorist Threat," Foreign Affairs, Sept/Oct 2006; Timothy L. Thomas, "Al-Qaida and the Internet: The Danger of Cyperplanning," Parameters, Spring 2003.

In recent years, however, a growing interest in using hacking methods to achieve various Jihad objectives has emerged. "Jihad" in both its technical meaning of "struggle" and its use by militant Muslims refers to a range of activities associated with combating the enemies of Islam and defending the pan-Islamic nation. This includes not only militant-style attacks, but proselytizing, recruitment, fundraising, psychological influence, economic warfare, and a number of other activities.[5] Pursuant to the conception of Jihad as a holistic political struggle, the community's activities are broader than conventional cyber-terrorism. Most fall into types of Jihad that is political but not immediately violent.

A illustrative example occurred during the online backlash to an incursion by Israel Defense Forces (IDF) into the Gaza Strip in December 2008. Hackers from the Muslim world self-mobilized to attack tens of thousands of Israeli websites. Most of these hackers executed simplistic attacks – defacing websites and leaving threatening messages, or they launched denial-of-service attacks to take the websites offline. Government, hospital, banking, and media sites were successfully attacked, in addition to the websites of thousands of large and small companies and organizations.[6] The stated motivations for the attacks fell under the rubric of supporting Jihad, but were not immediately violent. The four most commonly articulated motivations for the anti-Israel hacks were:

> *Inflicting financial damage to Israeli businesses, government, and individuals*: A message on the Arabic hackers' site Soqor.net exhorted hackers to "Disrupt and destroy Zionist government and banking sites to cost the enemy not thousands but millions of dollars…"
>
> *Delivering threats of physical violence to an Israeli audience*: One Moroccan hackers' team posted symbols associated with violent Jihadist movements and an image of explosion, along with a threatening message for Israelis.
>
> *Using cyber attacks as leverage to stop Operation Cast Lead*: Many of the defacements contained messages indicating attacks on Israeli sites and servers would stop only when Israel ceased its violence in Gaza.

[5] See, for example, the popular pamphlet "39 Ways to Serve and Participate in the Jihad." Variations on this document have been widely circulated on Jihadist websites since 2003. The pro-Jihadist translation service "Tibyan Publications" has published an English translation available at: http://www.archive.org/details/39WaysToServeAndParticipate. Indeed, the document supplies two definitions for "electronic Jihad:" one refers to organizing and distributing information on the Internet, the other refers to hacking. The hacking activities recommended involve taking offline American and other websites, and do not refer directly to any cyberterrorist scenarios.

[6] Project Grey Goose Phase II Report; available http://greylogic. U.S./?page_id=85. U.S. and NATO military websites were also attacked. A group of Turkish hackers defaced one of three subdomains of mdw.army.mil, the URL of the U.S. Army Military District of Washington, as well as the website of the Joint Force Headquarters of the National Capital Region. The same group left a threatening message on the NATO parliament site www.nato-pa.int. The message read: "Stop attacks u israel and usa! you cursed nations! one day muslims will clean the world from you![6] See: McMillan, Robert. "Hackers Deface NATO, U.S. Army Web Sites," Computer World, January 9, 2009. The NATO defacement is available at: http://www.zone-h.org/content/view/15003/30/.

> *Fulfilling the Religious Obligation of Jihad*: Some hackers couched their activities in religious terms, insisting that cyber attacks were tantamount to fighting Jihad against Islam's enemies. One hacker wrote, " Use [the hacking skills] God has given you as bullets in the face of the Jewish Zionists. We cannot fight them with our bodies, but we can fight them with our minds and hands…By God, this is Jihad."[7]

This sort of Jihadist "hacktivism" has become a popular way for sympathizers to target perceived enemies of the faith. The Netherlands and Denmark have also been targeted by similar grass-roots campaigns in response to their newspapers' decisions to publish cartoons depicting the Prophet Mohammed in 2006.[8] U.S. websites have been targeted.[9] A smaller-scale effort targeted Chinese websites during Uighur-Han Chinese violence in 2009.[10] Such attacks may be popular because they are approved by the mainstream of the Muslim world. The Islamic university al-Azhar in Cairo, the single most influential religious institution in the Sunni Muslim world, issued a fatwa in October 2008 approving cyber attacks against American and Israeli websites. "This is considered a type of lawful Jihad that helps Islam by paralyzing the information systems used by our enemies for their evil aims," read the fatwa.[11] The fatwa explicitly endorsed attacks on websites, but it was not clear whether it could be extended to justify true cyber terrorist attacks.

While many of the Jihadist-hackers online have embraced a menacing form of hacktivism, there are intimations that others seek to harness these skills for cyber terrorism purposes. The prominent al-Qaeda strategist Abu Ubaid al-Qureishi has discussed the potential of cyber-terrorism. Al-Qureishi was a bilingual analyst who exploited English-language western sources, including writings by U.S. military, in the strategic documents he wrote in Arabic for the al-Qaeda core group in Afghanistan.[12]

In his essay titled *The Nightmares of America*, al-Qureishi describes the five terrorism scenarios he asserts frighten the U.S. most. He explains that the purpose of his exercise was to exploit western security analysis to uncover the greatest vulnerabilities in U.S. security. Al-Qureishi believed al-Qaeda should let these analysts, who publish prolifically in the open source domain, lead the way:

> In order to become acquainted with the enemy's hidden weak points, one must examine the studies that Western strategic analysts have written about the real or

[7] Motivations are excerpted from: Project Grey Goose Phase II Report; available http://greylogic. U.S./?page_id=85

[8] Project on Jihadist Websites First Quarter 2008, International Centre for Political Violence and Terrorism Research, May, 2008, p. 24.

[9] See footnote 2. Also, the Israeli portals of American companies were among those aggressively targeted in the response to Operation Cast Lead.

[10] The author observed a mild campaign against Chinese websites during this time on Jihadist hacking forums.

[11] AKI. "Sunni Scholars Sanction Electronic Jihad," October 16, 2008.

[12] Sources vary as to whether al-Qureishi is still alive.

> imagined security gaps and dangers threatening the security and safety of American society. Their fears must be studied carefully, because they usually point to weak points in American national security.[13]

Cyber terrorism is one of the five methods of attack outlined in the essay. Al-Qureishi describes four advantages of attacking over the Internet: cyber terrorist attacks can be conducted anonymously from a distance; the technology required is inexpensive; cyber attacks do not require exceptional skill; and few people are needed. His target list is from U.S. reporting on the subject: "As for the targets that the Jihad movements might choose, they range, in the view of American experts, from huge electrical grids to nuclear power plants, financial institutions, and the 9-1-1 emergency telephone network."[14]

He describes previous successes by hackers and concludes that, based on the rapid dissemination of hacker knowledge over recent years and the transformation of the U.S. economy into "a basically informational economy...[there is] a possibility [of launching] repeated, focused attacks with a very considerable effect."[15]

It is rare to find a document like al-Qureishi's essay that includes both the method of attack and possible targets. In discussing possibilities for violent attacks, Jihadists in terrorist forums rarely provide targeting information. Instead, their discussions focus on the techniques and tactics available to carry out an attack against an unspecified target. Jihadists write prolifically on surveillance, recruiting, kidnapping, executions, bomb-making, and other methods of violence, but have few discussions of specific terrorist plots against expressly identified targets. Targeting selection is assisted by higher-level strategic and theological documents, which provide religious justifications and strategic guidance for striking large classes of targets – such as oil targets in the Arabian Peninsula, or American tourists in the Middle East – without specifying particular locations. The objective is to distribute the tactical knowledge necessary for an entrepreneurial terrorist group to plan and execute its own attack, while minimizing the risk that the plot will be anticipated and disrupted.

