EJLT European Journal of Law and Technology

Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity

Reich, P.C., Weinstein, S., Wild C., & Cabanlong A.S., [1]

Cite as: Pauline C. Reich, Stuart Weinstein, Charles Wild & Allan S. Cabanlong, Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity in European Journal of Law and Technology, Vol. 1, Issue 2, 2010

Abstract

In this paper, the authors undertake a study of cyber warfare reviewing theories, law, policies, actual incidents - and the dilemma of anonymity. Starting with the United Kingdom perspective on cyber warfare, the authors then consider United States' views including the perspective of its military on the law of war and its general inapplicability to cyber conflict. Consideration is then given to the work of the United Nations' group of cyber security specialists and diplomats who as of July 2010 have agreed upon a set of recommendations to the United Nations Secretary General for negotiations on an international computer security treaty. An examination of the use of a nation's cybercrime law to prosecute violations that occur over the Internet indicates the inherent limits caused by the jurisdictional limits of domestic law to address cross-border cybercrime scenarios. Actual incidents from Estonia (2007), Georgia (2008), Republic of Korea (2009), Japan (2010), ongoing attacks on the United States as well as other incidents and reports on ongoing attacks are considered as well. Despite the increasing sophistication of such cyber attacks, it is evident that these attacks were met with a limited use of law and policy to combat them that can be only be characterised as a response posture defined by restraint. Recommendations are then examined for overcoming the attribution problem. The paper then considers when do cyber attacks rise to the level of an act of war by reference to the work of scholars such as Schmitt and Wingfield. Further evaluation of the special impact that non-state actors may have and some theories on how to deal with the problem of asymmetric players are considered. Discussion and possible solutions are offered. A conclusion is offered drawing some guidance from the writings of the Chinese philosopher Sun Tzu. Finally, an appendix providing a technical overview of the problem of attribution and the dilemma of anonymity in cyberspace is provided.

1. The United Kingdom Perspective

> "If I went and bombed a power station in France, that would be an act of war. If I went on to the net and took out a power station, is that an act of war? One

> could argue that it was." [2]
>
> "If someone bombed the electric grid in our country and we saw the bombers coming in it would clearly be an act of war. If that same country uses sophisticated computers to knock out our electricity grid, I definitely think we are getting closer to saying it is an act of war." [3]

Lord West of Spithead believes that foreign states and terrorist groups are regularly launching cyber-attacks on the UK's computer systems with the potential to cause widespread damage. [4] He said there had been "300 significant attacks" on the government's core computer networks in the last year and warned of chaotic scenes if one successfully targeted infrastructure such as the UK's communications systems. [5] Lord West goes on to indicate:

> There is no doubt some state actors have sucked out huge amounts of intellectual copyright, designs to whole aero engines, things that have taken years and years of development. The moment you mention a particular state, they will deny it. The problem with cyberspace is that attribution is extremely difficult. It's almost impossible to do it in terms of evidence that would be necessary in a court of law. [6]

A digital attack against the UK causing even minor damage would have a "catastrophic" effect on public confidence in the government according to the UK's Government Communications Headquarters' Cyber Security Operations Centre (CSOC). [7] The warning forms part of a preliminary "horizon scanning" report produced by the new unit, CSOC, whose job it will be to continually monitor internet security, producing intelligence on botnets, denial of service attacks and other digital threats to national security. [8] According to CSOC, one of the problems hampering the prevention of cyber attacks is that an internationally agreed definition of cyber warfare remains elusive, with state actors making increasing use of hired criminals and 'hacktivists' to carry out deniable cyber attacks on their behalf. [9]

2. United States Views

2.1. Martin Libicki

> "The establishment of the 24 th [US] Air Force and U.S. Cyber Command marks the ascent of cyberspace as a military domain. As such, it joins the historic domains of land, sea, air, and space. All this might lead to a belief that the historic constructs of war-force, offense, defense, deterrence - can be applied to cyberspace with little modification. Not so. Instead, cyberspace must be understood in its own terms, and policy decisions being made for these and other new commands must reflect such understanding. Attempts to transfer policy constructs from other forms of warfare will not only fail but also hinder policy and planning". [10]

Lord West's viewpoint differs significantly from that of Martin Libicki, the author of The Rand Corporation's 2009 study for the United States Air Force entitled *Cyberdeterrence and cyberwar,* and many other significant works about cyber policy [11]. Libicki's monograph discusses "the use and limits of power in cyberspace, which has been likened to a medium of potential conflict, much as the air and space domains are." [12] He urges the military and civilian policymakers to look at the operational realities behind the phrase "fly and fight in cyberspace." [13]

In doing so, Libicki draws the following conclusions. Cyberspace is its own medium with its own rules. Cyber attacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Permanent effects are hard to produce. The medium is fraught with ambiguities about who attacked and why, about what they achieved and whether they can do so again. Something that works today may not work tomorrow (indeed, precisely because it did work today). Thus, deterrence and war fighting tenets established in other media do not necessarily translate reliably into cyberspace. Such tenets must be rethought. [14] Libicki's 2009 monograph is an attempt to start this rethinking.

Libicki sets out his own view of what constitutes an act of war in Cyberspace. [15] Starting with traditional definitions of what constitutes an act of war, Libicki states that what constitutes an act of war may be defined in one of three ways: universally, multilaterally, and unilaterally. [16]

2.1.1. Universal Definition

A universal definition is one that every state accepts, such as when the United Nations says that something is an act of war. [17] The next-closest analog is if enough nations have signed a treaty that says as much. [18] Unfortunately, as far as cyber war goes, Libicki concludes that no such United Nations dictum exists, and no treaty says as much. [19] "One might argue that a cyber attack is like something else that is clearly an act of war, but unless there is a global consensus that such an analogy is valid, a cyber attack cannot be defined as an act of war." [20]

2.1.2. Multilateral Definition

According to Libicki, a cyberattack (with specified characteristics) can be seen as an act of war if a set of states has so defined what is meant by cyberattack. He focuses on NATO, the most obvious such organization, and its failure to declare that the 2007 attack on Estonia merited invocation of the treaty's collective-defense clauses. [21] Libicki noted here however that the problem of attribution made it difficult for NATO:

> Had NATO declared that the attack was actionable, it might have served as a warning to potential attacking states, but whether they would have felt that this constituted a legitimate definition would be another matter. NATO would react to a cyber attack as it so declared, and the attacker would react to NATO's reaction as it deemed in its best interest. Legitimacy may play a role if the attacker did not believe that a cyber attack was as serious as a real attack and did not want NATO's reaction to serve as the last word on the subject. [22]

2.1.3. Unilateral Definition

Finally, there is the third scenario in which "any state can unilaterally declare that a cyber attack (of certain characteristics) is an act of war." [23] Such a declaration may be found reasonable by some states as an act that they may find reasonable, legitimate, and actionable, while others may not agree. [24] Libicki points out that "potential attackers may or may not take such a declaration seriously". [25] However, according to Libicki, "if the state responded to a cyber attack by retaliating, those skeptical of the claim might regard the response as illegitimate if it used a different modality from that of the attack itself." [26]

Interestingly, in his analysis of the power station falling victim to cyber attack, Libicki disagrees with Lord West's analysis:

> Consider the following two vignettes. In the first, a rogue state, acting through a cutout (e.g., a phony engineering consulting firm), sends a manual to an electric power operator that persuades him to react to a thunderstorm by setting switches incorrectly. This error plunges the city into a week-long blackout and fries several hard-to replace transformers. Dastardly perhaps, but this would probably not be regarded an act of war. In the second scenario, a rogue state employs a hacker to break into a computer system to change its instructions so that it reacts to the normal parameters of a thunderstorm (e.g., downed tree limbs severing power lines) by setting switches badly. The same effects result. If the first vignette is not an act of war, why would the second be? [27]

Libicki suggests that the answer as to whether a particular attack is an act of war comes down to whether it is in the interest of a state to declare a particular as such: "Would a country be better off having an explicit cyber-deterrence policy or maintaining its current implicit cyber-deterrence policy (that is, reserving a general right to retaliate at a time and in a manner of its choosing should it be deliberately hurt badly enough)?" [28] Interestingly, a nation state making use of an explicit cyber-deterrence policy may find its options limited because it has made such a public stance:

Deterrence is in the mind of the potential attacker. What better way to persuade such attackers of the risks of aggression than by saying so in clear terms? Unfortunately, an explicit policy removes the purity of separating the easy cases ("we know who did it, and we can hit back") from the hard cases ("we are not sure about either") because others-attackers and third parties alike-will not be able to distinguish easily between unwillingness to retaliate and inability to know against whom or how to retaliate. Thus, a cyber attack that does not engender a response can undermine the credibility of the state with an explicit retaliation policy. [29] Lord West has suggested in the past that we make use of "hackers" to work for the state and show us our own defence weaknesses.

Do the use of military jargon and the strategic debates left over from the Cold War really add to the cyber-warfare discussion? In addressing the issue of a proper response to a cyber-attack, do we fall victim to the cliché of becoming "arm-chair" warriors? When does a cyber-attack that may or may not be sponsored and supported by another nation cross the line and become an official act of war? At what point should a state become

responsible for non-state actors within its territory? And for nations reliant on the Internet and other ICT modalities that are the primary victims of these attacks, what should the rules of engagement be when faced with the onslaught of rival countries determined to probe weaknesses and wreak havoc on other countries' critical information infrastructures? Is it productive for a nation such as the United States or the United Kingdom to adopt a pro-active approach to cyber warfare? [30]

What should the rules of engagement be for nations to take with respect to taking action via law or technology or other measures (trade embargoes, for example) against other countries that attack or spy through cyberspace? Is it technologically feasible to do so to protect private sector and/or critical information infrastructure networks? Would it be effective in terms of national interest to do so rather than to engage in conflict in cyberspace or traditional warfare? Does a democracy have to wait until it is attacked by foreign actors before it may take aggressive measures to protect its critical information infrastructures?

3. U.S. Military Perspectives on the Law of War and Its General Inapplicability to Cyber Conflict

3.1. Walter Gary Sharp, Sr.

Dr Walter Gary Sharp, Sr. is currently Senior Associate General Counsel for Intelligence, Office of the General Counsel, U. S. Department of Defense and Adjunct Professor of Law, Georgetown University Law Center, and Judge Advocate, U.S. Marine Corps (Retired) and a pioneer in the area of cyberspace and military/national intelligence issues. [31] [32] Dr Sharp who is widely cited in U.S. military law circles wrote in 1999 stating that "the open architecture of the Internet is ideally suited for asymmetrical warfare, corporate espionage, and criminal activity." [33] Emphasizing the vulnerability of states, private industry, and individuals from the information they voluntarily post on the Internet or from unauthorized access of their information systems, Sharp warns of the threat that asymmetric players [34] can have in the CyberSpace environment. "Dedicated and persistent CyberSpace [35] actors such as recreational hackers, corporations seeking a competitive advantage, organized criminals, terrorists, and states can now gain access to almost *any* Internet-linked information infrastructure in the world." [36] "Execution of an organized, large-scale attack against a state or a business can begin anonymously with the stroke of a single key on a computer keyboard, with commands being delivered around the world literally at the speed of light" quoting Sharp [37].

In *Cyberspace and the Use of Force* [38], Gary Sharp "delineated those peacetime state activities falling within the information highway that constitute an unlawful threat or use of force and examined the circumstances under which states have the right to use force in response to such a threat or use of force." [39] Being amongst the first scholars to point out that information technology is both redefining national security and the use of force by states, Sharp argues "that computer espionage, computer network attacks, as well as the subversion of political, economic, and/or non-military information bearing on a nation's capabilities and vulnerabilities may well constitute an unlawful use of force in cyberspace

under traditional international law principles." [40]

3.2. Keith Alexander

3.2.1. Rules of Engagement

General Keith B. Alexander, US Army, is the Commander, US Cyber Command (USCYBERCOM) and Director, National Security Agency/Chief, Central Security Service (NSA/CSS), Fort George G. Meade, Maryland. [41] As the Director of NSA and Chief of CSS, he is responsible for a Department of Defense (DOD) agency with national foreign intelligence and combat support responsibilities. NSA/CSS civilian and military personnel are stationed worldwide. [42] As Commander, USCYBERCOM, General Alexander is responsible to plan, execute and manage forces for coordinating Department of Defense computer network attack (CNA) and computer network defense (CND) as directed by US Strategic Command. [43] He was confirmed as Commander USCYBERCOM on 7 May 2010.

General Alexander "has warned Congress that policy directives and legal controls over digital combat are outdated and have failed to keep pace with the military's technical capabilities". [44] He also stressed that computer network warfare is evolving so rapidly that there is a gap between the military's technical capabilities and legal controls over digital combat and what he calls a "mismatch between our technical capabilities to conduct operations and the governing laws and policies." [45] In unclassified written answers to questions sent to him by prior to his confirmation hearing, General Alexander wrote: "If confirmed, I will operate within applicable laws, policies and authorities." [46] General Alexander further pledged that "I will also identify any gaps in doctrine, policy and law that may prevent national objectives from being fully realized or executed." [47] General Alexander noted that there was no theory of deterrence to guide planning for cyber warfare similar to strategies that guided nuclear planning in the Cold War, and that it remained difficult to assess exactly who carried out an attack over computer networks. [48] General Alexander asserted that commanders have clear rights to self-defense, and that while "this right has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in cyberspace, as long as it complied with law of war principles... would be lawful." [49]

At his confirmation hearing, General Alexander explained through a series of responses to hypothetical questions presented by Senator Carl Levin of Michigan who is the Chair of the Armed Services Committee the complexities of operating cyber defense in line with traditional rules of engagement:

3.2.2. Support during a traditional armed conflict

> *Levin:* Assume the following: That U.S. forces are engaged in a traditional military conflict with a country - we'll call it Country C - now how would you conduct cyber operations in that country in support of the combatant commander? Under what authorities, processes, and borders would you be operating in that particular scenario?
>
> *Alexander:* We would be operating under Title 10 authorities [50] under an

execute order supporting, probably, that regional combatant commander. The execute order would have the authorities that we need to operate within that country and we'd have a standing rules of engagement of how to defend our networks. I think that's the straightforward case, [it] would be an execute order that comes down that regional combatant commander that includes the authorities for cyber [that] are parsed out and approved by the President.

3.2.3. The complexity of neutrality and third parties

Levin: Now the second hypothetical, I want to add a complicating factor to the scenario. Assume that an adversary launches an attack on our forces through computers that are located in a neutral country. That's what you determine - the attack is coming from computers in a neutral country - how does that alter the way you would operate and the authorities that you would operate under?

Alexander: So that does complicate it. It would still be the regional combatant commander that we're supporting under Title 10 authorities. There would be an execute order. In that execute order…the standing rules of engagement, it talks about what we can do to defend our networks and where we can go and how we can block. The issue becomes more complicated when on the table are facts such as: We can't stop the attacks getting into our computers, and if we don't have the authorities…we'd go back up to a strategic command, to the [defense secretary], and the President for additional capabilities to stop [the attack]. But right now the authorities would be to block it in theater in the current standing rules of engagement, and it would be under and execute order, and again, under Title 10 in support of that regional combatant command.

Levin: Is that execute order likely to have any authority to do more than defend the networks or would you have to, in all likelihood, go back for that authority…?

Alexander : It would probably have the authority to attack within the area of conflict against the other military that we are fighting, and there would be a rules of engagement that articulate what you can do offensively and what you can do defensively…what you would not have the authority to do is reach out into a neutral country and do an attack, and therein lies the complication for a neutral country…

Levin: And neutral being a third country presumably, is that synonymous or does the word neutral mean literally neutral?

