Steps towards Monitoring Cyberarms Compliance

Neil C. Rowe[1], Simson L. Garfinkel[1], Robert Beverly[1], and Panayotis Yannakogeorgos[2]
[1]U.S. Naval Postgraduate School, Monterey, California, USA
[2]Air Force Research Institute, Maxwell AFB, Alabama, USA
ncrowe at nps dot edu
slgarfin at nps dot edu
rbeverly at nps dot edu
yannakog1 at gmail dot com

Abstract

Cyberweapons are difficult weapons to control and police. Nonetheless, technology is becoming available that can help. We propose here the underlying technology necessary to support cyberarms agreements. Cyberweapons usage can be distinguished from other malicious Internet traffic in that they are aimed precisely at targets which we can often predict in advance and can monitor. Unlike cybercriminals, cyberweapons use will have political goals, and thus attackers will likely not try hard to conceal themselves. Furthermore, cyberweapons are temperamental weapons that depend on flaws in software, and flaws can get fixed. This means that cyberweapons testing will be seen before a serious attack. As well, we may be able to find evidence of cyberweapons on computers seized during or after hostilities since cyberweapons have important differences from other software and are difficult to conceal on their development platforms. Recent advances in quick methods for assessing the contents of a disk drive can be used to rule out irrelevant data quickly. We also discuss methods for making cyberweapons more responsible by attribution and reversibility, and we discuss the kinds of international agreements we need to control them.

Keywords: cyberweapons, cyberattacks, agreements, monitoring, forensics, reversibility

This paper appeared in the Proceedings of the 10th European Conference on Information Warfare and Security, Tallinn, Estonia, July 2011.

1 Introduction

Cyberweapons are software that can be used to achieve military objectives by disabling computer systems, networks, or key functions of them. They can be malicious software installed secretly through concealed downloads or deliberate plants by human agents, or they can be attempts to overload online services. Cyberweapons are a growing component in military arsenals (Libicki 2007). Increasingly countries are instituting "cyberattack corps" with capabilities to launch attacks in cyberspace on other countries as an instrument of war, either alone or combined with attacks by conventional military forces (Clarke and Knake 2010). Cyberattacks seem appealing to many military commanders in comparison to conventional arms. They seem to require fewer resources to mount since their delivery can be accomplished in small payloads such as malicious devices or packets. They also seem "cleaner" than conventional weapons in that their damage is primarily to data and data can be repaired, although they are they are difficult to control and often perform actions close to perfidy, outlawed by the laws of war (Rowe 2010 JTE). Cyberweapons can be developed with modest technological infrastructure, even by underdeveloped countries (Gady 2010) taking advantages of international resources. So there is a particular threat of cyberattacks from "rogue states" such as North Korea and terrorist groups that hold extreme points of view.

Many of the information-security tools we use to control threats and vulnerabilities with the common criminal cyberattacks (Brenner 2010) will aid against the cyberweapon threat. Good software engineering practices, access controls, and system and network monitoring all help. But they are insufficient to stop cyberattacks today because of the increasing numbers of cyberattacks and the inherent weaknesses of these countermeasures. State-sponsored cyberattacks will be even harder to stop because they can exploit significant resources and could be more sophisticated than the attacks common today. They will likely employ a variety of methods simultaneously to have a high probability of success, and they can be tested thoroughly under a range of circumstances. Most current defensive measures will probably be useless against them.

2 Approach

What can be done against such threats? We believe that countries must negotiate international agreements similar to those for nuclear, chemical, and biological weapons. Such agreements (treaties, conventions, protocols, and memoranda of understanding) (Croft 1996) can dictate the ways in which cyberweapons can be used, as for instance stipulating that countries agree to use cyberweapons only in defense to a cyberattack or in a serious crisis. Agreements can require action against hacker groups within a country as part of that country's internal policing so that a nation cannot shift blame for cyberattacks and cyberweapons onto them. Very little has been done in proposing such agreements to date. It is time to plan out what such agreements will entail and how they should be enforced. The EastWest Institute in the U.S. recently proposed a cyberwar "Geneva Convention" (Rooney 2011).