The same is largely true of the Jihadist-hacker forums. The forums provide advice, manuals, and information on hacking tools and skills, usually without directing individuals against specific targets. Attacks are usually advertised after they have been successful.[16] A hacker will state his intention to use a certain hacking technique or tool against a general category of targets, such as "Zionist computers" or "Crusader websites."

The skills and knowledge observable in the forums must be considered in the context of intention. The forums are defined by explicit, overwhelming political motivations. While

[13] Al-Qureishi, Abu Ubaid. "The Nightmares of America," February 13, 2002. Originally obtained from the Jihadist website *al-Qal'ah* (now defunct) on June 6, 2005.

[14] Ibid.

[15] Ibid.

[16] This is not always true, certainly there are posts in which one hacker will urge others to help him attack a certain site, but it is the case most of the time.

other hacking movements may be dominated by those professing criminal or ego-driven motivations, the Arabic-language hacking forums monitored consistently exhibit Jihadist-motivations.[17] While some may be content to fulfill their obligation to wage Jihad by defacing the homepages of Dutch newspapers, others are likely to have more dangerous ambitions against the U.S.

As evidence of this, one can examine other materials available to Jihadist-hackers on one of the hacker forums examined. This hacker forum is one section of a larger extremist website called *The Electronic Mujahideen Network*. A member of the hacker forum is also granted access to the other sections, which contain items encouraging terrorist operations, including bomb-making manuals and theological treatises justifying mass casualty attacks against infidels. The membership of the Electronic Mujahideen Network is likely to be more extremist and violent by nature than members of the Soqor.Net network, which is devoted entirely to hacking and IT-related topics. Moreover, by placing a hacking forum side-by-side with other forums devoted to more traditional terrorist methods, the administrators of the website are implicitly suggesting the use of the cyber means towards violent ends. Other violent Jihadist websites have also included hacker sections.

The skills and tools available in the hacking forums can be used to support conventional attacks. For example, Indonesian Jemaah Islamiya terrorist leader Imam Samudra organized the 2005 Bali bombings from his prison cell using a laptop provided to him by a prison guard. Samudra used the net to organize personnel and raise funds via online financial crime.[18] Samudra also authored a book in 2004 that contained a chapter advocating hacking for the sake of Jihad.[19]

Younis Tsouli, an aspiring terrorist living in the U.K., used his knowledge of cyber security to cover his tracks online while helping to coordinate the planning of potentially disastrous bombings in Canada, the U.S., Bosnia, and the U.K.[20] He functioned as the lynchpin of an international network of aspiring terrorists who used Jihadist websites to communicate and obtain tactical information. His colleague, Tariq ad-Dour, was in charge of terrorist financing. He used Trojan horses and phishing scams to obtain 37,000 credit card numbers, to which he charged $3.5 million, including over 250 plane tickets. Ad-Dour laundered the money using online gambling websites.[21]

Tsouli, Ad-Dour, and a third accomplice aspired to be the Osama Bin Laden and Ayman

[17] Zone-H poll shows that roughly 1/10th of defacements worldwide are politically motivated, with another 1/10th motivated by "patriotism." Presentation by Kenneth Geers and Peter Feaver. "Cyber Jihad and the Globalization of Warfare." Available at: http://www.chiefofstation.com/pdf/Cyber_Jihad.pdf

[18] AsiaNews.It. "Bali Terrorist Organised Attacks from Behind Bars," Aug 24, 2006. Indonesia Matters. www.Anshar.net & Chatroom Jihad, Aug U.S.t 24, 2006.

[19] Sipress, Alan. "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace," The Washington Post, December 14, 2004.

[20] NEFA Foundation, "Irhaby 007's American Connections," July 2007. http://www.nefafoundation.org/miscellaneo U.S./Irhaby007_AmericanConnections.pdf

[21] Krebs, Brian. "Terrorism's Hook Into Your Inbox," The Washington Post, July 5, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html.

al-Zawahiri of the new generation of terrorists, operating as terrorist "venture capitalists" who facilitate and finance plot ideas proposed to them by different entrepreneurial terrorist cells – as Bin Laden and Zawahiri have been reported to do. When the three were arrested in late 2005, they were associated with terrorist plots against targets in Sarajevo, Washington D.C., southern Ontario, and undisclosed cities in the U.K. They were also involved in plots against military bases in Georgia and Florida.[22]

Tsouli and his accomplices could have successfully combined their hacking skills A hacking primer he authored, "The Encyclopedia of Hacking the Zionist and Crusader Websites," is a popular download on the Electronic Mujahideen Network and other Jihadist websites.[23]

Another kind of operation that combines conventional and cyber is an electromagnetic pulse weapon (EMP) attack. EMP has garnered increased interest on Jihadist forums, especially the Electronic Mujahideen Network, where four articles on the subject have been recently published. The articles contain descriptive information on the construction and impact of EMP weapons. They are not so detailed as to suggest engineering experience or experimentation with building a prototype; rather, they reflect open source research performed in English and translated into Arabic.[24]

Another kind of "combination" attack scenario is one in which terrorists exploit the timing of a natural disaster or economic downturn to amplify the impact of a cyber attack. During the severe economic downturn of late 2008, several Jihadist forum members urged their counterparts in the U.S. to take advantage of the country's vulnerable position to launch a terrorist attack.[25] Although this did not occur, it reflects an awareness of the power to amplify the impact of an attack – either cyber or conventional – by timing it correctly. Some believe hackers can make a significant impact on the economy without carrying out a large-scale attack if done during an economic downturn.

Deterring sub-state attackers will depend on forms of deterrence that do not rely on the threat of punishment but rather on cost-imposing approaches. Central to these are measures taken to discourage an attacker through assured defense, possibly involving trans-attack actions such as disconnection. To the extent that sub-state groups are unable to mount sufficiently large attacks, discouraging them may be the answer, at least for the present. Tracking Jihadist activity on-line will be important, especially since they must use the Internet for their internal training and motivational purposes.

[22] Katz, Rita and Josh Devon. "Web of Terror," Forbes, July 5, 2007.

[23] A translation of this manual is available from the CIA Open Source Center.

[24] One of the articles was a paraphrased translation of this paper by A U.S.tralian research Carlo Kopp, available from globalsecurity.org. http://www.globalsecurity.org/military/library/report/1996/apjemp.htm

[25] Project on Jihadist Websites Third Quarter 2008. International Centre for Political Violence and Terrorism Research, October 2008, p. 5.

CYBER DETERRENCE IN PRACTICE

While many countries can look to their own resources and their own defense, the U.S. position has, since WW II, been that collective defense is important for strong and weak alike. Coalition actions, some under the UN, some under NATO, and some ad hoc arrangements represent current examples. Extended deterrence, to be viable, requires demonstrations of capability so that allies and adversaries can adjust their expectations.