Alexander: Well it could be either, sir, it could be a third country or it could be one that we don't know. I should have brought in [to the conversation] attribution, because it may or may not be a country that we could actually attribute [an attack] to, and that further complicates this. And the neutral country could be used by yet a different country, the adversary, and it's only a

path through. In physical space this is a little bit easier to see, firing from a neutral country, I think the Law of Armed Conflict has some of that in it. It's much more difficult and this is much more complex when a cyber attack could bounce through a neutral country…

3.2.4. The complicated case of homeland security assistance

Levin: Now a third scenario, more complicated yet. Assume you're in a peacetime setting [and] all of the sudden we're hit with a major attack against the computers that manage the distribution of electric power in the United States. Now, the attacks appear to be coming from computers outside the United States, but they're being routed to computers that are owned by U.S. persons located in the United States, the routers [are] in the United States. How would [Cyber Command] respond to that situation and under what authorities?

Alexander: That brings in the real complexity of the problem...because there are many issues out there on the table that we can extend, many of which are not yet fully answered. Let me explain: First, the [Homeland Security Department or DHS] would have the responsibility for defense of that working with critical infrastructure. [DHS] could through the defense report for civilian authorities [construct] reach out to the Defense Department and ask [for] support. And, sir, one of our requirements in the unified command plan is to be prepared for that task. So we would have that responsibility if asked to do that, again we'd get an execute order and we'd have the standing rules of engagement that we operate under all the time. The issues now [however] are far more complex because you have U.S. persons, civil liberties and privacy all come into that equation, ensuring that privacy while you try to, on the same network potentially, take care of bad actors. A much more difficult problem.

As a consequence you have a joint interagency task force, the FBI [that] has a great joint-cyber investigative task force that would be brought in, all of these come to bear. This is the hardest problem because you have attribution issues, you have the neutrality issue that we mentioned in the second scenario, you have [interagency groups] working together with industry, and I think that's one of the things that [President Barack Obama] is trying to address with DHS and with [DOD]: how do we actually do that with industry. That's probably the most difficult and the one that we're going to spend the most time trying to work our way through: How does the [DOD] help [DHS] in a crisis like that? [51]

Additionally, when directed, USCYBERCOM conducts full-spectrum military cyberspace operations in order to enable actions in all domains and ensure US/Allied freedom of action in cyberspace. Most recently in testimony before the US Congress on 23 September 2010, General Alexander outlined the difficulties faced by US Department of Defense:

Conflict in cyberspace, moreover, is highly asymmetric. Minor actors can afford

> and deploy tools to magnify their effects; witness the recent press reports about arrests in Europe of several individuals charged with creating the so-called "Mariposa botnet"-a collection of 13 million computers slaved together for criminal purposes. The tools these actors can employ are almost anonymous-a defender can sometimes learn where an attack came from, but can be time-consuming. That means "attribution" in cyberspace is costly and comparatively rare. The "price" an adversary pays for a capability-a tool or weapon-can be slight; the cost and impact borne by the victim of his attack can be very high. [52]

Speaking of the problem of attributing, General Alexander notes that it is very hard "telling one actor from another and divining actors' intentions":

> Not every event that affects our networks rises to the level of a national security threat. It is important to remember that hacking, spreading malware, and other malicious activities are crimes, defined domestically as well as internationally by the Convention on Cybercrime, and accordingly have legal consequences. Even if you spot an intrusion and you know it originated from an adversary, you usually cannot tell an intelligence operation from a military one. [53]

As part of the overall strategic plan of the US Department of Defense, emphasis must be placed on deterrence. General Alexander notes:

> Attacks by hackers and criminals can cause "nation-state sized" effects; indeed, the accidental "release" of malware might do the same, and the problem of attributing the attack to a particular actor similarly remains difficult to impossible. We have to study deterrence anew, from a variety of perspectives, and to gain clarity on our authorities. To take a thought from Sun Tzu, we must understand the cyber environment and, the capabilities of our adversaries, and our own abilities as well. This is not going to be easy, and it is not going to yield answers soon. If we know one thing from the Cold War, it is that stable deterrence can take years to achieve, and is the product of planning, analysis, and dialogue across the government, academe, and industry, and with other nations as well. Cyber deterrence will require progress in situational awareness, defense, and offensive capabilities that adversaries know we will use if we deem necessary. [54]

4. United Nations Role?

In July 2010, it was announced that a group of "cyber security specialists and diplomats representing 15 countries has agreed on a set of recommendations to the United Nations Secretary General for negotiations on an international computer security treaty." [55] The recommendations are as follows: On 30 July 2010, the United Nations Secretary-General transmitted the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ("Group").

The Group was established in 2009 pursuant to paragraph 4 of General Assembly resolution 60/45. [56] In that resolution, entitled "Developments in the field of information and telecommunications in the context of international security", the General Assembly requested that a group of governmental experts be established in 2009, on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as concepts aimed at strengthening the security of global information and telecommunications systems. [57] The Secretary-General was requested to submit a report on the results of that study to the General Assembly at its sixty-fifth session. [58]

The Summary of the Group's Report highlights the problems faced by the global community in dealing with the worldwide threat to information security:

> The growing use of information and communications technologies (ICTs) in critical infrastructure creates new vulnerabilities and opportunities for disruption. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Since ICTs are inherently dual-use in nature, the same technologies that support robust e-commerce can also be used to threaten international peace and national security.
>
> The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence, and they can act from virtually anywhere. These attributes facilitate the use of ICTs for disruptive activities. Uncertainty regarding attribution and the absence of a common understanding creates the risk of instability and misperception.
>
> There is increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. The growing sophistication and scale of criminal activity increases the potential for harmful action. While there are few indications of terrorist use of ICTs to execute disruptive operations, it may intensify in the future. [59]

The Summary concludes with a call for greater international cooperation between States, the private sector and civil society:

> Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. The report of the Group of Governmental Experts offers recommendations for further dialogue among States to reduce risk and protect critical national and international infrastructure. [60]
>
> The Group report calls for certain cooperative measures including devoting

significant "attention to non-criminal areas of transnational concern such as the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to State use of ICTs, which could affect crisis management in the event of major incidents." [61] Measures should be elaborated to "enhance cooperation where possible. Such measures could also be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability." [62] The report notes that "as disruptive activities using information and communications technologies grow more complex and dangerous, it is obvious that no State is able to address these threats alone." [63] Not only does the Report call for further collaboration among States, and between States, the private sector and civil society, but it also urges capacity-building to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security. [64]

The Group concludes the Report by recommending further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions:

i. Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure;

ii. Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;

iii. Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;

iv. Identification of measures to support capacity-building in less developed countries; and

v. Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25 (Resolution adopted by the General Assembly [*on the report of the First Committee (A/64/386)*] 64/25. Developments in the field of information and telecommunications in the context of international security). [65]

Some suggestions from the law community (from outside the above circles) have been for use of United Nations resolutions, for example, when there are cyber conflicts. [66] India, a strong supporter of the United Nations and its various initiatives, called for a United Nations resolution to declare certain groups to be terrorist organizations after the Mumbai 26/11 attacks and to be added to the UN list of terrorist organizations. Through that measure, and perhaps other international pressure, Pakistan declared certain groups to be terrorist organisations and officially banned them. [67]

5. Use of Cybercrime Law

Professor Dr Henrik W.W. Kaspersen (2009) in a draft discussion paper prepared for the Council of Europe [68] speaks of the jurisdiction issue that complicates the use of a nation's cybercrime law to prosecute violations that occur over the Internet:

> One need not be clairvoyant to predict that a facility of Internet that connects over 1.5 billion Internet users on this globe engaged in intense communications may not fit easily into the traditional legal approach on the assertion of jurisdiction as applied in the real and compartmented world of more or less static sovereign States. [69]

Kaspersen (2009) writes that while it is very clear that a sovereign State enjoys sovereignty over enforcing its own criminal law in its territory, what about the scenario where one state gathers on-line electronic evidence that is physically located in a computer in another territory but that is logically available - retrievable by means of software - to law enforcement authorities of another State. [70] Similarly a concern must be raised that the Internet may give rise to concurring claims of jurisdiction and thereby to conflicts of jurisdiction. [71] If more than one State asserts jurisdiction over a particular criminal act, a dispute or even a conflict may occur between the States involved. [72] In short, jurisdiction over the Internet limits the availability of domestic cybercrime laws as a tool to prevent cyber-attacks.

The case of Gary McKinnon, the British national with alleged Asperger's syndrome, whose "on-again, off-again" extradition to the US to stand trial for allegedly hacking into the Pentagon's computer network some eight years ago shows just how politically "dicey" decisions can be to extradite individuals to stand trial for alleged cybercrimes that whilst committed in one jurisdiction (UK) have an affect in another jurisdiction (US). [73] Should McKinnon be tried in the UK if his acts took place in the UK? Or does the fact that his alleged crimes were directed at the US military mean that the US Government has the right to try him in the US?

6. Actual Incidents and Limited Use of Law and Policy Resulting in Restraint - So Far

6.1. Estonia 2007

As has been well-documented in the popular and other media, Estonia was attacked from late April to early May, 2007. According to Jaak Aaviksoo, Estonia Minister of Defence, "most of the attacks were carried out against government servers and Estonian news portals, but also the two biggest banks in Estonia came under heavy attack. At the highest moments, the amount of cyber traffic from outside Estonia targeting government institutions was 400 times higher than its normal rate. … Some of the attacks were carried out in waves and were executed with very precise timing. They were unusually well-coordinated and required resources unavailable to common people. At one point, attacks were carried out in a very precise timeframe and included groups of computers - "botnets"

- that were possibly rented out earlier for this purpose." [74] He characterizes it in terms of proportional effect:

Taking into account the size of Estonian infrastructure and the scope of the attacks, it was one of the most significant coordinated cyber-attacks against a sovereign state in the world….Although the attack was defeated without any long term consequences, there were some immediate effects that affected all Estonian people, such as unavailability of online banking or difficulties in communication. In a country where 98% of bank transactions are made online and where majority of citizens fill tax forms online, I am sure that you can realize the impact that such prolonged incidents could have… The impact of the attacks was also amplified by the psychological effect and intimidation that it had on the general populace. Besides directly affecting the target, cyber-attacks created widespread confusion and miscommunication in the general public, as it was impossible to get online information on events in Estonia from abroad. [75]

Estonia took many steps after these attacks. It reached out to NATO for military assistance but NATO could not utilize its then-existing authority and policy to intervene. Estonia subsequently adopted new law and policy [76] to deal with any future such attacks on its Internet infrastructure. NATO opened the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia in 2008. Since then there have been a number of conferences at the Centre to discuss legal issues related to cyber attacks. [77] NATO policy and activities have been evolving over time. [78]

6.2. Georgia 2008

Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul (2008) in their work *Cyber Attacks Against Georgia: Legal Lessons Identified* made a number of recommendations to address what they identified as "certain gray areas" that exist in the context of Eastern European capabilities against cyber attacks. [79] Studying the cyber attacks that took place against Georgian government websites and ICT networks the same day that Georgia launched its military action in South Ossetia on 7 August 2008, the report makes a number of recommendations. [80] Based on the legal lessons identified and learned from the recent public cyber attacks (Estonia 2007, Lithuania 2008, Georgia 2008), the authors suggest that new approaches to traditional Law of Armed Conflict principles need to be developed in order to provide effective legal remedies under this area of law. [81] In particular, they recommend that although the Geneva Convention does not explicitly define armed conflicts as to include cyber attacks, they suggest that the latest developments in information warfare "welcome such interpretation." [82]

Jon Bumgarner (2009), the Chief Technical Officer of the US Cyber-Consequences Unit, an independent non-profit research institute, undertook a special report of the Georgia cyber-campaign entitled, *Overview by the US-CCU of the Cyber-Campaign Against Georgia in August of 2008.* [83] The report issued in August 2009 made a number of startling observations with respect to what took place in Georgia in the summer of 2008:

> Many of the cyber attacks were so close in time to the corresponding military operations that there had to be close cooperation between people in the Russian military and the civilian cyber attackers. When the cyber attacks began,

> they did not involve any reconnaissance or mapping stage, but jumped directly to the sort of packets that were best suited to jamming the websites under attack. This indicates that the necessary reconnaissance and the writing of attack scripts had to have been done in advance. Many of the actions the attackers carried out, such as registering new domain names and putting up new Web sites, were accomplished so quickly that all of the steps had to be prepared earlier. [84]

Bumgarner notes that "the organizers of the cyber attacks had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out." [85] Most shockingly, Bumgarner concludes:

> From the cyber campaign against Estonia in April and May 2007, Russians had already learned that a cyber campaign mounted by civilians could cause serious economic and psychological disruptions in a country without provoking any serious international response. This lesson was reinforced by their experiences with the cyber campaigns against Lithuania at the end of June 2008 and against Kazakhstan in January 2009, where major local disruptions produced remarkably little international press coverage.
>
> The campaign against Georgia took place under different conditions, because Russia was engaged in overt military action against the country, but the cyber component was still carried out by civilians, and there were no international reprisals. Given this history, it would be very surprising if most future disputes and conflicts involving Russia and its former possessions or satellites weren't accompanied by cyber campaigns. [86]

6.3. Republic of Korea 2009

Two of the authors of this article have conducted a detailed study of the South Korea media reports, U.S. military reports, Information Security expert and Korean government reports, including interviews in Korea and Japan, of the July 2009 attacks on South Korea and the United States. What is abundantly clear is the lack of unanimity of Information Security specialists on the place of origin of the attacks - reports from the South Korea press began by attributing them to North Korea, later to the United Kingdom and the United States with botnets ultimately involving computers in multiple countries, and as recently as September 2010, at the RSA Conference [87] held in Tokyo, a South Korean government official was saying that the current view is again that the source of the attacks was North Korea, while on the other hand a tech person from a South Korean firm interviewed in Tokyo said that the source was South Korea.

A chronology of reports in the South Korean English language media and other media can be divided into three stages of analyses.

1. Three Stages of Analysis of the Source of Attacks

STAGE 1 - INITIAL REPORTS -JULY 2009

The initial reports indicated that the attacks were suspected to have come from North Korea. Over the next weeks, it was found that they actually came from such locations as the UK and Miami, Florida, as well as South Korea.

Nature -There were three rounds of DDOS attacks.

As of 7 July, it was reported by Agence France Presse that about 12,000 computers in South Korea and 8,000 abroad were "apparently exploited" as vehicles for the attacks. [88]

Damages & Countermeasures

The Republic of Korea reportedly engaged in the following countermeasures:

Seized samples of the malicious code

Delivered samples to a vaccine vendor

Blocked the exploited server from disseminating M. code

Blocked the server from sending malicious code that could destruct hard drives

Issued an official announcement [89]

Various South Korean government agencies and others were involved in the investigation of the attacks. They include the Korea Internet & Security Agency [90], the Seoul Prosecutor's Office, Korean Communications Commission and the National Intelligence Service.

In addition, Ahn Labs provided assistance with anti-virus vaccine disseminated in South Korea. To date, there have been no reports that anyone was prosecuted for the attacks, although the Republic of Korea has adopted law that could be applied to such situations. The most that could be done was to determine what the attacks were and to issue various reports about where they came from. No individuals were identified. Ultimately, no state was reported to have ordered them.