(Johnson 2002) was skeptical in 2002 of the ability to implement cyberarms control, citing the difficulty of monitoring compliance. But the evolution of attacks since 2002 undermines many of his arguments. Cyberweapons are no longer a "cottage industry" but require significant infrastructure for finding exploits, finding targets, gaining access, managing the attacks, and concealing the attacks, and this infrastructure leaves traces. This is because target software, systems, and networks are becoming increasingly hardened and complex, and attacking them is becoming harder; and also because vulnerabilities are being found and fixed faster than ever. Also, digital forensics has advanced significantly since 2002, making it possible to determine all kinds of things from analysis of disk drives. Some technologies central for criminal cyberattacks today like code obfuscation have little legitimate use and are good indicators of cyberattack development, and we expect that the technologies used by cyberweapons will be similar.

Thus we think international agreements on cyberweapons are worth the effort even though finding cyberweapons and observing their use is hard. The situation is similar to that with chemical weapons for which there are, for example, many methods for making mustard gas that can use common chemicals with legitimate uses. Although proving that a facility is used for chemical or biological weapons production is difficult, the type of equipment at a facility can give a good probability that it has been used to manufacture such weapons, as U.N. inspectors realized in Iraq in the 1990s when they discovered evidence of airlocks in alleged food-production facilities. International conventions banning chemical and biological weapons having been effective despite the difficulties of verifying production and stockpiling of such weapons (Price 1997). We think that similar examinations, and therefore conventions, should be possible in the cyberdomain. Even if developers of cyberweapons delete or hide evidence on their disks, there are many ways to retrieve it (Garfinkel 2006). We should start researching now how to perform effective cyberinspections.

We realize that policy is too often driven by crises, so it may take a serious cyberattack to interest a country in negotiating cyberarms limitations. Such a cyberattack is technically feasible (Clarke and Knake 2010) and could happen at any time. We need to be ready with proposals if it happens. In the meantime, progress can be made by the United Nations in negotiating broad cyberarms agreements. Such agreements could be helpful when rogue countries such as North Korea and terrorist organizations threaten the development of cyberwarfare capabilities and broad international cooperation is possible.

Two recent cases provide motivation. One is the cyberattacks on Georgia in August 2008 discussed in (Rowe 2010 ECIW). These were denial-of-service attacks against predominantly Georgian government Web sites. They were effective but there was collateral damage from the imprecision of the attack. Evidence suggests that private interests in Russia were responsible for the attacks (USCCU 2009). The other case is the "Stuxnet" worm and corresponding exploits targeting SCADA systems (Markoff 2010). These used traditional malware methods for modifying programs. Since Stuxnet targeted industrial systems with no associated financial incentive, it was clearly developed by an information-warfare group of a nation-state. It appears that Stuxnet was discovered because it spread well beyond its intended target. Nevertheless, in November 2010 it was reported that Stuxnet may have been successful in destroying multiple uranium processing centrifuges that are part of the Iranian nuclear effort.

3 Details

To achieve international agreements on cyberweapons, we see four issues: (1) locating them on computers; (2) noticing

their use; (3) encouraging the more responsible kinds of cyberweapons; and (4) choosing appropriate types of agreements.

3.1 Analysis of drives to find cyberweapons

The U.S. analyzed a number of captured computers and devices in its recent military operations in Iraq and Afghanistan. This was useful in identifying insurgent networks and their interconnections. Similarly, we believe that a good deal can be learned about a country's cyberweapons from the computers used to develop or deploy them. As part of a negotiated settlement of a conflict, a country may agree to forego cyberweapons, and may agree to submit to periodic inspections to confirm this (United Nations 1991).