Demonstration of cyber power is thus a part of deterrence. There are, however, difficulties in demonstrating cyber offense and defense capabilities. Demonstrations of cyber power could be counter-productive if they were sufficiently impressive. It is difficult to conceive of potentially nation-harming cyber demonstrations that are safe. The U.S. policy has been to keep secure the extent of our cyber attack and defense capabilities. It has been successful, to the point that attackers may not be adequately aware of U.S. offensive and defensive capabilities. While this is good defense, it weakens deterrence.[26]

The current U.S. focus on protecting military computers, thus adhering to clear DoD areas of responsibility, is a politically sound course domestically, and it is fully justified as a force protection mission. But DoD “rides on” the economy and its interconnected infrastructures. Hence simply protecting itself is only the start of a more extended set of necessary U.S. defensive actions.

This notwithstanding, creating a cyber deterrent will depend on having something specific beyond the level of policy and doctrinal statements. One needs cyber plans of action. Talk depends on earned credibility, but executable plans are real. Plans of action can be used to establish the level of "forces" required, the feasibility of specific attacks, targeting doctrine, intelligence requirements, understanding consequences of execution, training and exercises needed, “cyber force” deployments, global situation awareness, and a host of practical matters. We need to know what the exercise cyber power looks like beyond the level of PowerPoint charts.

Cyber power can effect both hard and soft results. Thus deterring the use of cyber force will depend on both forms of power. Diplomatic and economic power are measured in ways quite different from the metrics of hard military power. Informational, i.e. cyber, power with aspects of both is not simply a subset of hard power. The integration of these three elements of power is not simple. The extension of military concepts and

[26] A recent NRC report, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities,*" National Academies Press, Washington, D.C., April 29, 2009 makes substantially the same points. In Chapter 3, "Military Perspectives on Cyberattack." it notes, "At the date of this writing, an unclassified and authoritative statement of current joint doctrine for the use of computer network attack is unavailable, and it is fair to say that current doctrine on the matter is still evolving." In Chapter 9, "Speculations on the Dynamics of Cyberconflict," under Section 9.1, Deterrence and Cyber Conflict," it notes, "It remains an open question as to whether the concepts of deterrence are relevant when applied to the domain of cyberconflict per se (that is, cyberconflict without reference to conflict in physical domains.")

technologies devised for industrial war to counterinsurgency, counter-terrorism, and peace-keeping, all mixed hard and soft enterprises, reveal the difficulties in strategic integration.[27] DoD "Deterrence Operations Joint Operating Concept," issued December 2006, recognizes this:

> Deterrence requires a national strategy that integrates diplomatic, informational, military, and economic powers. The Department of Defense must develop strategies, plans, and operations that are tailored to the perceptions, values, and interests of specific adversaries.

Power is measured in known strengths, but uncertainty has a value also. Deterrence depends not only on firm measures of strength, but on uncertainty in the use of that power. A potential aggressor is deterred because he is not certain whether the future will be better or worse for him than the present. Thus the creation of uncertainty is as important for deterrence as projecting certainty.

A FRAMEWORK FOR THINKING ABOUT CYBER CONFLICT AND CYBER DETERRENCE

Unless one has an understanding of cyber conflict, construction of policy declarations can not lead anywhere. The purpose of the preceding discussion has been to establish what cyber conflict "looks like." Contrary to what appears to be the prevailing view, that cyber conflict is like kinetic conflict but with cyber weapons and cyber warriors substituted, the basis for the declarations proposed here is different.

Cyber conflict is the delivery of "cyber force." Cyber force is the means of utilizing the inherent power of information for control and its transmission through public networks to achieve national goals. It takes place not in kinetic space but in the space of a myriad of electrical connections. In practice, a "cyber attack" consists of transmitting software or data from one computer to another.

Control can be of physical systems, or of people. In the latter case cyber force produces effects previously the province of "psychological operations." This can include trust attacks, social alienation attacks, and exhaustion attacks. They have much in common with swarming attacks.[28]

[27] Rupert Smith, *The Utility of Force: The Art of War in the Modern World*, Random House/Vintage Books, New York, (2007).

[28] A quite comprehensive study of swarming in kinetic conflicr is the the Pardee RAND Graduate School dissertation of Sean A. Edwards, "Swarming and the Future of Warfare," 2005. In contrast to linear warfare, swarming tactics are a characteristic of modern conflicts where forces undertake non-linear dispersed operations. He notes that swarming tactics are of two types: cloud swarms where the forces arrive at the target as a single mass and vapor swarms where attackers are initially dispersed and converge on the target. There are cyber equivalents to these: distributed denial of service in the case of the former and slow build-up of attacks over time that enable an overwhelming blow on a target in the latter. Swarming attacks can be defeated by, among other means, superior situation awareness, undermining attack enablers, and

Control of the "battlespace" requires control of the network connectivity that makes such attacks possible. At a minimum it means an attacker can disconnect what he threatens and the attacker can, in response, disconnect the attacker. But matters are unlikely to come to that point. In this both real and abstract battlespace, a more delicate minuet takes place continually: a cat-and-mouse game, the thrust and feint of chess, fencing or boxing. It has a parallel to the war between spam and spam filters we all fight, and traditional electronic warfare of measure, CM, CCM, … C^nM. Intelligence operations, particularly Sigint, cryptography, and deception are the essence. One might reasonably borrow the title of R.V. Jones' account of British scientific intelligence in 1939–1945, *The Wizard War,* to describe it.

In this framework, preemption takes on a very different meaning from preemption in kinetic conflict. It may not be to pass a point of no return. It can simply be to take the next step in the wizard war. It is the $C^{n+1}M$ to the C^nM set of countermeasures.[29]

B. Declaratory Policy Contributions to Cyber Defense

Perspectives on Declaratory Policy

Declaratory policies begin as words on paper. They can be ignored, overtaken by events, or become irrelevant under technological change. To be of value, there must be a plausible chains of events to implement them.

An example is the Universal Declaration of Human Rights adopted as UN General Assembly Resolution 217 A (III) in 1948. It asserts a number of human rights declared to be universal. Translated into 375 languages, it has spawned follow-on treaties dealing with elimination of racial discrimination (1969), elimination of discrimination against women (1981), a convention against torture (1984), and a convention on the rights of the child (1989). While many of these goals are still not universally recognized, the treaty structure has resulted in countless human rights watch groups, progress reports, political demonstrations, and international pressure to meet its ideals. It synthesizes widely felt concerns and stimulates action. To use a current expression, it is a declaration with "legs."

The fact a declaration, U.S. or otherwise, is unilateral is not a limitation for its broader applicability, given plausible ways to advance its intent. Declarations can be seen a warning; as laying down an invitation for others to embrace its goals; or they can propose

using "bait" tactics. Examples of these can be found in the declarations suggested in the following discussion.

[29] Michael Schrage argues, in "A Softer Way to Preeempt Hostile Attacks," in the Washington Post, Aug 21, 2005 that "soft" preemption, consisting of disrupting information flows or other non-disruptive technical interference could arguably save lives if taken in lieu of conventional resorts to force. See <www.washingtonpost.com/wp-dyn/content/article/2005/08/20/AR2005082000108.html>

normative standards of behavior, to be furthered through the declaration's logic and the recognized appeal of its goals. When a few major states, supported by non-state groups as well, undertake to implement its intent, the words begin to turn into actionable pressures and decisions.

Recognizing that declarations can be a starting point on the path to more formal international agreements, it is well to keep that in mind in formulating them. There are four characteristics that will be important.