On the other hand, Professor Peter Sommer of London School of Economics cautioned against coming to quick conclusions, because any instigator would disguise the source of the attacks, and stated, "Initial diagnoses are often wrong. [91]" It turned out that he was correct, as shown by subsequent reports summarized below:

December 17, 2009 - The Japanese National Police Agency reported that it believed that eight servers in Japan were involved in the July 2009 attacks. The agency indicated that it had detected a software program on the servers which issued instructions to computers that sent the denial of service attacks to overload the servers of 35 government and private sector organizations in the Republic of Korea and the United States. It also noted that "hundreds of similar servers have been confirmed in dozens of countries and that tens of thousands of terminals were involved in the cyber attack." [92]

STAGE 2 ANALYSIS - JULY 15 - OCTOBER 2009

On July 15, 2009, the Korea Communications Commission ("KCC") reported that the Vietnamese computer security company Bach Khoa Internetwork Security had told KISA that "the master server behind the attacks was located in the UK. After the DDOS attacks began, KISA had sent samples of the computer virus to the 16 member nations of the Asia Pacific Computer Emergency Response Team, which includes Vietnam. The KCC then passed on the information to the National Intelligence Service, state prosecutors and the police, while an international investigation has been launched. KISA speculates that the master server, which uses a Windows 2003 operating system, spread the virus through 125 host websites across the world. Damage was reported in 166,000 computers in 74 countries, including South Korea, the US, China, Japan, Canada, New Zealand and the U.K. In South Korea alone, around 78,000 computers were infected." [93]

A conflicting anonymous report from a Grand National Party (South Korea) official stated that the National Intelligence Service had obtained "a document in which North Korea ordered on June 7 a hacking unit, 'Number 100', under the wing of the General Staff of the People's Army, to destroy puppet communication networks of South Korea and to develop hacking programs that conceal the identity of the attackers." [94]On July 10, 2010, the national telecommunications regulator, the KCC, blocked five Internet addresses found to have diffused the malicious codes that launched the DDoS attacks. [95]

STAGE 3 ANALYSIS - OCTOBER 2009 TO AUGUST 2010

Representatives of the Republic of Korea government continued to insist as of September 2010 that the attacks came from North Korea, or via China. Representatives of a South Korean information security firm interviewed off the record stated that the attacks came from South Korea and were a political ploy. It must be recalled that around the same time, the South Korean legislature was considering adoption of a Cyber security bill to which there were political objections stating that the law was too repressive. [96]

There have been no reported arrests or prosecutions or reports of any military or other measures taken as a result of the attacks. One reason may be the

problem of attribution of the exact source of the attacks.

6.4. Japan 2010

On September 19, 2010, news media reported that Japan suspected its Defense Ministry and National Police Agency websites had come under cyber attack by a Distributed Denial of Service attack due to a row with the People's Republic of China ("PRC") over the September 7, 2010 collision of a Chinese fishing trawler and two Japanese Coast Guard vessels near a disputed island chain in the East China Sea. China's largest known hacker group had warned that it would attack Japanese websites to protest the incident. The Japanese government ordered that government entities take self-defense measures, such as shutting down their websites, for a short period of time. [97]

6.5. Ongoing Attacks on the United States

A report prepared for Congress indicates that the number of cyber attacks against the U.S. Government was "rising sharply" in 2009. [98] Moreover, this report states the suspicion that many of these attacks were coming from Chinese state and state-sponsored entities. [99]During 2008, there were 54,640 total cyber attacks against the US Department of Defense, according to the report, citing data provided by U.S. Strategic Command officials. [100] The number of instances significantly increased in the first half of 2009, when there were 43,785 cyber incidents targeting the Department of Defense, the report states. [101]

The report examines the problem of attribution and draws the following conclusions:

> Cyber attacks that originate in China can defy easy classification; some malicious activity appears to originate from private hacking groups, while other activity is almost certainly state sponsored. The latter…can be recognized to a certain extent by two important factors. First, cyber incidents leave behind signatures that can, with forensic analysis, sometimes reveal the affiliation of the responsible actors to a reasonable degree of certainty. This sometimes allows investigators to implicate the Chinese government directly, or sometimes even specific parts of the Chinese government, such as the People's Liberation Army (PLA)…Second, the nature of the malicious activity-including the type of information targeted-helps supplement the understanding of the attackers and their affiliations. One can infer state involvement in some instances based on the specific targeting of government and defense networks. [102]

Dennis Blair, former director of national intelligence, told the Senate Select Committee of Intelligence in February 2010 that the computerized critical infrastructure of the US is "severely threatened" by malicious cyberattacks and cyberespionage now occurring on an "unprecedented scale with extraordinary sophistication." [103] According to Mark Clayton (2010) of the *Christian Science Monitor*, Mr Blair made the following observations to the committee:

- Sensitive information is "stolen daily from both government and private sector networks."

- Investigations are finding "persistent, unauthorized, and at times unattributable presences on exploited networks, the hallmark of an unknown adversary...."
- The US cannot be certain its cyberspace infrastructure will be available and reliable in a crisis.
- The US and the world face greater vulnerability to disruption as a result of the trend toward convergence of voice, facsimile, video, computers, and controls that operate critical infrastructure on a single network: the Internet. These include banking, power, and water supplies.
- Cyber threats are increasingly subtle and sophisticated. Last year saw the deployment of "self-modifying malware, which evolves to render traditional virus detection technologies less effective." [104], [105]

Most significantly, there was Deputy Defense Secretary's William J. Lynn III's piece in *Foreign Affairs* which declassified the following event:

> In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary. [106]

The article written by Deputy Secretary of Defense, William J. Lynn III, examines the problem faced by the Department of Defense from the more than 100 foreign intelligence organizations that are trying to hack into the digital networks that support U.S. military operations. [107] Dealing with the threat posed by cyber warfare, Lynn notes that the Pentagon is partnering with allied governments and private companies to prepare itself for the catastrophic threat posed by cyber espionage. [108] In the article, Lynn "presents new details about the Defense Department's cyber strategy, including the development of ways to find intruders inside the network. That is part of what is called 'active defense.'" [109] For instance, counterfeit hardware has been detected in systems that the Pentagon has bought which could expose the network to manipulation from adversaries. [110] Lynn also "puts the Homeland Security Department on notice that although it has the "lead" in protecting the dot.gov and dot.com domains, the Pentagon - which includes the ultra-secret National Security Agency - should support efforts to protect critical industry networks." [111]

6.6. Other Incidents and Reports on the Origin of the Attacks

6.6.1. Project Grey Goose

Project Grey Goose started as an open source effort to better understand the nature of

cyber activities between Russia and Georgia. The idea was originally conceived by Jeffrey Carr at IntelFusion, and his call for volunteers quickly spread through the network of intelligence community blogs. In a report released in two Phases, Phase I dealt with the Russia/Georgia Cyber War- Findings and Analysis and was released on 17 October 2008. [112] Phase II was released on 20 March 2009 and dealt with the evolving state of cyber warfare. [113] Phase II dealt with a marked increase in cyber attacks by State and Non-State hackers since the Russia Georgia War of 2008. In addition to the Russia Georgia War of 2008, Phase II also focused on the cyber clashes resulting from Israel's Operation Cast Lead and the Web site defacement of India's Eastern Railway. [114]

The approach taken by Jeffrey Carr/Project Grey Goose illustrates the approach and thinking of Information Security/tech experts in relation to the attribution problem, which is one of the major obstacles to developing international law and military strategy to address cyber attacks affecting national security of nations with dependence on the Internet and cyberspace.

The report aimed to answer the following questions, namely:

> How effective is Social Network Analysis in Computer Network Exploitation?
>
> How critical is the ability to access black (classified) data in a cyber intelligence effort?
>
> Is there evidence that points to Russian government involvement in the Georgia cyber attacks of July and August 2008? [115]

The report concluded that:

> non-state hackers rely on publicizing their exploits to build their online reputations. Thanks to this need for recognition among their peers, data mining foreign language forums and social media sites can produce meaningful results. It is not, however, sufficient in and of itself and should be combined with server-level data, as well as an examination of geopolitical events occurring around the time of the cyber attacks. Furthermore, when State interests are involved, a review of the Nation State's military doctrine related to Information Warfare is also important. If all of this information is available, then there is little need for accessing classified (black) data. In fact, the incorporation of black data can be counterproductive as it precludes the sharing of information between non-cleared international researchers which often adds speed and veracity to an otherwise challenging pursuit. [116]

6.6.2. GhostNet and ShadowServer

GhostNet is the name given by researchers at the Information Warfare Monitor to a large-scale cyber spying operation discovered in March 2009. [117] Its command and control infrastructure is based mainly in the PRC and has infiltrated high-value political, economic and media locations in 103 countries. [118] Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama's Tibetan exile

centers in India, London and New York City were compromised. [119] Although the activity is mostly based in China, there is no conclusive evidence that the Chinese government is involved in its operation. [120]

On 6 April 2010, the Shadowserver Foundation and The Information Warfare Monitor issued a joint report entitled "Shadows in the Cloud: Investigating Cyber Espionage 2.0. [121] The report highlights the ever increasing problem posed by the increasing embedding of crime and espionage in the fabric of global cyberspace. The report calls for a global convention on cyberspace to make order out of what is increasingly becoming a dangerously disordered domain.

7. Recommendations for overcoming the attribution problem

We should consider some of the points that James Lewis (2009) makes in a paper for the Center for Strategic and International Studies analyzing the "Korean" cyber attacks of July 2009 (see detailed discussion in VI.C. above) with respect to the issue of attribution. First, Lewis points out that there is also a further tension between a policy need for rapid response and the technical reality that attribution is a time-consuming task: "Shortening the time for investigation may well increase the likelihood of errors being made in response (e.g., responding against the wrong machine or launching a response that has large unintended effects)." [122]

Speaking more about on the problem of overcoming the attribution problem, Lewis notes that:

> This failure of attribution leads to several conclusions on the state of cyber conflict. Cyber conflict is a new and complicated strategic problem. There is neither an adequate policy framework to manage conflict in cyberspace nor a satisfactory lexicon to describe it. Uncertainty is the most prominent aspect of cyber conflict - in attribution of the attacker's identity, the scope of collateral damage, and the potential effect on the intended target from cyber attack. Many concepts - deterrence, preemption, proportional response - must be adjusted or replaced for the uncertain cyber environment. This uncertainty has significant political implications for both attackers and defenders and creates constraints and thresholds for the use of cyber "weapons." [123]

Lewis suggests "that there can be no reflexive rules of engagement for cyber conflict. Some militaries have rules of engagement for self-defense that give a commander the discretion to fire back when fired upon, without prior approval from higher authorities. This sort of rule could be rarely exercised in cyberspace, if ever, since a counterstrike in cyberspace is likely to lack clear attribution and clear scoping of the side effects on neutral parties." [124] Lewis is equally dismissive of the effectiveness of cyberspace deterrence: "Weak attribution and unpredictable collateral damage make deterrence ineffective in cyberspace. Deterrence is a threat of retaliation, but it is hard to credibly threaten unknown parties and counterproductive to threaten or damage the wrong party." [125] In short, weak attribution makes traditional deterrence concepts largely irrelevant in cyberspace.

On 15 July 2010, the US House of Representatives, Committee on Science and Technology, Subcommittee on Technology and Innovation held a hearing entitled, *Planning for the Future of Cyber Attack Attribution*. [126] The purpose of the hearing was to discuss attribution in cyber attacks, and how attribution technologies have the potential to affect the anonymity and privacy of internet users. [127] The witnesses who testified were:

- Dr. David Wheeler, a Research Staff Member of the Information Technology and Systems Division at the Institute for Defense Analyses;
- Mr. Robert Knake, International Affairs Fellow at the Council on Foreign Relations;
- Mr. Ed Giorgio, President and Co-Founder of Ponte Technologies; and
- Mr. Marc Rotenberg, President of the Electronic Privacy Information Center. [128]

7.1. Dr David Wheeler

In written testimony submitted to the Subcommittee, Dr Wheeler made the following observations on the problem of attribution in relation to his work for the Department of Defense as an advisor:

1. There are a large number of different attribution techniques. Each technique has its strengths and weaknesses; no single technique replaces all others.
2. Attribution is difficult and inherently limited. In particular, attackers can cause attacks to be delayed and perform their attacks through many intermediaries in many jurisdictions, making attribution difficult. In some cases this can be partly countered, for example, by treating some information-gathering techniques as attacks (and attributing them), using multiple techniques, and using techniques that resist this problem (such as exploiting/forcing attacker self-identification and attacker surveillance). Nevertheless, because of the difficulty and uncertainty in performing attribution, computer network defense should not *depend* on attribution. Instead, attribution should be part of a larger defense-in-depth strategy.
3. Attribution tends to be easier against insiders or insider intermediaries.
4. Prepositioning is necessary for many attribution techniques.
5. Many techniques are immature and will require Department of Defense funding before they are ready for deployment.
6. A useful first step for the Department of Defense would be to *change the terrain*of its own network. By this, we mean modify Department of Defense computers and networks to aid attribution techniques. This includes hardening routers and hosts so exploiting them as intermediaries is more difficult, limiting spoofable protocols, disabling broadcast amplification/reflection, and implementing network ingress filtering. Changing the terrain should also be applied to key networks the Department of Defense relies on, to the extent the Department of Defense can convince those network owners to do so. [129]

Dr Wheeler also spoke of the controversial technique of breaking into a host machine or series of host machines (termed by some a "hack back"), usually going backwards toward

the attacker. [130] The defender, knowing the same attack methods as the attacker does, can simply reverse the attack chain. [131] The "hack back" approach has many additional disadvantages. [132] Fundamentally this involves a number of complex legal issues. [133] It is also an extreme measure with many social issues, such as privacy concerns. [134] This is especially true if the counter-attack is performed by anyone other than the host owner or authorized administrator. [135] In short, hack back is an approach with a large number of important disadvantages. [136]

7.2. Mr. Robert Knake

Robert Knake's testimony emphasizes the fact that "for the highest level threat, that of cyber warfare, the attribution problem is largely overstated." [137] He stresses that "as with other Internet based attacks, technical attribution may be difficult and the forensics work will take time, but at present there are a limited number of actors that are capable of carrying out such attacks." [138] Mr Knake suggests that instead of attribution pinpointing the exact person who carried out a catastrophic cyber attack, other countries might hold a non-cooperating country culpable for not investigating a cyber attack traced to its jurisdiction: [139]

> Based on this new paradigm of sovereignty [referring to requests to the Taliban to turn over Bin Laden, and the actions taken against them due to their non-cooperation] states should be expected to pass laws making international cybercrime illegal and enforce them. They should have mechanisms in place to respond to international requests for assistance and they should have some ability to oversee the hygiene of their national networks. Better attribution through post-incident forensic techniques will be a crucial part of this new paradigm, but the development of ironclad attribution will not necessarily lead to better security in cyberspace. [140]

7.3. Mr. Ed Giorgio

Mr Giorgio's testimony emphasized the balance between privacy and the need to be able to identify and trace activities over the Internet: "When balancing the need for anonymity with attack attribution, there is no silver bullet, be it technology, policy, economic incentives, or cultural change, which will solve the problem." [141] For Mr Giorgio, attribution must develop and adjust to ever-changing technology:

> In a world of insecure computers and botnets (commandeered armies of innocent computers) we will need attack attribution to point us to the offending computer, its owner or institutional affiliation, and its geographic location. But as computers become virtualized we will lose the ability to attribute action to specific computers and as we move to cloud computing we will even lose the ability to geo-locate the computer. This doesn't mean that we can't encode the user identity, computer ID, process ID, and institutional affiliation into the computer's (IP) address, because with the proper R&D we can move to a next generation of internet protocols which do precisely that. [142]

7.4. Mr. Marc Rotenberg

Mr Rotenberg spoke of the risks and limitations of attempting to establish a mandatory Internet ID that may be favored by some as a way to address the risk of cyber attack. [143] He spoke of the significant implication for human rights and freedom online of such a mandatory Internet ID. For instance, it is not clear -- according to Mr Rotenberg -- that it would be constitutional to mandate such a requirement in the United States. [144] As Mr Rotenberg emphasized that any proposal to mandate online identification will create new risks to privacy and security. [145] Mr Rotenberg pointed to the situation in the PRC where the establishment of attribution requirements to address cyber security concerns has been used to track the activities of citizens and to crack down on controversial political views. [146]

8. When Do Such Acts Rise to the Level of an Act of War?

8.1. Schmitt Analysis

Dementis and Sousa (2010) suggest that "cyber conflicts can be analyzed in light of two areas of international law: *jus ad bellum*, also known as the law of conflict management, and *jus in bello*, the law of war. *Jus ad bellum* is the law governing the resort to the use of force-whether force is permissible or not, and *jus in bello* is the law that governs activities once *jus ad bellum* has determined that force may be used." [147] Professor M. N. Schmitt (1999) argues that "... as the nature of a hostile act becomes less determinative of its consequences, current notions of 'lawful' coercive behavior by states, and the appropriate responses thereto, are likely to evolve accordingly." [148] Michael, Wingfield and Wijesekera [149] (2003) suggest that "the Schmitt Analysis, then, is useful as a legal algorithm, but it is even more useful as a method for highlighting areas of uncertainty or disagreement in multiple legal analyses, and for providing a principled means by which to address all relevant aspects of a use of force against software-intensive systems that are part of the critical infrastructure." [150] Schmitt (2002) [151] argues that "computer network attacks are subject to humanitarian law if they are part and parcel of either a classic conflict or a 'cyber war' in which injury, death, damage or destruction are intended or foreseeable. This being so, it is necessary to consider the targets against which computer network attacks may be directed."