Detection of cyberweapons might seem difficult. But there are precedents in the detection of nuclear, chemical, and biological weapons (O'Neill 2010). Cyberweapons development generally requires unusual computer usage in secret facilities since most cyberweapons require secrecy to be effective, which rules out most software development facilities. Clues to cyberweapons can also be found inside computers. Certain types of software technology such as code obfuscation and spamming aids are good clues to malicious intent. Code for known attacks (for providing reuse opportunities) and stolen proprietary code such as Windows source code (for testing attacks) are other good clues. Technologies such systematic code testers, "fuzzing" utilities, and code for remote control of other computers provide supporting evidence of cyberweapons development though they have some legitimate uses. Data alone can be a clue, such as detailed reconnaissance information on adversary computer networks. Diversity of software techniques is a clue to cyberweapons development because the unreliability of cyberweapons requires use of multiple methods as backup. Once suspected cyberweapons are found, they can be studied systematically to confirm their nature using malware analysis (Malin, Casey, and Aquilina 2008).

A cyberweapon inspection regime would have to be performed on-site and with automated tools, as a party to a cybermonitoring regime would not allow a potential adversary to remove materials from a secret facility. Cyberweapon monitors would likely be required to use bootable CD-ROMs that would contain programs to analyze the contents of a computer system and look for evidence of cyberweapon development. Inspection would require a scheme for management of the necessary passwords and keys for the systems inspected, which could be aided by key escrow methods. Inspection regimes should also require "write-blockers" to assure that the monitors did not themselves plant cyberweapons on the systems being monitored. Other useful ideas from monitoring of nuclear capabilities (O'Neill 2010) include agreed inspector entry into the inspected country within a time limit, allowed banning of certain inspectors, designation of off-limits areas, and limits on what kind of evidence can be collected.

A good prototype of what can be done in analysis of drives is our work on the Real Data Corpus, our collection of drive images (mostly disks) collected from around the world. Currently this collection includes more than 2000 disk images. Recent work has characterized disks and drives as a whole, including understanding of the type of user and the type of usages (Rowe and Garfinkel 2010). Clusters of files that have no counterpart in others in a corpus are particularly interesting, and can be the focus of more detailed forensic analysis. For faster assessment, random sampling of fragments taken from the middle of a file can accurately identify different types of data (Garfinkel et al. 2010). Tools for detecting deception markers are also useful since illegal cyberweapons development would need to be concealed. Deception could be in the form of deleted, renamed, or encrypted files, and could be enhanced by other techniques such as changing the system clock or manipulating a log file.

3.2 Network monitoring for cyberweapons

There are many tools to discriminate legitimate from abusive network traffic. Such inferential intrusion detection has limitations due to the difficulty of defining malicious traffic in a sufficiently general way without incurring a large number of false positives (Trost, 2010). But the attack landscape is different for politically and economically motivated state-sponsored cyberattacks:

1. ***Targets***: State-sponsored attacks will be targeted to particular regions and political agendas, in contrast to most criminals, who target victims indiscriminately.

2. ***Sophistication***: Cyberarms will be the product of well-funded nations with significant resources. Thus they will use new and sophisticated techniques rather than the common simpleminded attacks we see on the Internet. That may mean their initial stages may be hard to detect. However, as with all weapons, they must eventually

produce a significant effect, and at that point their use will be obvious.

3. ***Attribution***: As with conventional warfare, the warring parties will likely follow specified (nondigital) protocols. Protocols will likely dictate that combatants reveal who they are at least in general terms.

These features mean that there will be clues to cyberweapons use in the nature of the targets, the sophistication and effectiveness of the attack, and the ability to attribute them. We can use conventional network monitoring to detect significant attacks; for instance, the denial of service in the Georgia attacks was easy to recognize. This does require a sufficiently broad deployment of network-traffic vantage points, secured both physically and virtually from tampering. One approach to deploying them is to have the vantage points be entirely passive and communicate over separate infrastructure via encrypted and authenticated channels. Centralization is an issue in the monitoring; the United Nations would probably want a centralized approach if they are to monitor. Ideally, a vantage point should exist at the ingress to each important network of a country, capable of full-rate traffic processing. If this is difficult, random sampling of traffic can be done. The monitoring infrastructure could be realized via government mandate or as part of efforts to enable wiretap compliance.