> (a) Verifiable – if declaratory policy is to effect change in something, actions taken or actions not taken, these should be observable. Being observable, parties to an international agreement can then decide if what is observed is consistent with the intent of the agreement. If it is not, the parties behaving in incompatible ways can be asked to clarify the events called into question, or the agreement itself can be amended to reflect changed circumstances.
>
> (b) Reciprocal – all parties should be held to the same standards. A signatory expecting to be a target of a prohibited action should be prepared to eschew that action itself.
>
> (c) Robust under change –negotiating agreements is sufficiently complicated they should have more than a transitory period of applicability. A common driver of obsolescence is technology. In the cyber world, technology changes so rapidly that agreements must be capable of dealing with very different future capabilities than those existing when it was formulated.
>
> (d) Consistent with prior agreements –prior agreements must be accommodated and their precedents recognized and used. Consistency with prior agreements eases the acceptance of new proposals. Inconsistencies complicate reaching new agreement.

The declarations proposed here are not offered in an advocacy sense. The intent is to table some strawmen to stimulate discussion of the role of such policy initiatives. The domestic and international issues surrounding them will require far more analysis than possible in this essay.

CIRCUMSTANCES ADDRESSABLE BY CYBER-RELATED DECLARATIONS

The starting point for examining the domain of declaratory cyber policies is to define what concerns they could seek to address. Professional literature and the public media are rich in enumerations of concerns introduced by the convergence of digital technology, ubiquitous devices for manipulating digital representations, and the relative ease with which ideas can be communicated and widely accessed: the Internet, portable wireless devices, social networks, increasing bandwidth, and the educational, business, government, political, and social innovations that can be built on these capabilities.

The concern here is attacks of "national significance." The Department of Defense uses as the definition of an "incident of national significance:"

> An actual or potential high-impact event that requires a coordinated and effective response by and appropriate combination of Federal, state, local, tribal, nongovernmental, and/or private-sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities.

In 2005 the Department of Homeland Security offered fifteen National Planning Scenarios for "'plausible terrorist attacks and natural disasters that challenge the Nation's prevention and response capabilities." Four provide some calibration for what might be addressed by declaratory policies: detonation of a 10 kT nuclear device; a major earthquake or hurricane; and a cyber attack. A commonly expressed concern in the cyber community is a "cyber Pearl Harbor." The 1997 report of the President's Commission on the Critical Infrastructure Protection referred to "cascading events" in what are believed to be unstable systems of systems.[30]

Equating "significant" cyber attacks to 10 kT nuclear detonations, major earthquakes, and hurricanes conveys some sense of what is under discussion, but a link between damage, death, and computers is needed. For computer-inflicted damage to be crippling in the sense of a national economy, it must be long-lasting. Interrupting the operation of computers, however inconvenient, does not rise to the level of crippling. Computers, power systems, and communication systems fail regularly and states do not collapse. If such failures were to be widespread and coordinated, a nation would sustain larger economic losses. But engineers design, build, and operate systems to be robust under stress through backups, hot standbys, redundancies, rapid repair plans, other approaches to damage limitation and service restoration. What is needed to create long-lasting social and economic impacts from cyber attacks is to cause physical damage to large, expensive equipment for which spares are not available and for which manufacturing replacements is lengthy. This will be the case with damage to electrical generators, high voltage transformers, pumping stations, communication switches, routers, and server farms supporting information utilities such as cloud computing.

There are several examples of technical and regulatory issues relating to what we now call cyber war. Following the invention of the telegraph in the 1840s, states realized that technical standards were needed if the full potential of the new technology were to be realized. The history of telegraphy, and its parallels to our current circumstances, is elaborated on by Standage.[31]

The nineteenth century struggles for the regulation of international communications were renewed with the invention of radio and the introduction of wireless telegraphy in the

[30] *Critical Foundations: Protecting America's Infrastructures,* Report of the President's Commission on Critical Infrastructure Protection, The White House, October 1997

[31] Tom Standage, *The Victorian Internet*, Walker and Company, New York (1998).

early twentieth century. The history has been recounted by Rutkowski.[32] The parallels to today in both cases are striking and the measures adopted provide a useful starting point for addressing present concerns. Rutkowski notes:

> “The first U.S. interagency committee dealing with wireless cyberwar was convened in 1904 and primarily led by the Navy Department.
>
> As the years progressed during the 1900’s, however, chaos emerged. Almost everyone was incented to get on the wireless internet. Commercial business, government, ordinary people, even the equivalent of “script kiddies” and hackers of today – the first radio amateurs – all got “on the net.” Enterprises constantly pushed the state-of-the-art; new digital protocols were developed; nations were competing; network architectures and applications were continuously evolving; wireless cyberwar was becoming real …
>
> For years, the Washington political scene engaged in incessant wrangling as the wireless infrastructure and cyber security became progressively worse. Private enterprises claimed that technology and innovation would be impeded if the Berlin provisions [of 1906] were implemented, and argued that the infrastructure was overwhelmingly privately owned. Washington lobbyists warned against the dangers of Federal government involvement. There was a general antipathy against foreign nations and intergovernmental organizations. The military community wanted its own freedom of action to keep ahead of the rest of the world. And lastly, there was no consensus on what agency in Washington should act.
>
> On 22 April 1912, President Taft ratified the first multilateral agreement to which the U.S. became a party – the 1906 Berlin Convention - ending more than a decade of cyber conflict that was implicated as a causal factor in the sinking of the Titanic eight days earlier on 14 April 1912. The sinking and the subsequent investigations so inflamed public opinion that the 1906 Berlin treaty was quickly signed and an additional set of domestic and international actions undertaken by the U.S. government, together with other nations, in London in 1912 to mitigate further cyber conflict.
>
> It was the first acceptance of an international telecommunication treaty by the U.S. – after refusing for nearly 50 years to become a party to any related agreements or instituting any regulation of the early wireless cyber environment …
>
> Any bright entrepreneur or kid with a modicum of knowledge and inventiveness could become part of the emerging global infrastructure. Fortunes were made overnight. However, the problem was that any kid’s wireless transmitter in a

[32] A. M. Rutkowski, “Lessons from the First Great Cyberwar Era.” Info, 12 Feb 2010.

> garage could wreak havoc on a network somewhere else in the world – including those supporting critical business, national security, or emergency needs …
>
> The cybersecurity course proved cyclic over the years as each new cyber technology emerged, or administrations and appointees changed, or the U.S. global ambitions advanced or diminished. In general, however, the cycle remained the same. Excitement, euphoria, and innovation by geeks are followed by unfettered industry assimilation and exploitation, which gives rise to pervasive public implementations and then conflict among nations to maintain perceived advantages."

LIMITS ON THE USE OF CYBER FORCE IN PEACETIME[33]

The UN Charter forbids "acts of aggression" and restricts "the threat or use of force" in peacetime.[34] Article 41 of the Charter empowers the Security Council to enforce these restrictions through the "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication, and the severance of diplomatic relations." If these measures prove insufficient, Article 42 provides for "such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea or land forces."

If a UN member suffers an "armed attack", the Charter reserves to it the right of individual and collective self-defense. However, responding with force to a non-force action is prohibited. UN General Assembly Resolution 3314 defines aggression as the "use of armed force ... against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the [UN] Charter."[35] As examples of aggression, the resolution cites invasion, attack, occupation, bombardment and blockade by armed forces.

Factors that may influence whether something is an act of force include expected *lethality*, *destructiveness,* and *invasiveness*. Lethality is measured by lives lost, both from primary and reasonably certain secondary effects. Destructiveness reflects physical and economic damage to tangible property. Invasiveness means incursion into the geographic

[33] This and the following section relies on extensive passages, not otherwise identified by quotation marks, from Gregory D. Grove, Seymour Goodman and Stephen J. Lukasik, "Cyber-attacks and International Law," Survival, Vol. 42 Number 3, Autumn 2000.