Professor Schmitt (2002) argues that a computer network attack ("CNA") can fall within the parameters of humanitarian law because of its consequences:

> In light of this interpretation, does computer network attack fall outside the ambit of "attacks" because it does not employ violence? No, and for precisely the same reason that armed attacks can include cyber attacks. "Attacks" is a term of prescriptive shorthand intended to address specific consequences. It is clear that what the relevant provisions hope to accomplish is shielding protected individuals from injury or death and protected objects from damage or destruction. To the extent that the term "violence" is explicative, it must be considered in the sense of violent consequences rather than violent acts. Significant human physical or mental suffering is logically included in the

> concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property likewise constitutes damage or destruction. The point is that inconvenience, harassment or mere diminishment in quality of life does not suffice; human suffering is the requisite criterion. As an example, a major disruption of the stock market or banking system might effectively collapse the economy and result in widespread unemployment, hunger, mental anguish, etc., a reality tragically demonstrated during the Depression of the 1930s. If it did cause this level of suffering, the CNA would constitute an attack within the meaning of that term in humanitarian law. [152]

Schmitt (2002) breaks down CNAs into three categories: 1) combatants and military objectives; 2) civilians and civilian objects; and 3) dual-use objects. [153] From Schmitt's vantage point, CNAs challenge existing notions of "attack" in addition to testing the traditional understanding of combatant status because of the use of typically civilian technology and know-how to conduct military operations via computer:

> Failure to strictly comply with the limitations on the participation of civilians in hostilities will inevitably lead to heightened endangerment of the civilian population and weaken humanitarian law norms. So the jury remains out. While humanitarian law in its present form generally suffices to safeguard those it seeks to protect from the effects of computer network attack, and even though it offers the promise of periodically enhancing such protection, significant prescriptive fault lines do exist. Therefore, as capabilities to conduct computer network attacks increase in terms of both sophistication and availability, continued normative monitoring is absolutely essential. We must avoid losing sight of humanitarian principles, lest the possible in warfare supplant the permissible. [154]

Professor Schmitt's suggested criteria for evaluating the consequences of cyber attacks are useful, but have been criticized by some commentators as falling short of what is necessary. His criteria are:

> "Severity: Armed attacks threaten physical injury or destruction of property to a much greater degree than other forms of coercion. Physical well-being usually occupies the apex of the human hierarchy of need." [155]

> "Immediacy: The negative consequences of armed coercion, or threat thereof, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodation is hampered in the former case." [156]

> "Directness: The consequences of armed coercion are more directly tied to the *actus reus* than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty." [157]

> "Invasiveness: In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability." [158]
>
> "Measurability: While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force." [159]
>
> "Presumptive Legitimacy: In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self defense. The cognitive approach is prohibitory." [160]
>
> "Responsibility: refers to the degree to which the consequence of an action can be attributed to a state as opposed to other actors. The premise is that armed coercion is within the exclusive province of states and is more susceptible to being charged to states, whereas non-state actors are capable of engaging in such soft activity as propaganda and boycotts." [161]

8.2. Wingfield Analysis

Professor Thomas Wingfield [162] extended Schmitt's analytical technique by providing a means for quantifying the qualitative measures of consequences: [163]

> Specifically, Schmitt examined why the framers of the [United Nations] Charter chose to characterize each type of coercion as they did. By applying a quantitative scale to each of the seven factors he identified, any given operation could be described in qualitative terms as being closer to one end of a spectrum or the other. In other words, an action's qualitative nature (in seven more or less binary areas) could be determined by applying any fixed quantitative figure (say, a one-to-ten scale). Schmitt's contribution in translating the qualitative Charter paradigm into its quantitative components-the legal equivalent of going from analog to digital-provides a framework for scholars and practitioners to organize analysis in something other than a quantum cloud of subjective uncertainty. [164]

Michael, Wingfield and Wijesekera (2003) suggest "that the Schmitt Analysis can be used to perform a more academically rigorous evaluation of the factors affecting a lawful response to a terrorist attack." [165] The authors used a scenario involving an attack on the Washington Metro at rush hour whereby the terrorists use malicious code to strike the software-intensive automatic train protection (ATP) system of the Metro. [166]

Furthermore, the attack was orchestrated from outside the U.S. by using compromised administrative computers that are used by Metro officials to monitor operations. [167] The authors concluded that this attack represented an "8" out of "10" in terms of severity relative to the September 11, 2001, attack on the World Trade Center. [168] The attack is extreme in both aspects of invasiveness, but lower for the intangible aspects and distance from the target, so we rated invasiveness as a "5" out of "10". When the Schmitt and Wingfield analyses and criteria are applied to the cyber attacks described in this article, they have not resulted in any legal or policy or other approaches to dealing with them.

Robert Knake divides and ranks cyber attacks into categories related to the seriousness of the threat they pose: cyber warfare, cyber espionage, brute force attacks, crime and nuisance. [169]

According to Libicki, cyber-warfare is used more for bothering (i.e. irritating or annoying) an adversary than defeating it, given that permanent effects are elusive. Moreover, Libicki notes that the threat of punishment has never done much to prevent cyber attacks on either civilian or military networks.

Lewis who was dismissive of the cyber incidents in Estonia and Georgia, concluding that they also did not rise to the level of an act of war: "These countries came under limited cyber attack as part of larger conflicts with Russia, but in neither case were there casualties, loss of territory, destruction, or serious disruption of critical services." [170] At the same time, however, Lewis recognizes the true intent behind such denial of service attacks - to create political instability: "The 'denial of service' attacks used against these countries sought to create political pressure and coerce the target governments, but how to respond to such coercion remains an open question, particularly in light of the uncertain attribution and deniability." [171] Thus, under the Schmitt and Wingfield analyses, neither the Estonian nor the Georgian attack could justify a military response on the part of NATO.

Is this the correct posture for countries dependent on the cyber networks to assume? Or rather is "a good offense the best defense" the better approach?

9. Non-state actors issue

Matthew Sklerov addresses the problem of not merely finding the source of the attack, but the attribution of agency to a national government when there are non-state actors operating from within that jurisdiction, e.g. hackers, criminals, terrorists. Sklerov calls this the "response crisis", suggesting that states from which cyber attacks are sent have an obligation to prevent non-state actors from engaging in actions from within their states to desist from armed attacks. He proposes that if the "host" states do not comply with this obligation, it would be legitimate for other states to attack them in "anticipatory self-defense", an approach he calls "active defense". [172]

Several commentators disagree with Sklerov's assertion that "automated or administrator-operated trace programs can trace attacks back to their points of origin." [173] According to Dr. Sandro Gaycken of the University of Stuttgart, "This sounds strange. IT-security professionals doubt that anything like this could exist." Many of the brightest in the industry repeatedly tried to come up with trace programs, but were unsuccessful. Only less serious companies claim to have actual solutions. Any existing technologies will be

immature, imprecise and quite likely in conflict with domestic and international law. This severely restricts Sklerov's approach. Even if the attribution of the type of actor can be allowed to be imprecise, the attribution of the location cannot. If there is a likelihood of, perhaps, 50 percent that the assumption about the location of an attacker is plain wrong, is that considered sufficient reason for an armed attack in anticipatory self-defense? The conclusion is, that, despite the fact that he has a well-argued case for the most part, Sklerov's approach does not provide a satisfactory solution for the "response crisis". [174]

10. Discussion

Clearly if ever there was a time for an informed debate on the issue of cyber attack, it is now:

> The topic of cyber attack is so important across a multitude of [US] national interests - not just defense or even just national security - that it deserves robust and open discussion and debate, both among thoughtful professionals in the policy, military, intelligence, law enforcement, and legal fields and among security practitioners in the private sector. [175]

There are huge differences among those observing the cyber conflict phenomena described in the press. An ongoing aspect of the debate is whether the cyberwar discussion is hype to enable the military establishment to obtain funding for its programs and support for national intelligence activities. On the one hand, there are the military and former White House officials who insist on the impending threats to the civilian and military networks owned by the private sector in the United States and other countries, and opposing views that say they are being alarmists for their own benefit. [176]

Some have attempted to come up with typologies of the phenomena and possible legal, military, policy and technological responses to them, for example: Irving Lachow of the National Defense University in the United States gives an overview of his view of the motivations, targets and methods for some of the activities described in this article [177]:

Table 19-1. Cyber Threats: Defining Terms

Black Hat Hacking	Ego, personal enmity	Individuals, companies, governments	Malware, viruses, worms and hacking scripts.
Cyber Crime	Economic gain	Individuals, companies	Malware for fraud, identity theft, DdoS for blackmail.
Cyber Espionage	Economic and political gain	Individuals, companies, governments	Range of techniques to obtain information.

Information War	Political or military gain	Infrastructures, information technology systems data (public or private)	Range of techniques or attack or influence operations.

CRN at the University of Zurich puts definitions into what it calls an "escalation ladder", focusing on the intention and effect of activities:

> Rung 1 - activism - "the normal, non-disruptive use of the Internet in support of a (political) agenda or cause"
>
> Rung 2 - hacktivism - "the marriage of hacking and activism, including operations that use hacking techniques against a target's internet site with the intention of disrupting normal operations"
>
> Rung 3 - cybercrime - "includes theft of intellectual property, extortion based on the threat of Distributed Denial of Service attacks (DDoS) attacks, fraud based on identity theft, etc. The intention of the attacker is economically driven."
>
> Rung 4 - cyberterrorism - "....unlawful attacks against computers, networks and the information stored therein, to intimidate or coerce a government or its people in furtherance of political or social objectives. Such an attack should result in violence against persons or property, or at least cause enough harm to generate the requisite fear level to be considered cyber-terrorism."
>
> Rung 5- cyberwar - "the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems." [178]

The CRN team (Brunner et al, 16-17) raises some useful questions:

> The underlying problem is that it remains unclear what is threatened, who is threatening, and what the potential consequences of cyberattacks could be. A cybersecurity strategy has to take into account very diverse types of threats, ranging from criminally motivated phishing activities to terrorist attacks on critical infrastructures… Does it then make sense to include all these threats in one cybersecurity strategy, or should there rather be separate strategies for cybercrime, cyberwar and cyberterror? The problem is that different threats are interlinked and the connections between them are not as clear. Cybercriminals may offer their services to terrorists or states, and they all exploit the same vulnerabilities. Treating different threats separately would be inconsistent with the soc-called "all-hazards approach", which has proven to be a useful concept to strengthen cybersecurity…. Clearer definitions are also required in order to develop a coherent international approach for cybersecurity, as the different perceptions of threats still hinder collaborative efforts. Finally a clear delineation of cyberthreats is required to define the responsibilities of different government agencies, which would be the first step towards better coordination of

> cyberscurity efforts. The inter-mixing of cybercrime with cyberwarfare and cyberterrorism, for example, often impedes a clear division of responsibility between military and civil agencies….the vague definitions of threats in the strategy papers lead to rather vague concepts for countermeasures…. " [Emphasis added] [179]

There are very few actual definitions of cyber war, though it is bandied about by the popular press regularly in articles asserting that all-out warfare in cyberspace is on its way. [180] Two definitions located through massive research of law and policy scholarship are as follows:

According to Lachow, "the term cyberwar is more focused on the "military aspects of competition":

> *"Cyberwar* refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to "know" itself." [181]

A reported Chinese definition of cyberwar is:

> A struggle between opposing sides making use of network technology and methods to struggle for an information advantage in the fields of politics, economics, military affairs, and technology. [182]

Perhaps a more workable term is "cyber attack", and this term has been used throughout this article. Peter J. Denning and Dorothy E. Denning define it as:

> "deliberate actions against data, software, or hardware in computer systems or networks. The actions may destroy, disrupt, degrade, or deny access. [They then describe cyber exploitation, which others call cyber espionage]. Both attack and exploitation require three things: access to a system or network, vulnerabilities in the accessed systems, and a payload… The payload is a program that performs actions once a vulnerability has been found and exercised. A payload may be a bot, data monitoring program, virus, worm, spyware, or Trojan horse; and it is likely to have remote access to the attacker's communication channels. …An attack payload is destructive, an exploit payload is nondestructive…." [183]

10.1. Information Warfare

Lachow infers from two other definitions, i.e. of netwar and cyberwar, that "*information war* can be understood to refer to cyber conflict at the nation-state level involving either direct military confrontation or indirect competition via disruption and deception." [184]

10.2. Electronic Warfare ("EW")

> The US military defines EW as any military action involving the use of electro-

> magnetic and directed energy to control the electromagnetic spectrum or to attack the enemy… The three major components of EW are electronic protect (EP), electronic support (ES), and electronic attack (EA). EP involves passive and active means to protect personnel and equipment from enemy EW. US forces use terrain masking, directional antennas, and other techniques to limit radio emissions. ES involves intercepting adversary electronic transmissions for further exploitation. US Forces use the intercepts to gather intelligence and also to locate or target the adversary's emitter. EA involves the use of directed energy to deny, disrupt or degrade an adversary's use of the electromagnetic spectrum. US forces direct energy at an adversary emitter to jam voice and data communications and radar. [185]

Developed and developing nations relying on the cyber networks and technology must consider such issues as degree of damage/harm, ability to attribute the sources of attacks in light of the use of botnets and other ways to keep the sources of attacks anonymous and impossible to trace and the relative benefits of deterrence vs. aggression before considering "retaliation in kind":

> Cyber attacks use software as a weapon launched over interconnected networks, to coerce an opponent or damage its ability to provide essential government, economic or military services. Advanced cyber weapons cause disruption or damage to data and critical infrastructure. A serious cyber attack would be an incident that disrupted critical services for an extended period, perhaps damaging military command or information systems, shutting off electrical power or fuel pipelines, or interrupting financial services. Cyber conflict will be part of warfare in the future and advanced militaries now have the capability to launch cyber attacks not only against data and networks, but also against the critical infrastructure that depend on these networks. [186]

Lewis talks of when a cyber attack can become an act of war:

> The "Korean" cyber incidents of early July [2009] did not rise to the level of an act of war. They were annoying and for some agencies, embarrassing, but there was no violence or destruction. In this, they were like most incidents in cyber conflict as it is currently waged. Cybercrime does not rise to the level of an act of war, even when there is state complicity, nor does espionage - and crime and espionage are the activities that currently dominate cyber conflict. The individuals and nations that engage in these activities do not think of themselves as engaging in warfare, at least as our current rules define it, and the lack of international norms for cyberspace only reinforces this sense of impunity. If a nation catches a spy, there is an increase in bilateral tensions, it may expel an attaché or demarche the guilty party, but it does not respond with military force. [187]

One of the problems that Lewis identifies is that the traditional definition of sovereignty does not offer much guidance in cyberspace. "Violation of sovereignty is not a useful threshold under current laws and norms for deciding when an event in cyberspace is an

act of war or justifies the use of military force." [188] Lewis proposes a solution:

> "[T]he legal and governance framework of cyberspace was designed to accommodate commerce, but it also enables covertness and reinforces deniability. Western nations, as the most frequent target of cyber attack and those most constrained by law, might gain if they were to decide collectively how to improve governance and what penalties should apply when a sovereign fails to exercise responsibility for actions taken in cyberspace under its jurisdiction." [189]

10.3. Possible Solutions

10.3.1. Long Term Proposals

Scott Shackelford proposes the following long term and short term approaches to the lack of a coherent legal regime to cover cyber attacks and cyber conflict. [190]A long term solution of course would be a multilateral treaty on cyber security: "Given the confused legal regime, the best way to ensure a comprehensive regime is through a new international accord dealing exclusively with cyber security and its status in international law." [191] Shackelford suggests that such a new treaty should:

1. define when a cyber attack rises to the level of an armed attack;
2. clarify which provisions of international law apply during cyber warfare; and
3. provide for enforcement mechanisms in the event of breach. [192]

Shackelford also suggests that the treaty should create a Multinational Cyber Emergency Response Team (MCERT) to both investigate which nations are behind cyber attacks, and have the defensive expertise needed to be fast responders when serious attacks occur; the MCERT could network together the current network of more than 250 national CERTs with the NATO-wide CERT based in Estonia. [193]

10.3.2. Interim Measures

In the absence of a new treaty, Shackelford suggests that NATO should partner with the global network of CERTs and work together to a multilateral security partnership that could:

1. root out state sponsors of cyber attacks;
2. better defend against cyber attacks by pooling resources and talent; and
3. provide invaluable intelligence to *overcome the fundamental issue of attribution.* [Emphasis added] [194]

A key component in combating cyber attacks would also include private sector involvement, especially, aggressive partnering with technology firms around the world such as Microsoft, Google and IBM, to name but a few. [195] Shackelford also calls for bilateral and multilateral partnerships with police bodies, including Interpol, to be established especially since, in his opinion, the majority of severe cyber attacks have a

criminal component. [196] Shackelford also calls upon the Obama Administration to release a white paper on how it would respond to different levels of cyber attacks to alleviate confusion and blunt the threat of nuclear war. This could be done in collaboration with foreign governments, in particular Russia and China, who could then follow suit. [197]

10.3.3. Russia, the United States, and Cyber Diplomacy

Along these lines of multilateral cooperation, the EastWest Institute released a report calling for Russia and the United States to work together to protect the world's digital infrastructure, including joint participation in NATO-Russia cyber military exercises. [198] According to the report's co-authors EWI's Franz-Stefan Gady and Greg Austin, this is just one step that the United States and Russia could undertake as a part of a broader effort to secure cyberspace - a potentially groundbreaking collaboration between the two former rivals. [199] *Russia, The United States, and Cyber Diplomacy: Opening the Doors* takes as its starting point the nations' pledge to begin talks on promoting cyber security made in the United Nations in December 2009. [200] The report recommends that Russia and the United States should undertake joint policy assessments of legal aspects of regulating cyber warfare, including both offensive and defensive activities, especially in the area of critical infrastructure and "rules of engagement." [201] The assessment should make recommendations on the best forum to advance multilateral moves toward regulation [202].

The essential act of war is destruction, not necessarily of human lives, but of the products of human labour. [203] Indeed, cyber attacks threaten the very essence of democratic nation states in particular in that they are open societies. Perhaps the greatest example of an open society is the Internet. The 2010 "Enemies of the Internet" list drawn up by Reporters Without Borders indicates that the worst violators of freedom of expression on the Internet are Saudi Arabia, Burma, China, North Korea, Cuba, Egypt, Iran, Uzbekistan, Syria, Tunisia, Turkmenistan, and Vietnam. [204] In these countries, the Internet's potential as a portal open to the world directly contradicts the propensity of these regimes to isolate themselves from other countries. [205] The report also identified several democracies "under surveillance": Australia, because of the upcoming implementation of a highly developed Internet filtering system, and South Korea, where laws characterized by critics as oppressive are creating too many specific restrictions on Web users by challenging their anonymity and promoting self-censorship. [206] When open societies such as Australia and South Korea start to take steps to monitor Internet activity, they fall prey of becoming 'part of the problem' when seeking to offer a solution. Countries such as the United States and the United Kingdom that possess the resources necessary to launch a retaliatory response to a cyber attack could become 'part of the problem' if they use their power in an aggressive approach rather than in a merely defensive fashion or engage in excessive surveillance of their own citizens. [207] (Refer to the testimony of Messrs. Giorgio and Rotenberg in VII.C. and D. Above for more discussion of the privacy and human rights implications when a "free society" undertakes surveillance of its citizens.)

One possible solution to the problem is a treaty to prevent cyber attacks becoming an all-out war. This is the viewpoint expressed by International Telcommunications Union

Secretary General Hamadoun Touré when he spoke earlier this year (31 January 2010) at a World Economic Forum debate on the topic of when a cyber attack becomes a declaration of war. [208] "A cyber war would be worse than a tsunami -- a catastrophe," Touré said, highlighting examples such as the attacks on Estonia. [209] He proposed an international accord, adding: "The framework would look like a peace treaty before a war." [210] According to Dr. Touré, countries should guarantee to protect their citizens and their right to access to information, promise not to harbour cyber terrorists and "should commit themselves not to attack another." [211]

One problem with the idea of a cyber treaty being an effective tool against cyber attacks was pointed out by Craig Mundie, chief research and strategy officer for Microsoft, at this same event: "There are at least 10 countries in the world whose Internet capability is sophisticated enough to carry out cyber attacks ... and they can make it appear to come from anywhere." [212] In the end, however, Mundie calls for greater control of the Internet infrastructure to prevent cyber attacks:

> People don't understand the scale of criminal activity on the Internet. Whether criminal, individual or nation states, the community is growing more sophisticated. We need a kind of World Health Organisation for the Internet. When there is a pandemic, it organises the quarantine of cases. We are not allowed to organise the systematic quarantine of machines that are compromised. [213]

10.4. Will any existing legal solution work?

Some of the policy strategies discussed are to place responsibility on the individual states to monitor their own networks (by creating CERTs if they do not already have them - China does have a CERT, am not sure about Russian Federation having one), to investigate their own criminals after adopting domestic Cybercrime law - both Russia and China have such law- but the law of war and other forms of law (law of the sea, space law, nuclear warfare paradigm) do not fit the current situation and have been rejected one after the other by various military, policy and law commentators. [214]

Treaties and legal considerations are only one set of factors that decision makers must take into account in deciding how to proceed in any given instance, according to Owens *et. al.* [215] They point out that "there will be no doubt many circumstances in which the United States (or any other nation) would have a *legal* right to undertake a certain action, but might choose not to do so because that action would not be politically supportable or would be regarded as unproductive, unethical or even harmful." [216] This point is well taken as one need only reflect that it is the same set of laws, e.g., *the Charter of the United Nations, the Hague and Geneva Conventions and the International Law of Armed Conflict,* that produced the debacle of whether a second justifying resolution of the United Nations Security Council was needed before the US and UK could invade Iraq in 2003. One need only look at the mess that resulted at that time to know that such decisive action can never be expected.

Owens *et al*. however suggest that under Article 51 of the UN Charter (which allows a nation to engage in the use of armed conflict for self-defense, including the situation in

which the nation is the target of an armed attack, even without Security Council authorization) a nation may be justified in using a cyber attack to intend to dissuade a nation using cyber attacks in the past from launching further attacks in the future, e.g., the 1986 El Dorado Canyon bombing on Libya by the United States. [217] This same argument however does not work in a case in which the attacker is not a nation-state, but a non-state actor or criminal or terrorist group. [218] It t is safe to say that most s if not all cyber attacks will not be clearly traceable to the acts of a nation-state, and although it may be possible to pinpoint the location from which the attacked was launched, the responsible individuals and decision-makers are much more difficult to trace given current technological tools and techniques. [219]

11. Conclusion

Whether the countries now locked in a cyberspace arms race and gearing up for possible Internet hostilities, including China, the United States, Russia, Israel and France, will heed the warning and avoid mutually assured destruction is another matter entirely. In the increasingly complex and interrelated world of cyberspace, Gandhi's adage "an eye for an eye and soon the whole world will be blind" seems more apt than ever. There may also be an analogy to President Kennedy's opportunity to push the red button to launch a nuclear attack in these scenarios, however, fortunately, the United Nations has fended off such actual events. However, countries reliant on Internet use for e-commerce, e-government, etc. must be prepared for the dangers of long and protracted cyber conflict/attack/war struggles, security and efforts for continuing its unrestricted use can be so costly as to undermine the very benefits. As Sun Tzu said long ago about the very art of warfare: "When you engage in actual fighting, if victory is long in coming, then men's weapons will grow dull and their ardor will be damped. If you lay siege to a whole town, you will exhaust your strength. Again, if the campaign is protracted, the resources of the State will not be equal to the strain. There is no instance of a country having benefitted from prolonged warfare." [220]

While the authors do not suggest that there is one clear path for countries dependent on Internet use to follow to assure themselves of victory in the battle against cyber attacks, we do note that the criteria for determining what is a victory have not changed since the 6 th century BCE:

> Thus we may know that there are five essentials for victory:
>
> He will win who knows when to fight and when not to fight;
>
> He will win who knows how to handle both superior and inferior forces;
>
> He will win whose army is animated by the same spirit throughout all its ranks;
>
> He will win who, prepared himself, waits to take the enemy unprepared;
>
> He will win who has military capacity and is not interfered with by the sovereign.

Hence the saying:

> If you know the enemy and know yourself, you need not fear the result of a hundred battles.
>
> If you know yourself but not the enemy, for victory gained you will also suffer a defeat.
>
> If you know neither the enemy nor yourself, you will succumb in every battle. [221]

In short, Sun Tzu anticipated the problems of responding to or dealing with the dilemmas surrounding today's cyber conflicts some 2,500 years ago.

Appendix - Technical Overview of the Problem of Attribution

The dilemma of anonymity

> The Internet's architecture and its evolving administrative and governance systems make the attribution of cyber attacks extremely challenging. The Internet has no standard provisions for tracking or tracing. A sophisticated user can modify information in IP packets and, in particular, forge the source addresses of packets (which is very simple for one-way communication). [222]

The most important paradox that exists in relation to the Internet today are the issues of anonymity, traceability and attribution. For some individuals, anonymity is a bad thing while for others it is very a good thing. Anonymity is a bad thing for law enforcement because it makes their work hard when attempting to identify criminals in cyberspace, and the same is true for Information Security professionals trying to trace sources of attacks. On the contrary, it is a good thing for those who want to have privacy when surfing the Web, for hackers, and for law enforcement, national security and military officials communicating in confidence among their peers. In any case, relinquishing anonymity depends on each individual user of the Internet, because there is no enacted law anywhere in the world that prohibits its use. If we were to abolish anonymity, we could ensure that people who access their own information are in fact themselves. We will be then be able to know who attacks whom, who sends spam, viruses, malwares and maybe attribute the precise actors that sent denial of service attacks to Estonia, Georgia, and South Korea.

Moreover, if we don't have anonymous users on the Internet, attribution will be just simple as pinpointing who is the criminal and punishing them accordingly. Thus, we would be able to say that we have a "violence-free cyberspace"; however, the current Internet architecture always allows anonymity and has no standard provisions for traceability, worldwide identification and attribution is still impossible. The main predicament now is, that an Internet in which all players "come out from behind the shadows" is not yet doable

in the present technology of internet and is expected to create more factions among various privacy rights organizations around the world if anonymity is abolished.

One of the biggest problems with attribution is tracing the source of the attack/packet. The emergence of botnets and malwares make it even more difficult to trace the origin of the attacks/packets. And when traced packets are identified, there is no certainty if the right person or location is identified or whether it might merely be the case in which the victim's computer is used as botnets.

Technically, it is still impossible to abolish anonymity. Strengthening international organisations and agencies that can identify cyber criminals and terrorists is an important first step. However, this first step must be taken with every country tightening up their statutes so as to support this goal. Assuming for the purposes of argument that we have the technical capability to prevent anonymity on the Internet, is there the political willpower in the democratic countries to prevent anonymity? Huge objections from civil libertarians and privacy rights groups can be expected.

Thus, in an ideal world the technical means must be coalesced with the policy agenda so as to produce a seamless understanding that balances the need to eliminate anonymity on the Internet while respecting civil liberties. Once this is achieved, the police agencies should be equipped with technical skills and policy knowledge that would help them in preventing cybercrimes in their own areas of responsibility and further promote international collaboration with other police agencies around the world.

Protecting critical information infrastructure networks

The best way to protect critical infrastructure networks from cyber attacks is to boost technical security measures and security policies. Strengthening technical measures in a layered (Defense-in-Depth) strategy is always the best defense against attackers, strategic positioning of our Information systems and those security personnel who handles it are the very essential part of security.

Security administrators/personnel must know how their systems work, and their technical vulnerabilities and patch up possible exploits that can be used against them by attackers attempting to penetrate their systems. Security administrators/personnel must conduct regular penetration testing and information technology audits in order to test the vulnerabilities of the systems to ensure proper deterrence. These administrators must also know the capabilities of possible attackers and the latest technologies, malwares and DDOS techniques used by hackers by conducting thorough and up-to-date technical security research. [223]

Utilizing (layered) Defense-in-Depth strategy is one of the best technical defenses for protecting the data. It is not safe to say that an information technology system is safe and secure because it possesses all the appropriate technical security capabilities. This is a classic fallacy of Internet security systems because all computers connected to the Internet are subjected to attack. If a company or an individual does not want to take this risk, then the only true defence is to "UNPLUG" its system from the Internet.

Technical solutions for attributing or deterring cyber attacks

Listed below are technical solutions for cyber attacks attribution or deterrence. [224] However, attackers have already found ways around each of these measures with countermeasures of their own.

- Hash-Based IP Trace back - Routers store hash values of network packets. Attribution is done by tracing back hash values across network routers.
- Ingress Filtering - All messages entering a network are required to have a source address in a valid range; this limits the range of possible attack sources.
- ICMP Return to Sender - All packets destined for the victim are rejected and returned to their senders.
- Overlay Network for IP Trace back - An overlay network links all ISP edge routers to a central tracking router; hop-by-hop approaches are used to find the source.
- Trace Packet Generation (e.g., iTrace) - A router sends an ICMP trace-back message periodically (e.g., every 1 in 20,000 packets) to the same destination address as the sample packet. The destination (or designated monitor) collects and correlates tracking information.
- Probabilistic Packet Marking - A router randomly determines whether it should embed message route data in a message; this routing data is used to determine routes.
- Hack back - Querying functionality is implemented in a host without the permission of the owner. If an attacker controls the host, this may not alert the attacker; thus, the information is more reliable.
- Honey pots - Decoy systems capture information about attackers that can be used for attribution.
- Watermarking - Files are branded as belonging to their rightful owners.