Whereas the targeting of a criminal attack is often widespread and indiscriminate to obtain maximum victimization rates and profit to the criminal (although there are exceptions for some sophisticated financial scams), cyberweapons are likely to be much more focused. A cyberweapon might attack a particular country, a type of service (e.g. electrical grid or water systems), or systems used by a certain political, ethnic or religious persuasion. Both the Georgia and Stuxnet attacks employed moderately focused targeting (insufficiently focused according to critics). However, potential vulnerabilities and attack vectors will not correlate much with targets and there must be significant testing. This complicates the job of the attacker and requires additional tools beyond those used in purely criminal endeavors. We can use this difference to our advantage in detecting cyberweapons development. Cyberweapons by their nature are complex pieces of software that include components for penetrating remote systems, controlling the remote systems, and propagating to other systems. Understanding the behavior of a cyberweapon in isolation, or in simulated environments is difficult – the more secret the testing, the less like the real world it will be, and the less accurate it will be at predicting real-world performance. We can see this demonstrated in the poor initial performance of complex new conventional weapons systems such as aircraft. We expect that countries wishing to employ cyberweapons will first unobtrusively try them against real targets to understand their real-world efficacy. An example is the attacks on Estonia in 2007 prior to the attacks on Georgia in 2008. The breadth of the initial testing provides a clue to forthcoming cyberweapons use.

Thus, detecting pre-hostility events at the network level is possible. It can be aided by metrics for detecting national or political bias in the targets of malicious network traffic. Standard statistical techniques can suggest that the victims represent a particular political perspective or country's interest more than a random sample would (Rowe and Goh 2007). For instance, a significance test on a linear metric encoding political or social agendas can provide a first approximation, while the Kullback-Leibler divergence can characterize the extent of difference between expected and observed traffic distributions. How do we identify the political or social agenda to search for? This requires help from experts on international relations. Nations have longstanding grievances with other nations, and particular issues are more sensitive in some nations than others. We can enumerate many of them and identify associated Internet sites.

We expect other properties of the observable network traffic to provide precursors to attack. Feature selection methods in finding discriminating network traffic features (Beverly and Sollins 2008) provide a start. Network-flow data may be sufficient for early warnings (Munz and Carle 2007). It will work well in tracking and analyzing attacks supported by hacker groups, such as the Chinese hacker groups (Hvinstendahl 2010) that are harnessed to attack Western organizations at times of political or social grievances against them. We also can look for particular sequences of events indicative of a systematic attack, say a broadcast of many footprinting packets followed by more specific footprinting, something not seen much in criminal cyberattacks.

An additional tool useful in detecting cyberweapons development is a decoy, a site deliberately designed to encourage attacks. A decoy can be designed to be more useful than a normal site by narrowing its content to just that necessary to invoke a response. A decoy can also be equipped with more detailed monitoring of its usage that would not be possible for most sites, and should use honeypot technology to implement attack resilience and intelligence-gathering capabilities that are not easily disabled. Decoys do not generally raise ethical concerns because they are passive, but guidelines should be followed in their use (Rowe 2010 JTE) since decoys are used by phishers.

Data fusion on World Wide Web usage can complement our network monitoring. If a country's government shows a

sudden increase in visits to hacker Web sites, it may suggest cyberweapons development.

3.3 Encouraging more-responsible cyberattacks

International agreements can stipulate the manner in which cyberwarfare can be conducted. Two important aspects of this are attribution and reversibility of attacks. For attribution, a responsible country will find it in their interests to make their attacks clear in origin to better enable desired political and social effects of an attack, which are often more important than the actual military value. The ability to trace the Georgia cyberattacks back to Russia without too much trouble suggests such an political effect was intended. Contrarily, it could be useful to a country to be able to prove it was not the source of a cyberattack for which it is being blamed. Attribution can be done by digital signatures attached to attack code or data that identify who is responsible for an attack and why. They could be concealed steganographically (Wayner 2002) to avoid providing a clue to the victim that they are being attacked. For attacks without code like denial of service, a signature can be encoded in the low-order bits of the times of the attacks.