[34] UN Charter, Art. 1, ¶1; and Art. 2. ¶ 4. The concepts 'armed attack', 'force' and 'aggression' are closely linked. This article focuses on 'force', rather than separately analyzing the three concepts, since force is a necessary component of the other two. For a separate analysis of these three concepts, see Walter G. Sharp, *CyberSpace and the Use of Force*, Aegis Research, Falls Church, VA, 1999, pp. 123, 127–28.

[35] Grove, Goodman, and Lukasik op. cit. G.A. Res. 3314, UN GAOR, 29th Sess., Supp. No. 31, p. 143, UN Doc. A/9631 (1974). General Assembly resolutions are not binding on member states. See UN Charter, Arts. 10, 11, 14.

territory of a sovereign adversary.[36]

The prevailing view is that economic sanctions and diplomatic responses do not constitute force under the UN Charter.[37] Furthermore, Article 41 suggests that interrupting communications is not inherently a use of force. Article 2 forbids the use of force against the "territorial integrity or political independence of any state." Interpreting the prohibition of Article 2 in the light of Article 41 also allows for the conclusion that using an information operation to interrupt communications in a non-lethal, non-destructive, non-invasive manner may be permissible under the Charter. Minimally invasive information operations, such as response-port scanning, are clearly non-force actions.[38]

On the other hand, lethal, destructive or invasive information operations would clearly be a use of force. *Certain information-technology operations could cause destruction equivalent to the use of armed force, and thus may themselves be considered uses of force*. For instance, making dam-control software malfunction, causing a flood that destroys a city, would clearly constitute a use of force. Walter Sharp argues that even more attenuated forms of destruction, such as causing massive economic crises by crashing stock exchanges, are uses of force.[39]

There is a sizeable grey area between actions that clearly constitute a use of force, and those that clearly do not. Severing communications or economic relations, which is generally authorized by Article 41 as a non-force reprisal, may be accomplished by blockade, which is not so authorized and in fact is permitted only under Article 42 should Article 41 measures prove ineffective. Therefore, a Security Council resolution permitting Article 41 action to sever communications does not permit a blockade, even if that blockade seeks to sever communications. Instead, a resolution under Article 42 would be required. Electronically disabling a source state's international commercial communications could constitute a *de facto* blockade, but whether it falls into the Article 41 or Article 42 category is uncertain.

Thus, certain information operations are uses of force and others are not, and it will not always be clear which is the case. A determination may only be reached after the fact, on the basis of observed lethality, destructiveness and invasiveness. In addition, information operations may have effects not intended by the state initiating them. For example,

[36] Lawrence Greenberg, Seymour Goodman and Kevin Soo Hoo, *Information Warfare and International Law,* National Defense University Press, Washington DC, 1997, pp. 11–13.

[37] Grove, Goodman, and Lukasik op. cit. Walter G. Sharp, *CyberSpace and the Use of Force*, Aegis Research, Falls Church, VA, 1999, p. 88

[38] A port scan is a common probing technique, by which an attacker attempts to communicate with each numbered access port that a computer presents to its network. By analyzing how the target computer responds, the attacker may determine whether security precautions are lacking on any given port. A port scan is the cyberspace equivalent of trying every doorknob in a building to see if one has been left unlocked. A response-port scan is an automated in-kind scan to scare the attacker away by demonstrating that the target knows what it is doing.

[39] Walter G. Sharp, *CyberSpace and the Use of Force*, Aegis Research, Falls Church, VA, 1999, p. 102

restricting a nation's access to Internet servers so as to sever its civil communications (a non-force action under Article 41) could unintentionally impair that country's military communications, thereby constituting an act of force under Article 42. To further complicate matters, the UN Charter is not the only body of law that may apply to active defense in peacetime. The International Telecommunications Union (ITU) Convention, for example, prohibits any interference in another state's communications in peacetime, and requires protection of private communications, subject to the right to intercept them for reasons of national and internal security.

Thus whether the use of cyber force in peacetime constitutes an armed attack subject to individual and collective self-defense is situation dependent. This offers some potential for declaratory policy, to define what kind of cyber attacks, with what effects, will be considered the use of force.

LIMITS ON THE USE OF CYBER FORCE IN WARTIME

In wartime, the fewest restrictions exist on the use of force, and many of the uncertainties surrounding information operations in peacetime do not apply. The laws of armed conflict distinguish between combatants (regular and irregular military forces) and non-combatants (civilians, the wounded and others legitimately outside the sphere of combat). They prohibit the intentional use of force against civilian assets by combatants, although civilian-owned assets that support the military may be targeted provided that certain principles are followed.

The first principle – military necessity – permits the application of regulated force to secure the complete or partial submission of enemy forces, provided that this is limited to military objectives.[40] The second principle – proportionality – restricts the application of force to situations in which civilian losses are proportional to military advantage.[41] When many civilian and non-combatant lives depend on a mixed-asset information infrastructure, but have limited combatant use (for example, a hospital information system), these first two principles would counsel against an attack. In cases in which a larger system supports both combatants and non-combatants, such as a power grid, the propriety of an attack depends on a comparison of the importance of the military objective in securing the enemy's submission, and the damage to non-combatants and their assets.

When an attack passes muster under the first two principles, a third – the avoidance of unnecessary suffering – needs to be applied.[42] Under this principle, unlawful uses of lawful weapons (using a rifle as an instrument of torture, for example) are prohibited. Furthermore, if an alternative method exists to accomplish a stated military objective

[40] US Air Force Judge Advocate General School, *International Operations Law Deskbook,* Montgomery, AL 1996, pp. 4–7.

[41] See *ibid*. Common shorthand for this second principle is "proportionality of civilian collateral damage."

[42] *Ibid*. Other law-of-armed-conflict principles and restrictions exist, but are not central to a discussion of infrastructure defense.

with less suffering and loss of life, property and resources, this third principle would counsel for its use. From the standpoint of military necessity, information operations may be promising alternatives to physical attacks in wartime because of their potentially lower lethality and destructiveness.

Precision-targeted information operations, for example, may disable combatant computer systems, encouraging the enemy to surrender without further harm. Difficulties in homing in exclusively on combat uses of non-combatant infrastructures, including unknown or unexpected links among information systems, may make such information operations impractical in the short term. On the other hand, even less discriminate information operations or physical attacks would still be permitted if they were more effective at bringing about enemy submission at a given level of collateral damage.

Cyber attacks can have results similar to the goals of psychological operations. Sun Tsu said, "Those skilled in war subdue the enemy's army without battle." Commenting on Sun Tsu's strategy, Griffith explains, "Never to be undertaken thoughtlessly or recklessly, war was to be preceded by measures designed to make it easy to win. The master conqueror frustrated his enemy's plans and broke up his alliances. He created cleavages between sovereign and ministers, superiors and inferiors, commanders and subordinates. His spies and agents were active everywhere, gathering information, sowing dissention, and nurturing subversion. The enemy was isolated and demoralized; his will to resist broken. Thus without battle his army was conquered, his cities taken and his state overthrown. Only when the enemy could not be overcome by these means was there recourse to armed force."[43] Were there computers in 400 B.C. (the period Sun Tsu describes is uncertain so the date is merely to give a general perspective) Sun Tsu would have enthusiastically adopted them.