Technical impediments limit the effective attribution of attacks

Tunneling impedes tracking. [225] However, it is also very useful for creating virtual private networks (VPNs) that are so critical for security. Anonym zing services are valuable to Internet users, e.g., to facilitate political discourse in countries with repressive regimes. While anonymizers can be defeated in theory, there are numerous practical difficulties to achieving attribution when a sophisticated user desires anonymity.

Even if an attack packet can be attributed to an IP address of a host computer, it is difficult to link the IP address to the actual perpetrator. A perpetrator can decouple his physical identity from an IP address by using cyber cafes, public Internet facilities (e.g., libraries) and prepaid Internet address cards that can be purchased from service providers without any personal identification.

Attribution techniques themselves have to be secured against attacks and subversion. Software used for authentication and data used for attribution must be protected. Moreover, attribution techniques should not create additional avenues for exploitation (e.g., a new DOS attack against the system).

TOR (The Onion Routing)

One example of the use of anonymity tools is the TOR Project. [226] The TOR Project is an online software application that enables individuals to remain anonymous on the Internet. While this anonymity tool was developed to protect individuals who post things on the Internet against repressive regime they live under or to protect those who report child abuse cases, it is also now being used by hackers to hide their identities while cyber-attacking or committing crimes online. These anonymity tools are very visible and many are available to acquire for free over the Internet. Even though TOR was developed with good intentions, it does not mean that if it is used for fraudulent or sinister purposes it will not work. Technically, TOR will follow its program and functionality without regard to the *mens rea* of its users. TOR protects against a common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. This information is critical for traffic analysis because knowing the source and destination of your Internet traffic allows others to track your behavior and interests. TOR is now becoming a problem for law enforcement and national security officers. Attackers uses TOR in addition to botnets within the end result that packets can be re-routed to other server around the world that is within the TOR network. This makes attribution extremely difficult.

Bibliography

H.E. Jaak Aaviksoo, "Strategic Impact of Cyber Attacks," Isamaa ja Res Publica Liit, 5 March 2010, < http://www.irl.ee/en/Media/Articles/1927/strategic-impact-of-cyber-attacks > Accessed 4 October 2010.

AFP Tokyo, "Japan suspects Chinese cyber attacks," Taipei Times, 19 September 2010, page 5, <http://www.taipeitimes.com/News/world/archives/2010/09/19/2003483219> Accessed 4 October 2010.

Agence France Presse, 'UN chief calls for treaty to prevent cyber war', *The Sydney Morning Herald*. (Sydney, 31 January 2010) < http://news.smh.com.au/breaking-news-world/un-chief-calls-for-treaty-to-prevent-cyber-war-20100131-n5t7.html > Accessed 4 October 2010.

The Air Force Law Review - Cyberlaw Edition. 64 A.F. L. REV. (2009) is devoted to the a variety of cyberlaw issues arising in the context of the military. < http://www.afjag.af.mil/shared/media/document/AFD-091026-024.pdf> Accessed 4 October 2010.

Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the House of Representatives Committee on Armed Services, 23 September 2010, available at: < http://armedservices.house.gov/pdfs/FC092310/AlexanderStatement.pdf > Accessed 4 October 2010.

General Keith B. Alexander, Unclassified Advance Questions for Lieutenant General Keith Alexander, US Army, Nominee for Commander, United States Cyber Command, Undated, < http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf > Accessed 4

October 2010.

Ben Bain, "Cyber Command nominee lays out rules of engagement", Federal Computer Week, 16 April 2010, Tesimony of General Alexander reproduced here with clarifications added in parentheses, < http://fcw.com/articles/2010/04/16/web-cyber-command-many-roles.aspx > Accessed 4 October 2010.

Lolita C. Bolder, "White House Among Targets of Cyber Attack", 8 July 2009, Associated Press, < http://www.msnbc.msn.com/id/31800532/>. Accessed 4 October 2010.

BBC Monitoring Service, "South Korean Daily 'Cyber Attack from UK-based IP Address, Not North', The Financial Times Limited, 15 July 2009, via LEXIS

BBC Monitoring Service, "Document Shows North Korea Ordered Cyber Attacks - South Spy Agency," The Financial Times Limited, BBC Monitoring Service, 11 July 2009, via LEXIS

J Broward, 'Britain fends off flood of foreign cyber attacks', *The Observer*, 7 March 2010, < http://www.guardian.co.uk/technology/2010/mar/07/britain-fends-off-cyber-attacks/print > Accessed 4 October 2010.

Elgin Brunner, Anna Michalkova, Manuel Suter, Myriam Dunn Cavelty, Focal Report 3: Critical Infrastructure Protection - Cybersecurity - Recent Strategies and Policies: An Analysis, CRN Reports, (Center for Security Studies (CSS), ETH Zurich (2009).

Michael Cheek, "Cyber Debate Finds No Exaggeration in Threat of Cyber War," June 10, 2010, < http://www.thenewnewinternet.com/2010/06/10/cyber-debate-finds-no-exaggeration-in-threat-of-cyber-war/ >; Accessed 4 October 2010.

Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It (Harper Collins: April 2010);

Mark Clayton, 'Google cyber attacks a 'wake-up' call for US, intel chief says', Christian Science Monitor, 4 February 2010, < http://www.csmonitor.com/USA/2010/0204/Google-cyber-attacks-a-wake-up-call-for-US-intel-chief-says > Accessed 4 October 2010.

Georgios Dementis and Gonçalo Sousa, A Legal Reasoning Component of a Network Secuirty Command and Control System, Thesis, Naval Postgraduate School, Monterrey, California, March 2010.< http://edocs.nps.edu/npspubs/scholarly/theses/2010/Mar/10Mar_Dementis.pdf > Accessed 4 October 2010.

Peter J. Denning and Dorothy E. Denning, "The Profession of IT: Discussing Cyber Attack," 53 COMMUNICATIONS OF THE ACM, No. 9, September 2010.

Earl, Robert S. and Norman E. Emery, A Terrorist Approach to Information Operations, Thesis, M.S. in Defense Analysis, Naval Postgraduate School, June 2003.

EastWest Institute, Press Statement, 14 September 2010. < http://www.ewi.info/russia-united-states-and-cyber-diplomacy-opening-doors > Accessed 4 October 2010.

Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified, Cooperative Cyber Defence Centre of Excellence Legal Task Team, November 2008 < http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf> Accessed 4

October 2010.

Estonia Cybersecurity Strategy for 2008-2013 (2008), < http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf> Accessed 4 October 2010.

FierceCIO, "Schneier and Neustar Proudly Welcomes the Intelligence Squared U.S. Debate 'The Cyber War Threat Has Been Grossly Exaggerated' to Washington," 25 May 2010, < http://www.fiercecio.com/press-releases/neustar-proudly-welcomes-intelliegence-swauared-u-s-debate-cyber-war-threat-hs > Accessed 4 October 2010.

Franz-Stefan Gady and Greg Austin, Russia, The United States and Cyber Diplomacy: Opening the Door, The EastWest Institute, 16 September 2010. < http://www.ewi.info/russia-united-states-and-cyber-diplomacy-opening-doors >. Accessed 4 October 2010.

Dr. Sandro Gaycken, "The Necessity of (Some) Certainty - A Critical Remark Concerning Matthew Sklerov's Concept of 'Active Defense'", Journal of Military and Strategic Studies, Vol.. 12, Issue 2, Winter 2010.

Dr. Eduardo Gelbstein and Pauline Reich, Law, Policy & Technology: Cyberterrorism, Information Warfare, Digital & Internet Immobilization , IGI Global, forthcoming 2010.

Statement of Edward J. Giorgio, President and Co-Founder, Ponte Technologies, Before the House of Representatives Committee on Science and Technology, Planning for the Future of Cyber Attack Attribution, 15 July 2010. < http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Giorgio_Testimony.pdf > Accessed 4 October 2010.

Tim Gray, "U.N. telecom boss warns of pending cyberwar," 10 September 2010, MSNBC, < http://www.msnbc.msn.com/id/39102447/ns/technology_and=_science-security > Accessed 4 October 2010.

Greylogic, Project Grey Goose, Phase I Report, 17 October 2008< http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report >Accessed 4 October 2010

Greylogic, Project Grey Goose, Phase II Report, 20 March 2009 < http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report > Accessed 4 October 2010.

Jim Harper, "Cybersecurity: A Meaningless Term", Cato Institute, DailyPodcast, 2 July 2009. <http://www.cato.org/dailypodcast/podcast-archive.php?podcast_id=937> Accessed 4 October 2010.

Victor Hazelwood, Defense-In-Depth, An Information Assurance Strategy for the Enterprise, 2006. < http://www.sdsc.edu/~victor/DefenseInDepthWhitePaper.pdf> Accessed 4 October 2010.

Rex B. Hughes, NATO and Cyberdefence - Mission Accomplished?, Ap: 2009 nr1/4, Available at: < http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf> Accessed 4 October 2010.

J. Hunker, R. Hutchinson, R. and J. Marguiles, "Critical Information Protection II", International Federation for Information Processing, Volume 290, eds. Papa, M., Shenoi. S., (Boston: Springer, 2008).

Japan Today, "Cyber attacks suspected on Defense Ministry, police agency websites," 19 September 2010, < http://www.japantoday.com/category/crie/view/cyberattacks-suspe...> Accessed 4 October 2010.

Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law", 88 Texas L. Rev. 1571< http://www.texaslrev.com/issues/vol/88/issue/7/kanuck> Accessed 4 October 2010.

Professor Dr Henrik W.W. Kaspersen, Council of Europe - Project on Cybercrime, Draft 5 - Cybercrime and Internet Jurisdiction (March 2009), < http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf > Accessed 4 October 2010.

ICANN No. 36 - 25-30 October 2009, Seoul, Korea < http://sel.icann.org/> Accessed 4 October 2010.

Robert K. Knake, International Affairs Fellow, Council on Foreign Relations, *Untangling Attribution: Moving to Accountability in Cyberspace*, Prepared statement before the Subcommittee on Technology and Innovation, Committee on Science and Technology United States House of Representatives, 15 July 2010. < http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Knake_Testimony.pdf > Accessed 4 October 2010.

Kyodo News Service, "Eight Japanese Computer Servers Suspected in July Cyber Attack," BBC Monitoring International Reports, 17 December 2009 via LEXIS.

Irving Lachow, "Cyber Terrorism: Menace or Myth?", in Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, Cyberpower and National Security Center for Technology and National Security Policy, National Defense University and Potomac Books, Inc., 2009.

J A Lewis, "The "Korean" Cyber Attacks and Their Implications for Cyber Conflict", Center for Strategic and International Studies, October 2009

<http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf> Accessed 4 October 2010.

M Libicki, Conquest in Cyberspace: National Security and Information Warfare Rand/Cambridge University Press (2007).

M Libicki, Cyberdeterrence and cyberwar, (Santa Monica: The Rand Corporation, 2009).

< http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf>

M Libicki, What is Information Warfare?, National Defense University, Institute for National Security Studies (1995).

Lim Chang-Won, S. Korean websites 'attacked by North Korea', Agence France Presse, 7 July 2009 < http://www.google.com/hostednews/afp/article/ALeqM5j0fiT6uNbuYyzji1rIU1jTa6cmJA >

Accessed 4 October 2010

William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", Foreign Affairs, September/October 2010 < http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain > Accessed 4 October 2010.

John Markoff, "Step Taken to End Impasse Over Cybersecurity Talks," New York Times, 16 July 2010, < http://www.nytimes.com/201007/17/world/17cyber.html> Accessed 4 October 2010.

James B. Michael, Thomas C. Wingfield and Duminda Wijesekera, Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System, *Proc. Twenty-seventh Annual Int. Computer Software and Applications Conf.*, IEEE (Dallas, Tex., Nov. 2003). < http://www.au.af.mil/au/awc/awcgate/nps/ws09-with-pub-info.pdf > Accessed 4 October 2010.

Ellen Nakashima, "Defense official discloses cyber attack", The Washington Post, 24 August 2010, < http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html > Accessed 4 October 2010.

National Security Agency/Central Security Service Website, Biography Director of National Security Agency/Central Security Service, General Keith Alexander, Date Posted: Jan 15, 2009, Last Modified: Sep 17, 2010, Last Reviewed: Sep 17, 2010, < http://www.nsa.gov/about/leadership/bio_alexander.shtml> Accessed 4 October 2010.

National Security Agency, "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments" (Undated). < *www.nsa.gov/ia/_files/support/defenseindepth.pdf > Accessed 4 October 2010.*

NATO PA-173 DSCFC 09 E bis - NATO and Cyber Defence, SVERRE MYRLI (NORWAY) - RAPPORTEUR, April 2009, < http://www.nato-pa.int/default.asp?SHORTCUT=1782> Accessed 4 October 2010.

W Owens, K Dam and H Lin, Technology, Policy, Law and Ethic Regarding U.S. Acquisition and

Use of CYBERATTACK CAPABILITIES, (Washington, D.C.: The National Academies Press, 2009) < http://www.nap.edu/openbook.php?record_id=12651&page=1> Accessed 4 October 2010, x.

Pauline Reich, General Editor, *Cybercrime & Security*, published by Oxford University Press (ISBN13: 978-0-379-01281-1/ISBN10: 0-379-01281-2

Reporters Without Borders, *Enemies of the Internet - Countries Under Surveillance,* 12 March 2010, < http://www.rsf.org/IMG/pdf/Internet_enemies.pdf> Accessed 18 March 2010.

Josh Rogin, The top 10 Chinese Cyber Attacks (that we know of), The Cable, 22 January 2010, < http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of > Accessed 4 October 2010.

Testimony and Statement for the Record of Marc Rotenberg, President, Electronic Privacy Information Center, and Adjunct Professor, Georgetown University Law Center, Hearing on "Planning for the Future of Cyber Attack Attribution" Before the Committee on Science and

Technology Subcommittee on Technology and Innovation U.S. House of Representatives, July 15, 2010. < http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Rotenberg_Testimony.pdf > Accessed 4 October 2010.

M.N. Schmitt. "Asymmetrical Warfare and International Humanitarian Law", Part II, pp. 11-48 (DOI: 10.1007/978-3-540-49090-6_2), in W. von Heinegg and V. Epping, International Humanitarian Law Facing New Challenges Symposium in Honour of Knut Ipsen (Springer 2007).

M. N. Schmitt, *Bellum Americanum*: The US view of Twenty-first Century war and its possible implications for the law of armed conflict. *Mich. J. Int. Law*19, 4 (1998).

M. N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework",*37 Columbia Journal of Transnational Law 885-937* , reprinted as *Institute for Information Technology Applications (USAF Academy) Publication # 1*, July 1999.

M.N. Schmitt, "Wired warfare: Computer network attack and *jus in bello*", RICR Juin IRRC June 2002 Vol. 84 No 846, 365-399 < http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/5C5D5C/$File/365_400_Schmitt.pdf > Accessed 4 October 2010.

Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World (Copernicus Books, 2003);

Bruce Schneier, "The Threat of 'Cyberwar' Has Been Hugely Hyped," CNN, 7 July 2010, < http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/> Accessed 4 October 2010.

Scott J. Shackelford, "Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks," 4 November 2009. < http://ssrn.com/abstract=1499849> Accessed 4 October 2010.

Scott James Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", 2008, < http://works.bepress.com/scott_shackelford/5> Accessed 4 October 2010.