Defensive capabilities will be a critical aspect of cyber deterrence, to a much greater extent than was the case in the strategic nuclear confrontation of the Cold War. Warning systems, both strategic and tactical, are central to cyber deterrence. Without them, and the near-real time response they potentially enable, cyber attacks are certain to succeed eventually as attackers learn and defenders are mired down by the vastness of their systems. In this regard, cost-imposing strategies are important if they can make the probe-and-prepare-in-advance character of cyber attacks more difficult.

Strategic and tactical warning in cyber conflict can provide elements of deterrence through the ability to influence adversary perceptions. Cyber war-fighting, more akin to crisis management than conventional conflict, is possible at a low level of physical violence. An important cyber response capability is near-real time control of network connectivity.

[43] *"Sun Tsu and the Art of War,"* translated and with an introduction by Samuel B. Griffith, Oxford University Press paperback, London (1973) pg. 39.

POSSIBLE POLICY DECLARATIONS

One type of declarations are those that establish a line past which we warn others not to venture. Drawing lines in the sand is treacherous, however, because they imply that anything not over the line is acceptable. Further, such a declaration must imply or define a threatened response, one intended to be serious enough to dissuade an attacker from the behavior defined. That carries with it the issue of U.S. credibility. Have we responded the way we threaten in similar situations in the past? It also binds the U.S. to do something, or the U.S. loses future credibility.

Another define normative behavior, goals we believe should serve as universal standards for all. Such declarations define ideal states that perhaps only a few states meet. There should be some reason to believe the proposed goals are realistic, as illustrated by the existence of at least some examples. As noted earlier, there should be some feasible path through which wider adoption can be facilitated. Because they call for changes in behavior, they must be viewed as long-term matters, but are important enough that any progress in these directions will be beneficial.

A third type of declarations serve to note ambiguous or unclear situations where further discussion and study is needed. These may be situations that identify matters requiring both domestic and international efforts. Or they can take the form of a statement such as "The U.S. supports X under condition Y."

In the following ten possible declarations are suggested to encourage discussion of how declaratory policy might be employed in deterring cyber conflict. They are presented in an order from the least controversial to those that are likely to engender the most reluctance.

The set can be viewed as a logical package. All, individually and as a group, would aid in protecting users of the cyber commons, making it a safer place for the conduct personal and national business. But they are not inextricably linked. In this sense the set is a menu from which to select based on domestic and international priorities.

1. Research and development of information technology should remain unfettered so that the greatest benefits can be secured for the well-being of all. To this end, potentially dangerous aspects of information technology should be openly discussed and international efforts undertaken to avert possible harm to all states and peoples.

Despite its flaws, it is clear that information technology has made major beneficial changes for people and for facilitating their interaction to exchange knowledge and to undertake economically important activities. This declaration simply says do not kill the goose that is laying the golden eggs. It is intended to head off the control or limitation of research and development in information technology. It does say, however, that the dark sides of the technology, the misuse of the technology and the abuse of the cyber commons, is a problem and it calls on all states to openly discuss the issues and to discuss and cooperate on solutions.

Openly discussing the problem will be more difficult than one might expect. Cyber flaws are concealed to the extent possible. Matters of fault, liability, and loss of trust are part of the problem. Avoidance of national blame is another. Much is concealed under the rubric of national security, some quite justified, as when it would reveal vulnerabilities that could be more widely exploited, and some covered up to minimize unrelated political problems.

So this is a two-sided declaration, one to not fetter the technology, but also a call to open discuss the problems, both technical and procedural that impact security.

The next declaration related to the facilities and operators of global public communications network.

2. Computer and information system resources connected by public international telecommunications facilities are critical for global discourse that is a human right and provide a common good from which all benefit. To this end, the availability of these open information resources to legitimate users should not be impeded.

This is consistent with the vision of the International Telecommunication Union, to which the U.S. is a signatory, that states "By connecting the world and fulfilling everyone's fundamental right to communicate, we strive to make the world a better and safer place." It is a direct repetition of a principles regulating international communication going back to the earliest days of wire and radio telegraphy. There is a good body of internationally accepted behavior: non-interference with legitimate users; prior rights of incumbency; state control of what comes into its jurisdictions through the licensing of operators; and an obligation to help users in distress, either to provide back-op facilities or to identify sources of interference.

A recent NRC report notes "Users of information technology …should be able to use the computational resources to which they are entitled and [the] systems that depend on these resources."[44]

The declaration goes further, however, in that it declares open and unrestricted use of the public telecommunications facilities is a human right. This applies only to the public communication system, defined as the set of state-licensed carriers operating under the aegis of international communication agreements. There is flexibility in the declaration, in the word "legitimate." States are free to define "legitimate users" however they choose, but they should not interfere with the legitimate users of other states. Thus states

[44] Seymour E. Goodman and Herbert S. Lin, Ed., *Toward a Safer and More Secure Cyberspace*, The National Academies Press, Washington, D.C. 2007, p. 53 item I in a Cybersecurity Bill of Right, Chap. 3.s.

maintain control of what their citizens do, but not what users over whom they have no jurisdiction can do.

The next two declarations begin to cut closer to the matter of identifying sources of abuse of the public network, particularly that where the traffic is between computers.

> 3. Users of public international telecommunication facilities should, for the protection of all users, have a unique identifier supported by a verifiable mechanism available to them so that parties sustaining harm through misuse of those facilities can seek redress.

Attribution is impeded by the almost complete anonymity possible on the Internet and related TCP/IP networks. On the other hand, in many states this proposal would meet strong objections on grounds of privacy. In view of greatly varying needs for both privacy and security and the sensitivity of content of communications, it will be helpful to shift the security–privacy tradeoff to the user. The point of the declaration is to provide means for redress in the event of harm. Users willing to accept communications from unidentified users would do so at risk of denying themselves redress for consequent harm. The unique identifier may be made available only by user request in the case of alleged harm suffered and be provided subject to the laws of the jurisdiction within which the harm occurs.

Unspecified here is the definition of "harm." Harm is culturally and politically dependent and it is unlikely that there will soon be global agreement on what is allowed and what is harmful and should be prohibited. By leaving harm undefined, the default definition is the way it is defined in the jurisdiction in which the harm is seen to have occurred. As in all cases where adjudication of claims is necessary, harm will in the end be defined by precedent and developing case law.

> 4. States shall establish a system of technical standards openly arrived at for all equipment attached to the public infrastructure, and the adequacy of those standards monitored though proof of performance publicly available.

This is in analogy to what is mandated in all systems, public or private. The integrity of the network requires that there be technical standards relating to what can and can not be connected to the network. Whether one is talking about data formats, voltages, or pipe pressures, there must be limits set by the design conditions used as a basis for constructing the system. Engineers can design for wide ranges of operating conditions; they can provide alternatives to take care of special situations; and older devices are replaced over time by newer and more fault-tolerant versions. But "anything-goes" is not technically feasible.

This can be accomplished in various ways. In the case of regulated infrastructure systems, there can be central certification laboratories. In the U.S. telecommunications systems much of this has been made a responsibility of the manufacturer with provision for verification of the process as needed. Another powerful technique is provided by markets. Error-prone, unreliable, and inflexible devices disappear from the market. Each jurisdictions will have its own certification mechanisms. International standards bodies help a great deal. International inconsistencies can be dealt with through standing or new resolution procedures.