Shadowserver Foundation and The Information Warfare Monitor, "JR03-2010 - Shadows in the Cloud: Investigating Cybver Espionage 2.0", 6 April 2010 < http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0> Accessed 4 October 2010.

Thom Shanker, Cyberwar Nominee Sees Gaps in Law, New York Times, 14 April 2010, < http://www.nytimes.com/2010/04/15/world/15military.html?scp=1&sq=Cyberwar%20Nominee%20Sees%20Gaps%20in%20Law&st=cse > Accessed 4 October 2010.

WG Sharp Sr, "The Past, Present and Future of Cybersecurity,"4 J. Natl. Security L. and Policy 13 (2010)

WG Sharp, Sr., Cyberspace and the use of force, (Falls Church, Va.: Aegis Research Corp., 1999)

WG Sharp, Sr., Redefining National Security in Today's World of Information Technology and Emergent Threats, , 9 Duke Journal of Comp. & Int. Law. 383, 384 (1999)

Matthew Sklerov, "Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent," 201 Mil. L. Rev. 1-85 (2009).

Joanna Sugden, Pentagon hacker Gary McKinnon wins extradition reprieve, The Times, 21 May 2010 < http://www.timesonline.co.uk/tol/news/uk/crime/article7131780.ece> Accessed 4 October 2010.

Sun Tzu, On the Art of War, tr. Dr Lionel Giles (1910), E-book available at: < http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf> Accessed 4 October 2010

Baqir Sajjad Syed and Iftikhar A. Khan, 'No guarantee against repeat of Mumbai-like attacks', Dawn.Com, 22 January < http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/news/pakistan/03-gates-warns-of-militant-havens-ahead-of-pakistan-visit-ss-02 > Accessed 4 October 2010

James P. Terry, Book Review, *9 Duke J. of Comp. & Int'l L. 491 (1999)*

The Tor Project, Website, < http://www.torproject.org>. Accessed 4 October 2010

United Nations A/65/201, 30 July 2010, Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, <http://www.unidir.org/pdf/activites/pdf5-act483.pdf> Available 4 October 2010.

United Nations General Assembly Resolution 64/25

< http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/463/33/PDF/N0946333.pdf?OpenElement > Accessed 4 October 2010.

U.S.-China Economic and Security Review Commission (111 th Congress, First Session), Report to Congress of the U.S.-China Economic and Security Review Commission (November 2009). < http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf> Accessed 4 October 2010.

US Cyber-Consequences Unit, *Overview by the US-CCU of the Cyber-Campaign Against Georgia in August of 2008*, August 2009< http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf > Accessed 4 October 2010.

US House of Representatives Committee on Science, Subcommittee on Science and Technology, Hearing Charter, *Planning for the Future of Cyber Attack Attribution*, Thursday, July 15, 2010, 10:00 a.m. - 12:00 p.m. 2318 Rayburn House Office Building. < http://democrats.science.house.gov/Media/File/Commdocs/hearings/2010/Tech/15jul/Hearing_Charter.pdf > Accessed 4 October 2010.

Statement of Dr. David A. Wheeler, Institute for Defense Analyses, Information Technology and Systems Division, on Planning for the Future of Cyber Attack Attribution Before the

U.S. House of Representatives Committee on Science and Technology Subcommittee on Technology and Innovation, July 15, 2010. < http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Wheeler_Testimony.pdf > Accessed 4 October 2010.

C Williams, 'Cyber attacks will 'catastrophically' spook public, warns GCHQ - Cheltenham spies "cyber arms race"', *The Register*, 22 February 2010. < http://www.theregister.co.uk/2010/02/22/csoc_report/ > Accessed 4 October 2010.

C. Wild, S. Weinstein, N. MacEwan & N. Geach, Electronic & Mobile Commerce Law: An analysis of trade, finance, media and cybercrime in the digital age, University of Hertfordshire Press, 2011 (forthcoming).

T. C. Wingfield, J. B. Michael, and D. Wijesekera (2003), "Optimizing Lawful Responses to Cyber Intrusions," *dodccrp.org* [Online]. < http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf> Accessed 4 October 2010.

Dr. H.Y. Youm, Soon Chun Hyang University, Korea, Presentation, Regional Asia Information Security Exchange (RAISE) 2010 meeting, Singapore, March 2010.

Vivian Yeo, 'South Korea to take stab at bot law', ZDNet News, 13 July 2010 < http://www.zdnetasia.com/south-korea-to-take-stab-at-bot-law-62201317.htm > Accessed 4 October 2010.

---

[1] Pauline Reich is Professor at Waseda University School of Law and the Director of the Asia-Pacific Cyberlaw, Cybercrime and Internet Security Research Institute at Waseda University, Tokyo, Japan. Stuart Weinstein is Associate Head of the University of Hertfordshire School of Law, St Albans, Hertfordshire, United Kingdom. Charles Wild is Head of the University of Hertfordshire School of Law, St Albans, Hertfordshire, United Kingdom. Allan S. Cabanlong earned his Master of Science from Waseda University Graduate School of Global Information and Telecommunication Studies (2010) and is a Police Senior Inspector/Information and Communications Technology Officer with the Philippines National Police.

[2] J Broward *quoting* Lord West of Spithead, Parliamentary Under-secretary for Security and Counter-terrorism, 'Britain fends off flood of foreign cyber attacks', *The Observer*, (London March 7, 2010)

http://www.guardian.co.uk/technology/2010/mar/07/britain-fends-off-cyber-attacks Accessed 4 October 2010.

[3] Agence France Presse *quoting* US Senator Susan Collins, 'UN chief calls for treaty to prevent cyber war', *The Sydney Morning Herald*. (Sydney, 31 January 2010) < http://news.smh.com.au/breaking-news-world/un-chief-calls-for-treaty-to-prevent-cyber-war-20100131-n5t7.html > Accessed 4 October 2010.

[4] J Broward *quoting* Lord West of Spithead, Parliamentary Under-secretary for Security and Counter-terrorism, 'Britain fends off flood of foreign cyberattacks', *The Observer*,

(London March 7, 2010)

http://www.guardian.co.uk/technology/2010/mar/07/britain-fends-off-cyber-attacks/ Accessed 4 October 2010.

[5] Id.

[6] Id.

[7] *quoting* C Williams, 'Cyber attacks will 'catastrophically' spook public, warns GCHQ - Cheltenham spies "cyber arms race"', *The Register*, (London February 22, 2010)

http://www.theregister.co.uk/2010/02/22/csoc_report/ >

[8] Id.

[9] Id.

[10] M Libicki, *Cyberdeterrence and cyberwar,* (Santa Monica: The Rand Corporation, 2009), p. 15.

http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf Accessed 4 October 2010.

[11] See, e.g., Martin C. Libicki, *Cyberdeterrence and Cyberwar,* Rand Corporation (2009), http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf;*Conquest in Cyberspace, National Security and Information Warfare* Rand/Cambridge University Press (2007); *What is Information Warfare?* National Defense University, Institute for National Security Studies, (1995).

[12] Id., p. 5.

[13] Id., p. 5.

[14] Id., p. 5.

[15] Id., p. 179.

[16] Id., p. 179.

[17] Id., p. 3.

[18] Id., p. 179.

[19] Id., p. 179.

[20] Id., p. 179.

[21] Id., p. 179.

[22] Id., p. 179.

[23] Id., p. 180.

[24] Id., p. 180.

[25] Id., p. 180.

[26] Id., p. 180.

[27] Id., p. 180.

[28] Id., p. 180.

[29] Id., p. 187.

[30] Id.

[31] The Air Force Law Review - Cyberlaw Edition. 64 A.F. L. REV. (2009) is devoted to the a variety of cyberlaw issues arising in the context of the military. < http://www.afjag.af.mil/shared/media/document/AFD-091026-024.pdf > Accessed 4 October 2010.

[32] See "The Past, Present and Future of Cybersecurity,"4 J. Natl. Security L. and Policy 13 (2010).

[33] Sharp, Walter Gary, Sr., "Redefining National Security in Today's World of Information Technology amd Emergent Threats", 9 Duke Journal of Comp. & Int. Law. 383, 384 (1999)

[34] 'Asymmetric' players include non-state actors using technology to achieve a parity of some sorts with the entrenched leaders.

[35] Sharp defines this as the environment created by the confluence of cooperative

networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web; Id., at 384.

[36] Id., at 384.

[37] Id., at 384.

[38] Walter Gary Sharp, Sr., Cyberspace and the use of force, (Falls Church, Va.: Aegis Research Corp., 1999).

[39] James P. Terry, Book Review, *9 Duke J. of Comp. & Int'l L. 491 (1999).*

[40] Id., at 492.

[41] Biography Director of National Security Agency/Central Security Service, General Keith Alexander, Date Posted: Jan 15, 2009, Last Modified: Sep 17, 2010, Last Reviewed: Sep 17, 2010, National Security Agency/Central Security Service Website, < http://www.nsa.gov/about/leadership/bio_alexander.shtml> Accessed 4 October 2010.

[42] Id.

[43] Id.

[44] Thom Shanker, Cyberwar Nominee Sees Gaps in Law, New York Times, 14 April 2010 available at: < http://www.nytimes.com/2010/04/15/world/15military.html?scp=1&sq=Cyberwar%20Nominee%20Sees%20Gaps%20in%20Law&st=cse > Accessed 4 October 2010.

[45] Id.

[46] Id.; Unclassified Advance Questions for Lieutenant General Keith Alexander, US Army, Nominee for Commander, United States Cyber Command, Undated, < http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf > Accessed 4 October 2010.

[47] Id.

[48] Id.

[49] Unclassified Advance Questions for Lieutenant General Keith Alexander, US Army, Nominee for Commander, United States Cyber Command, Undated, < http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf > Accessed 4 October 2010.

[50] Title 10 of the United States Code outlines the role of armed forces in the United States Code. It provides the legal basis for the roles, missions and organization of each of the services as well as the United States Department of Defense.

[51] Ben Bain, "Cyber Command nominee lays out rules of engagement", Federal Computer Week, 16 April 2010, Testimony of General Alexander reproduced here with clarifications added in parentheses, < http://fcw.com/articles/2010/04/16/web-cyber-command-many-roles.aspx> Accessed 4 October 2010.

[52] Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the House of Representatives Committee on Armed Services, 23 September 2010, available at: < http://armedservices.house.gov/pdfs/FC092310/AlexanderStatement.pdf > Accessed 4 October 2010.

[53] Id., p. 6.

[54] Id., p. 6.

[55] John Markoff, "Step Taken to End Impasse Over Cybersecurity Talks," The New York Times, 16 July 2010, < http://www.nytimes.com/2010/07/17/world/17cyber.html > Accessed 4 October 2010.

[56] United Nations A/65/201, 30 July 2010, Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, available at: < http://www.unidir.org/pdf/activites/pdf5-act483.pdf> Accessed 4 October 2010.

[57] Id., Transmittal Letter.

[58] Id., Transmittal Letter.

[59] Id., Summary.

[60] Id.

[61] Id., p. 7.

[62] Id., p. 7.

[63] Id., p. 7.

[64] Id., p. 7.

[65] Id, p. 8; General Assembly Resolution 64/25 can be found at:

<http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/463/33/PDF/N0946333.pdf?OpenElement> Accessed 4 October 2010.

[66] See, for instance, Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law", 88 Texas L. Rev. 1571, < http://www.texaslrev.com/issues/vol/88/issue/7/kanuck> Accessed 4 October 2010.

[67] Baqir Sajjad Syed and Iftikhar A. Khan, 'No guarantee against repeat of Mumbai-like attacks', Dawn.Com, 22 January 2010< http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/news/pakistan/03-gates-warns-of-militant-havens-ahead-of-pakistan-visit-ss-02 > Accessed 4 October 2010.

[68] Professor Dr Henrik W.W. Kaspersen, Council of Europe - Project on Cybercrime, Draft 5 - Cybercrime and Internet Jurisdiction (March 2009), < http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf > Accessed 4 October 2010.

[69] Id., p.5.

[70] Id., p.5.

[71] Id., p.5

[72] Id., p. 6.

[73] Joanna Sugden, Pentagon hacker Gary McKinnon wins extradition reprieve, The Times, 21 May 2010 < http://www.timesonline.co.uk/tol/news/uk/crime/article7131780.ece > Accessed 4 October 2010.

[74] H.E. Jaak Aaviksoo, "Strategic Impact of Cyber Attacks," Isamaa ja Res Publica Liit, 5 March 2010, < http://www.irl.ee/en/Media/Articles/1927/strategic-impact-of-cyber-attacks > Accessed 30 September 2010.

[75] Id.

[76] Estonia Cybersecurity Strategy for 2008-2013 (2008), < http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf> Accessed 4 October 2010.

[77] NATO Cooperative Cyber Defence Centre of Excellence Tallinn, < https://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD > Accessed 4 October 2010

[78] NATO and Cyber Defence: Mission Accomplished? Rex B. Hughes, http://www.atlcom.nl/site/English/nieuws/wp-content/Hughes.pdf; NATO PA-173 DSCFC 09 E bis - NATO and Cyber Defence, < http://www.nato-pa.int/default.asp?SHORTCUT=1782> Accessed 4 October 2010.

[79] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified, Cooperative Cyber Defence Centre of Excellence Legal Task Team, November 2008. < http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf > Accessed 4 October 2010.

[80] Id., p. 4.

[81] Id., p. 31.

[82] Id., p. 31.

[83] US Cyber-Consequences Unit, *Overview by the US-CCU of the Cyber-Campaign Against Georgia in August of 2008*, August 2009< http://www.registan.net/wp-

content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf > Accessed 4 October 2010.

[84] Id., p. 3.

[85] Id., p. 3.

[86] Id., p. 9.

[87] < http://www.rsaconference.jp/english/> Accessed 4 October 2010.

[88] Lim Chang-Won, S. Korean websites 'attacked by North Korea', Agence France Presse, 7 July 2009. < http://www.google.com/hostednews/afp/article/ALeqM5j0fiT6uNbuYyzji1rIU1jTa6cmJA > Accessed 4 October 2010.

[89] Dr. H.Y. Youm, Soon Chun Hyang University, Korea, Presentation, Regional Asia Information Security Exchange (RAISE) 2010 meeting, Singapore, March 2010.

[90] ICANN No. 36 - 25-30 October 2009, Seoul, Korea < http://sel.icann.org/> Accessed 4 October 2010.

[91] Lolita C. Bolder, "White House Among Targets of Cyber Attack", 8 July 2009, Associated Press, < http://www.msnbc.msn.com/id/31800532/> Accessed 4 October 2010.

[92] Kyodo News Service, "Eight Japanese Computer Servers Suspected in July Cyber Attack," BBC Monitoring International Reports, 12/17/09 via LEXIS.

[93] "South Korean Daily 'Cyber Attack from UK-based IP Address, Not North', The Financial Times Limited, BBC Monitoring Service, 7/15/09, via LEXIS

[94] "Document Shows North Korea Ordered Cyber Attacks - South Spy Agency,"

The Financial Times Limited, BBC Monitoring Service, 7/11/09, via LEXIS

[95] Id.

[96] Vivian Yeo, 'South Korea to take stab at bot law', ZDNet News, 13 July 2010< http://www.zdnetasia.com/south-korea-to-take-stab-at-bot-law-62201317.htm > Accessed 4 October 2010.

[97] AFP Tokyo, "Japan suspects Chinese cyber attacks," Taipei Times, 19 September 2010, page 5, < http://www.taipeitimes.com/News/world/archives/2010/09/19/2003483219>; see also, Japan Today, "Cyber attacks suspected on Defense Ministry, police agency websites,"19 September 2010< http://www.japantoday.com/category/crie/view/cyberattacks-suspe ...> Accessed 4 October 2010.