The point is to address faulty hardware, such as might be the result of building in vulnerabilities during the manufacturing process to provide attack channels, or it could be applied to address embedded or bundled software containing malware. There are precedents in some classes of equipment such as medical devices where faulty software can result in unsafe operation.

The next two declarations are a set intended to address current practices that render public telecommunication networks insecure.

> 5. The distribution of malicious software is incompatible with the free and beneficial use of public international telecommunications facilities. All nations shall undertake efforts to eliminate such activities within their jurisdictions that violate the rights of people everywhere, or they can be held complicit.

Malware is produced somewhere, in some state's jurisdiction. This does not say that malware production is prohibited, for there are many reasons why malware might be produced: for defensive R&D, as an intellectual puzzle, as a student exercise in computer security training, and as a form of free speech. What the declaration says is that its *distribution* is prohibited. The declaration then says it is the responsibility of each state to prevent the distribution of malware. Clearly this can only refer to international distribution. A state is free to allow its citizens to suffer from domestically-produced malware if it chooses.

> 6. Seeking and/or obtaining unauthorized access to or control of computers outside the jurisdiction of a state shall be prohibited. States shall be expected to undertake actions to prevent such unauthorized access from within their jurisdiction, or they may be held complicit, and they shall be required to render assistance to states who have detected such unauthorized access.

This declaration addresses botnets. They are to be prohibited, and like the malware declaration, their detection and elimination is a matter for each state to accomplish within its own jurisdiction. But the prohibition is only when a computer in another jurisdiction is captured. A state is responsible for what it allows its citizens to do and that is mediated by its own laws. As with malware, a state that allows its citizens to capture a computer in another state and fails to prevent or eliminate the violation can be held complicit. What the declaration goes on to say is that regardless of the local *mores*, a state is required to render assistance when other states become aware of the intrusion into a computer in their jurisdiction.

The next four declarations address circumstances where cyber conflict through the facilities of the public telecommunication network is the issue.

7. In the event an attack, consisting of placing malicious software in the computers of another sovereign state, is detected by the target state, the attacker shall be required to remove the offending software under such terms of verification as mutually agreeable to target state and attacker state. All states shall assist in determining the origin of such malicious software when called upon by the state detecting such software.

This declaration relates to a characteristic of cyber attacks that is quit different from attacks employing conventional or nuclear force. While all attacks require a great deal of planning and preparation, conventional and nuclear attacks announce themselves in a very obvious way, and with very direct means of attribution. The use of cyber force involves that the attacker violate the sovereignty of the target state long in advance. The attacker must probe the computer networks to be attacked to determine what vulnerabilities will be exploited. Malicious code will be inserted into the systems to be attacked. Viruses can be released that can wait for a signal to initiate the attack. Insiders may have been recruited and placed in critical locations. These may be active in providing current information or they may be sleepers.

The upside of this is these advance software preparations can be detected by the target nation in advance of the attack. It may be in the interest of both parties to restore the pre-attack conditions as quietly as possible, in essence a no-harm-no-foul response. The declaration says a state can respond in such a case with cyber or other forms of force if it chooses, but an alternative resolution may be to require the offending state to withdraw its software, and to inform the injured state of the nature and location of the malicious software.

This leads to a cat-and-mouse game. What does the injured party know and can the attacker leave some of it software agents in place. If a state knows the attacker has not been fully compliant, do they call the attacker on it, revealing sources and methods, or does the state leave the software in place an monitor it, or even "double" it? Implicit is the ability to detect malicious but passive software. At a minimum what will be needed is that all software carry a digital signature and that all computers on the network be clean *ab initio*. In essence this reduces monitoring software environments to the equivalent of public health monitoring.

This recognizes that cyber conflict is not a matter of sudden violence but is much more like traditional intelligence operations, with move and counter move. Cyber conflict will consist of continual moves, not episodes of violence. To this end the current role of NSA in the newly created Cyber Command is well advised.

The next declaration returns to the matter of attribution. A previous declaration called for assistance in identifying the source, at least to the point of state origin and of the states through with attacks are mounted. The declaration is phrased in terms of the U.S. but it can easily be generalized .

8. In the event the U.S. suffers a cyber attack of national significance that threatens its economy and security, it will undertake to ascertain the circumstances that enabled it. All states are called upon to assist in this determination. The U.S. will hold any states it believes to be complicit in the attack subject to such responses as are within its capability. An attribution of complicity can include all states whose communications facilities were wittingly employed in the attack or were employed through the negligence of a state to prevent such electronic communications from it.

This declaration says several things. First all states are called upon to assist in determining attack attribution. It says the U.S. can respond by any kind of force within its capability. But then it takes a draconian position, that any state whose telecommunication facilities were employed in the attack *can* be held complicit. "Can" allows the U.S. to let truly innocent states, innocent in its view of course, off the hook. But what it really means is that all states are responsible for seeing that attacks do not use their telecommunications facilities unimpeded. Some states will lack the resources to do adequate monitoring. The novelty of the attack may truly astound all. But it says that if states are to benefit from advances in information and communication technology, they have a corresponding responsibility to police their neighborhoods.

9. A state is entitled to seek information for the purpose of warning of a planned or impending electronic communication attack. It may do so it any way possible provided it does no harm to any states holding that information.

This declaration is, in essence, about what is euphemistically called cyber exploitation, aka known as intelligence collection. Given the continual nature of cyber conflict, and the need for an attacker to pre-place software, it says that a defender should not only look within his own computers for attack warning, but should look for attack preparations in the computers of potential attackers. This is, in practice, no different from intelligence collection. But in the set of possible declarations it is best made explicit. The "do-no-harm" condition is what intelligence collectors do anyway, since one never want a target to know what one has found out about him.

10. A strategic attack on the U.S. employing an electronic communication attack will be considered a use of force under Articles 41 and 42 of the UN Charter. The U.S. will be entitled to undertake self-defense through "such action by air, sea, or land forces as may be necessary to restore international peace and security."

This is the only "line-in-the-sand" declaration in the group. In one sense it says the obvious, that an attack of national significance will be taken for what it is, an attack by a sovereign state which will trigger a justified self-defense response. What is a departure from current policy is that it puts cyber force in the category of force to which an armed response is justified. The quote is from the UN charter.

Assessing the Potential Utility of the Declarations

The ten declarations are related to the cyber conflict issues raised in Part A:

1	Protection of cyber R&D	Technology aids defense as well as offense; proposes not to restrict it at this early stage in its development
2	Availability of public telecommunications resources	Proposed as a human right for personal and economic benefits
3	Identity management	Addresses the current anonymity on the public telecommunications network that defeats deterrence by impeding responses
4	Technical standards for network attachments	Addresses the need for assurance that devices, when first connected to the public telecommunications network are free of malware
5	Ban malware distribution	Malware is a cyber weapon that should be eliminated through actions by each of the states in the part of the Internet over which they have jurisdiction
6	Ban botnets	Botnets are the cyber weapon delivery system that should be eliminated through actions by each of the states of the part of the Internet over which they have jurisdiction
7	No-harm-no-foul conflict termination	Proposes a termination process that can be effective before the initiation of cyber conflict
8	Attribution of attacker	Establishes right of a state to seek information relating to attack attribution and to hold complicit states used as transit for the attack
9	Enables early warning activities	Provides a way to prevent damage pre-attack through preemption and trans-attack through damage limitation
10	Defines justification for self-defense against use of cyber force	Establishes the circumstance under which a state can avail itself of its right to self-defense

Stepping back to understand the relative importance of the ten proposed declarations, the following structure emerges:

Declarations #2, 8, and 10 are the central core. The keystone is Declaration #2, the assertion that the availability of the public telecommunication network is a right that should not be abridged. It recognizes that a state can define the terms of access for its citizens, but denies that any state can define the access available to citizens of other jurisdictions. Declaration #8 is the matching statement of the responsibility that must be discharged if a state is to avail itself of the right of access for its citizens in Declaration #2. Declaration #10 defines the conditions under which a state can justify self-defense in the case the right of access to the public telecommunications network is denied or harm is sustained though the malicious actions of another. The definition of “harm” is left to the state that sees itself as a victim, but in invoking such a right the merit of its complaint will ultimately be judged by its peers and the public.