[98] U.S.-China Economic and Security Review Commission (111 th Congress, First Session), 2009 Report to Congress of the U.S.-China Exonomic and Security Commission (November 2009), p. 179. < http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf > Accessed 4 October 2010.

[99] Id., p. 179.

[100] Id., p. 168.

[101] Id.

[102] Id., p. 181.

[103] Mark Clayton, 'Google cyber attacks a 'wake-up' call for US, intel chief says', Christian Science Monitor, 4 February 2010, < http://www.csmonitor.com/USA/2010/0204/Google-cyber-attacks-a-wake-up-call-for-US-intel-chief-says> Accessed 4 October 2010.

[104] Id.

[105] See for more information, Josh Rogin, The top 10 Chinese Cyber Attacks (that we know of), The Cable, 22 January 2010< http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of> Accessed 4 October 2010.

[106] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", Foreign Affairs, September/October 2010< http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain > Accessed 4 October 2010.

[107] Id.

[108] Id.

[109] Ellen Nakashima, "Defense official discloses cyber attack", The Washington Post, 24 August 2010, < http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html > Accessed 4 October 2010.

[110] Id.

[111] Id.

[112] Greylogic, Project Grey Goose, Phase I Report, 17 October 2008 < http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report > Accessed 4 October 2010.

[113] Greylogic, Project Grey Goose, Phase II Report, 20 March 2009 available at:

< http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report > Accessed 4 October 2010.

[114] Id., p. 3.

[115] Id., p. 4.

[116] Id., p. 5.

[117] < http://en.wikipedia.org/wiki/GhostNet> Accessed 4 October 2010.

[118] Id.

[119] Id.

[120] Id.

[121] Shadowserver Foundation and The Information Warfare Monitor, "JR03-2010 -

Shadows in the Cloud: Investigating Cybver Espionage 2.0", 6 April 2010. <http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0> Accessed 4 October 2010.

[122] J A Lewis, "The "Korean" Cyber Attacks and Their Implications for Cyber Conflict",

Center for Strategic and International Studies, October 2009 < http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf > Accessed 18 March 2010.

[123] For a technical overview of the problem of attribution see Appendix A.

[124] Lewis, op cit., p. 2.

[125] Lewis, op cit., p. 2.

[126] US House of Representatives Committee on Science, Subcommittee on Science and Technology, Hearing Charter, *Planning for the Future of Cyber Attack Attribution*, Thursday, July 15, 2010, 10:00 a.m. - 12:00 p.m.

2318 Rayburn House Office Building. < http://democrats.science.house.gov/Media/File/Commdocs/hearings/2010/Tech/15jul/Hearing_Charter.pdf > Accessed 4 October 2010.

[127] Id.

[128] Id.

[129] Statement of Dr. David A. Wheeler, Institute for Defense Analyses, Information Technology and Systems Division, on Planning for the Future of Cyber Attack Attribution Before the U.S. House of Representatives

Committee on Science and Technology Subcommittee on Technology and Innovation, July 15, 2010, p. 53.

< http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Wheeler_Testimony.pdf > Accessed 4 October 2010.

[130] Id., p. 39.

[131] Id.

[132] Id.

[133] Id.

[134] Id.

[135] Id.

[136] Id.

[137] Robert K. Knake, International Affairs Fellow, Council on Foreign Relations, *Untangling Attribution: Moving to Accountability in Cyberspace*, Prepared statement before the Subcommittee on Technology and Innovation, Committee on Science and Technology United States House of Representatives, 15 July 2010, p. 4.

< http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Knake_Testimony.pdf > Accessed 4 October 2010.

[138] Id., p. 4.

[139] Knake, op cit., p.4.

[140] Id. at 7.

[141] Statement of Edward J. Giorgio, President and Co-Founder, Ponte Technologies, Before the House of Representatives Committee on Science and Technology, Planning for the Future of Cyber Attack Attribution, 15 July 2010, p. 12. < http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Giorgio_Testimony.pdf > Accessed 4 October 2010.

[142] Id., p. 13.

[143] Testimony and Statement for the Record of Marc Rotenberg, President, Electronic Privacy Information Center, and Adjunct Professor, Georgetown University Law Center, Hearing on "Planning for the Future of Cyber Attack Attribution" Before the Committee on Science and Technology Subcommittee on Technology and Innovation U.S. House of Representatives, July 15, 2010, p.1. < http://democrats.science.house.gov/Media/file/Commdocs/hearings/2010/Tech/15jul/Rotenberg_Testimony.pdf > Accessed 4 October 2010.

[144] Id., p. 1.

[145] Id., p. 1.

[146] Id., p. 3.

[147] Georgios Dementis and Gonçalo Sousa, A LEGAL REASONING COMPONENT OF A NETWORK SECURITY COMMAND AND CONTROL SYSTEM, Thesis, Naval Postgraduate School, Monterrey, California, March 2010, p. 22., < http://edocs.nps.edu/npspubs/scholarly/theses/2010/Mar/10Mar_Dementis.pdf > Accessed 4 October 2010.

[148] M. N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework",*37 Columbia Journal of Transnational Law 885-937* , reprinted as*Institute forInformation Technology Applications (USAF Academy) Publication # 1*,July 1999. See also Schmitt, M. N.,*Bellum Americanum*: The US view of Twenty-first Century war and its possible implications for the law of armed conflict. *Mich. J. Int. Law*19, 4 (1998), pp. 1051-1090.

[149] James B. Michael, Thomas C. Wingfield and Duminda Wijesekera, Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System, *Proc. Twenty-seventh Annual Int. Computer Software and Applications Conf.*, IEEE (Dallas, Tex., Nov. 2003). < http://www.au.af.mil/au/awc/awcgate/nps/ws09-with-pub-info.pdf > Accessed 4 October 2010.

[150] Id., p.1.

[151] M.N. Schmitt, "Wired warfare: Computer network attack and *jus in bello*", RICR Juin IRRC June 2002 Vol. 84 No 846, 365-399, 375 < http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/5C5D5C/$File/365_400_Schmitt.pdf > Accessed 4 October 2010; See also M.N. Schmitt. "Asymmetrical Warfare and International Humanitarian Law", Part II, pp. 11-48 (DOI: 10.1007/978-3-540-49090-6_2), in W. von Heinegg and V. Epping, International Humanitarian Law Facing New Challenges Symposium in Honour of Knut Ipsen (Springer 2007).

[152] Id., p. 377.

[153] Id., p. 379.

[154] Id., p. 399.

[155] Michael N. Schmitt, Computer Network Attach and the Useof Force in International Law: Thoughts on a Normative Framework, (1999) 37 Colum. J. Transnat'l L. 885, 914.

[156] Id., at 914.

[157] Id., at 914.

[158] Id., at 914.

[159] Id., at 915.

[160] Id., at 915.

[161] Id., at 915.

[162] T. C. Wingfield, J. B. Michael, and D. Wijesekera (2003), "Optimizing Lawful Responses to Cyber Intrusions," *dodccrp.org* [Online]. <http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf> Accessed 4 October 2010.

[163] Dementis and Sousa, Op cit., p. 21.

[164] *Quoting* Michael, Wingfield and Wijesekera, *Op Cit.*, p. 2.

[165] Id., p. 4.

[166] Id., p. 3.

[167] Id., p. 3.

[168] Id., p. 3.

[169] Knake, *Op Cit.*, p. 4.

[170] Lewis, op cit., p. 2.

[171] Lewis, op cit., p. 3.

[172] Matthew Sklerov, "Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent," 201 Mil. L. Rev. 1-85 (2009).

[173] Id. at 74.

[174] Dr. Sandro Gaycken, "The Necessity of (Some) Certainty - A Critical Remark

Concerning Matthew Sklerov's Concept of 'Active Defense'", Journal of Military and Strategic Studies, Vol.. 12, Issue 2, Winter 2010 at 6.

[175] W Owens, K Dam and H Lin, Technology, Policy, Law and Ethic Regarding U.S. Acquisition and

Use of CYBERATTACK CAPABILITIES, (Washington, D.C.: The National Academies Press, 2009:< http://www.nap.edu/openbook.php?record_id=12651&page=1>, x. Accessed 4 October 2010.

[176] For example, Richard Clarke and Admiral Mike McConnell vs Bruce Schneier, Marc Rotenberg and various civil liberties organizations, and perhaps White House Cybersecurity Czar Howard Schmidt. See Michael Cheek, "Cyber Debate Finds No Exaggeration in Threat of Cyber War," June 10, 2010, < http://www.thenewnewinternet.com/2010/06/10/cyber-debate-finds-no-exaggeration-in-threat-of-cyber-war/ > Accessed 4 October 2010; and RSA clips, Schneier and Neustar Proudly Welcomes the Intelligence Squared U.S. Debate 'The Cyber War Threat Has Been Grossly Exaggerated' to Washington,", FierceCIO, 25 May 2010, < http://www.fiercecio.com/press-releases/neustar-proudly-welcomes-intelliegence-swauared-u-s-debate-cyber-war-threat-hs ... > Accessed 4 October 2010; Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to do About It, (Harper Collins: April 2010); Bruce Schneier, Beyond Fear: Thinking Sensibility About Security in an Uncertain World (Copernicus Books, 2003); Bruce Schneier, "The Threat of 'Cyberwar' Has Been Hugely Hyped," CNN, 7 July 2010, < http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/> Accessed 4 October 2010; Tim Green, Quiz: Separate Cyber Security Fact from Fiction, < www.cio.com/article/505375/Quiz_Separate_Cyber-Security_Fact_From-Fiction > Accessed 4 October 2010.; Jim Harper, "Cybersecurity: A Meaningless Term", Cato Institute, DailyPodcast, 2 July 2009. < http://www.cato.org/dailypodcast.podcast-archive.php?podcast_id=937 > Accessed 4 October 2010.

[177] Irving Lachow, "Cyber Terrorism: Menace or Myth?", in Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, Cyberpower and National Security Center for Technology and National Security Policy, National Defense University and Potomac Books, Inc., 2009 at p. 439.

[178] Elgin Brunner, Anna Michalkova, Manuel Suter, Myriam Dunn Cavelty, Focal Report 3: Critical Infrastructure Protection - Cybersecurity - Recent Strategies and Policies: An Analysis, CRN Reports, (Center for Security Studies (CSS), ETH Zurich (2009) (pp. 16-17).

[179] Id.

[180] See, e.g., Tim Gray, "U.N. telecom boss warns of pending cyberwar," 10 September 2010, MSNBC, < http://www.msnbc.msn.com/id/39102447 > Accessed 4 October 2010.

[181] Lachow, 441, citing Arquilla and Ronfelt at 30.

[182] Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia,"' in Franklin D. Kramer,et al, at 466, citing Pu Duanhua, "Network Control: New Access Control Concerning Outcome of Future War, *China National Defense News,* February 8, 2007.

[183] Peter J. Denning and Dorothy E. Denning, "The Profession of IT: Discussing Cyber

Attack," 53 Communications of the ACM, No. 9, at 29,30, 9/10.

[184] Lachow at 441.

[185] Earl, Robert S. and Norman E. Emery, A Terrorist Approach to Information Operations, Thesis, M.S. in Defense Analysis, Naval Postgraduate School, June 2003 at 24.

[186] Lewis, *Op cit,* p. 2.

[187] Id., p. 2.

[188] Id., p. 3.

[189] Id., p. 6.

[190] Scott J. Shackelford, "Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks," 10 February 2010, page 7, < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849 > Accessed 4 October 2010.; See also Scott James Shackelford. 2008. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law" < http://works.bepress.com/scott_shackelford/5> Accessed 4 October 2010.

[191] Id., p. 7.

[192] Id., p. 7.

[193] Id., p. 7.

[194] Id., p. 8.

[195] Id., p. 8.

[196] Id., p. 8.

[197] Id., p. 8.

[198] Franz-Stefan Gady and Greg Austin, Russia, The United States and Cyber Diplomacy: Opening the Door, The EastWest Institute, 16 September 2010. < http://www.ewi.info/russia-united-states-and-cyber-diplomacy-opening-doors > Accessed 4 October 2010.

[199] EastWest Institute, Press Statement, 14 September 2010 < http://www.ewi.info/russia-united-states-and-cyber-diplomacy-opening-doors > Accessed 4 October 2010.

[200] Gady and Austin, Op cit., p. 23.

[201] Id., p. 23.

[202] Id., p.23.

[203] Quote attributed to George Orwell.

[204] Reporters Without Borders, *Enemies of the Internet - Countries Under Surveillance,* 12 March 2010, < http://www.rsf.org/IMG/pdf/Internet_enemies.pdf> Accessed 4 October 2010.

[205] Id., p. 3.

[206] Id., p. 4.

[207] See testimony of Robert K. Knake, July 15, 2010, op cit pages 7-8: "The vision of perfect attributing can best be summed up as the idea of giving packets license plates. Under such a system, compromised systems or the proxies could not be used to hide the identity of attackers because each packet would be labeled with a unique identifier, possibly an IPv6 address that has been assigned to an individual after having that individual's identity authenticated in some verifiable way. Access to the network would require authentication, and each packet produced by the user would be traceable back to that user. The privacy implications of such a system would be obvious, turning the Internet into the ultimate tool of state surveillance. The security benefits for pursuing criminals and state actors, however, would be minimal. Without cooperation from all foreign states, criminal activity would simply gravitate to states that do not authenticate identity before issuing identification numbers or choose not to participate in the system at all…"

[208] Agence France Presse *quoting* US Senator Susan Collins, 'UN chief calls for treaty to prevent cyber war',

The Sydney Morning Herald . (Sydney, 31 January 2010)

< http://news.smh.com.au/breaking-news-world/un-chief-calls-for-treaty-to-prevent-cyber-war-20100131-n5t7.html >

Accessed 18 March 2010.

[209] Id.

[210] Id.

[211] Id.

[212] Id.

[213] Id.

[214] See, e.g., Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," <http://works.bepress.com/scott_shackelford/5/> (2008) at 27-46 Accessed 4 October 2010; Why Strategic Cyber Warfare Shouldn't Be a Military Priority, Interview with Martin C. Libicki, Rand Corp., October 14, 2009, < http://www.govinfosecurity.com/podcasts.php?podcastID=354> Accessed 4 October 2010; David Perera, "Lewis: Cold War lessons of limited value for cyber attack deterrence," 7 July 2010, Fierce GovernmentIT, available at: < http://www.fiercegovernmentit.com/story/lewis-cold-war-lessons-limited-value-cyber-attack-deterrence/2010-07-07 > Accessed 4 October 2010.

[215] Owens et al., op cit., pp. 241-244.

[216] Id., p. 244.

[217] Id., p. 244.

[218] Id., p. 244.

[219] See Section VII. A. Testimony of Dr David Wheeler above.

[220] Sun Tzu, On the Art of War, tr. Dr Lionel Giles (1910), E-book <

http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf> Accessed 4 October 2010.

[221] Id., p. 8.

[222] J. Hunker, R. Hutchinson, R. and J. Marguiles, "Critical Information Protection II", International Federation for Information Processing, Volume 290, eds. Papa, M., Shenoi. S., (Boston: Springer, 2008), pp 87-99.

[223] See National Security Agency, "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments" (Undated).

< www.nsa.gov/ia/_files/support/defenseindepth.pdf > Accessed 4 October 2010; Victor Hazelwood, Defense-In-Depth, An Information Assurance Strategy for the Enterprise, 2006. < http://www.sdsc.edu/~victor/DefenseInDepthWhitePaper.pdf> Accessed 4 October 2010.

[224] Ibid.

[225] Ibid.

[226] < http://www.torproject.org> Accessed 4 October 2010.