The next set of Declarations, #5, 6, and 1 relate to the regulation of cyber “weapons.” The first two suggest what should be prohibited through actions of each state exercising its responsibility for the cyber commons within its jurisdiction while Declaration #1 warns that cyber technology *per s*e should not be limited, despite its downsides, because of its substantial upsides.

Declaration #7 proposes a conflict termination process that can be helpful in controlling escalation of cyber conflict.

Declaration #9 establishes the right of a nation to assure itself that other states are not preparing to launch a cyber attack. There are two aspects to this right. The first is that a nation should look inside its own computers, not those of others, because that is where the early warning evidence will be found. How this is done can constitute a privacy violation absent further definition of the process. One possibility is to extend personal identifiers to computers, with communications from those not "cleaned" so labeled in the same way unidentified users are apparent. The declaration implicitly recognizes that intelligence collection will be a part of a warning process as well. This is already a well-established "right" subject to the consequences a state risks if discovered.

The remaining two Declarations, #3 and 4, address implementation measures that will reduce the ease with which cyber attacks can be carried out. In effect they raise the bar for successfully initiating cyber conflict and are, in effect, a mild form of cyber "arms limitation."

The ten declarations can be assessed against the four characteristics proposed as measures of their potential for becoming part of multilateral agreements.

	DECLARATION	VERIFIABLE	RECIPROCAL	ROBUST	CONSISTENT
1	Protection of cyber R&D	Y	Y	Y	Y
2	Availability of telecommunications resources	Y	Y	Y	Y
3	Identity availability	Y	N	N	Y
4	Technical standards of network attachments	Y	Y	N	Y
5	Ban malware distribution	Y	N	Y	Y
6	Ban botnets	Y	N	Y	Y
7	No-harm-no-foul conflict termination	N	N	Y	Y
8	Attribution of attacker	Y	N	Y	Y
9	Enabling early warning activities	Y	N	N	Y
10	Self-defense against cyber force	Y	N	Y	Y

Shown are some judgments regarding the degree to which the proposed declarations will meet the four conditions of being verifiable, whether all nations are likely to agree to the proposed limits on their activities, being robust under technical change, and being consistent with earlier international agreement that have been widely adopted in the past. "Y" indicates the characteristic is probably consistent with those metrics. "N" means it is not obvious if all. government would accept such a limitation on its freedom of action.

The most promising are the declarations for protection of R&D and the right of access to the global telecommunications system. The other eight declarations are problematic in varying degrees since they are likely to be seen as limiting future technical options for national security or commercial market positions. The easiest condition to satisfy is that of consistency with existing agreements, but this should not be surprising since the declarations proposed were formulated as logical extensions of existing international understandings.

The negatives in the above table should not be cause for discouragement. Declaratory policies are long-term enterprises. One chips away where one can and hopes that as time passes the need for the protections proposed will be more widely accepted. As a practical matter, the Internet is heavily influenced by the larger states so that even limited multilateral agreements can leverage a great deal of effective action. While not wishing ill, the frequently alarms over Pearl Harbors and 9/11 may have to occur before leaders and followers appreciate the seriousness of a wired global economy.

There remains the matter of plausible implementation processes. In much of the current discussion, there seems to be an acceptance that the problem of cybersecurity is too big for any but governments. The enumeration of the difficulties then proceeds to point our that most of the world's cyber assets are privately owned, and that most owners see security as a cost rather than as a profit center. So the logic goes, not a great deal of substance will really happen.

This downward spiral into chaos need not be the way to read the situation. Governments are inevitably limited in what they can do: appropriations must compete with other needs; regulation is resisted; too strong a government hand is seen as big government and incursions on civil liberties and privacy. On the other hand, private owners of facilities and services can set their own rules, beholden only to market and shareholder expectations. This argues for purely private solutions. At each step those solutions will be limited but as the security situation worsens, more effective solutions will demanded, and accepted, not because of government action but by market demands.

This the oft-repeated calls for "public–private" partnerships may be counter-productive, especially when each waits for the other to take action. Instead of private owners asking government what rules they must accept, faster progress may be possible if private owners tell governments what they need. It would seem to be worth a try. Meanwhile. The government can secure its own networks, fund the R&D it needs, and establishes a market for strong security solutions. The declarations proposed can serve as directions for private actions. At the same time, voluntary technical standards, using the Internet, and its social networks, as mechanism to encourage public and private exchange of solutions, and encouraging legally acceptable self defense can be effective.

THE BOTTOM LINE

Deterrence, on the Cold War retaliation model, is unlikely to be effective in dealing with cyber force. This model is a dead-end and continuing to pursue it simply distracts smart people from doing something more useful. Deterrence itself is not impossible, but it must be based on broader concepts than retaliation and punishment.

Sub-state actors are not subject to deterrence based on threats of retaliation. They currently attack sovereign states, nuclear and non-nuclear, with impunity. Treating states and sub-state groups with a one-size-fits-all approach will result in addressing neither as well as they might.

Defense in cyber conflict is a critical part of cyber deterrence. It includes strategic and tactical warning, situation awareness, cyber order-of-battle, and the collection, retention, and analysis of cyber incident forensics.

Cyber force is quite unlike conventional force and nuclear force. It can be "soft" in its effects, extended in time, and cumulative in its impact. Cyber attacks are not simply to be seen as the equivalent of strategic bombing but without the aircraft.

An important element of cyber defense will be real-time control of network connectivity. The cyber security problem arises from connectivity. Control of connectivity needs to be part of the solution.

Shared voluntary private efforts can contribute to cyber situation awareness and can provide a useful element of real-time cyber defense.

Declaratory policies are not ends in themselves. It is a beginning of a lengthy campaign to further a vision of a desired future. Declaratory policies are only useful to the extent that they leverage other forces and mechanisms. They are seeds, not trees.

ACKNOWLEDGEMENTS

Part of the work reported here was supported by a grant from SAIC to the Georgia Institute of Technology Center for International Security, Technology, and Policy. The discussion of sub-state attackers in Part A is taken from that work by Rebecca Givner-Forbes, whose assistance is gratefully acknowledged.[45]

The author also wishes to thank the following reviewers who have provided helpful advice and guidance for developing this or earlier drafts: Dave Elliott, Sy Goodman, Tony Rutkowski, John Savage, Al Buckles, Michael Schrage, Greg Grove, and Tom Seivert.

[45] The full-text can be found in Stephen J. Lukasik and Rebecca Givner-Forbes, "Deterring The Use of Cyber Force," December 14, 2009. See <www.cistp.gatech.edu/publications/files/cyber_deterrencev2.pdf>.