Nations should also be encouraged to use attack methods that are more easily repairable, following the same logic behind the design of easily removable landmines. (Rowe 2010 ECIW) proposed four techniques that can be used to make cyberattacks that are easier to reverse by the attacker than by the victim even when the victim tries to restore from backup (Dorf and Johnson 2007). They are: (1) encryption of key software and data by the attacker where the victim does not have the key to decrypt it; (2) obfuscation of a victim's system by the attacker by data manipulations that are hard to understand yet algorithmic and reversible; (3) withholding by the attacker of key information that is important to the victim; and (4) deception by the attacker of the victim to make them think their systems are not operational when they actually are. In the first two cases, reversal can be achieved by software operations by the attacker; in the third case, the attacker can restore missing data; and in the fourth case, the attacker can reveal the deception.

How do we encourage attackers to use reversible attacks? There are several incentives. One would be if the attacker will eventually need to pay reparations, as the United Nations could stipulate as part of a negotiated settlement of a conflict (Torpey 2006). Even in an invasion or regime change, it is likely that the impacts of cyberweapons will need to be mitigated—indeed, the perceived possibility of mitigation will likely drive the adoption of cyberweapons. Another incentive comes from international outcry at using unethical methods and the resulting ostracism of the offending state, as with the use of biological weapons. Another incentive is if a victim is likely to respond in like kind, wherein use of a reversible attack could encourage an adversary to do the same because otherwise they would appear to be escalating the conflict (Gardam 2004). Also, nonreversible attacks could be interpreted as violating the laws of warfare in regard to unjustified force when reversible methods are easily available. Responses of the international community to analogous such violations include sanctions, boycotts, fines, and legal proceedings (Berman 2002).

3.4 Support for international cooperation

Global cybersecurity is hindered by a lack of cybersecurity action plans at the national level (Ghernouti-Helie 2010). Reducing vulnerabilities and threats from cyber attack requires the policy community to support norms of behavior among states, enforceable at the national level, to secure the "cyber commons". The 2010 U.S. *Quadrennial Defense Review* advocates strengthening international partnerships to secure the cyber domain using technical, legal and organizational cooperation, and a recent U.S. GAO report (USGAO 2010) recommended that the U.S. "establish a coordinated approach for the federal government in conducting international outreach to address cybersecurity issues strategically."

Several international agreements dealing with cybercrime can serve as models for cyberarms control. The Council of Europe Convention on Cybercrime, adopted in November 2001, seeks to align domestic substantive and procedural laws for evidence gathering and prosecution, and to increase international collaboration and to improve investigative capabilities for coordinating E.U. efforts on cyber crimes. Adopted and ratified by the US in 2007, it is considered a model law for the rest of the world. The World Summit on the Information Society Declaration of Principles endorsed a global culture of cybersecurity that is promoted, developed, and implemented in cooperation with all stakeholders and international expert bodies. The International Telecommunications Union (ITU) and U.N. General Assembly have also passed several resolutions addressing the criminal misuse of information. The efforts of the ITU have culminated in the International Multilateral Partnership against Cyber Threats (IMPACT) although the United States does not currently support it. IMPACT is a Global Response Centre based in Cyberjaya, Malaysia. It was set up in 2009 to serve as the international community's main cyberthreat resource by proactively tracking and defending against cyberthreats. The center's alert and response capabilities include an Early Warning System that enables IMPACT members to identify and

head off potential and imminent attacks before they can inflict damage on national networks.

Many of the ideas mentioned here benefit from international cooperation (Yannakogeorgos 2010; Yannakogeorgos 2011). An example is sharing of data collected from monitoring of the Internet (Erbschloe 2001). Data on just source address, destination address, and packet size is not very sensitive or subject of privacy concerns, and should be useful to share even when traffic is encrypted. The European Convention on Cybercrime makes a step in that direction. So that appears to be a good initial focus for international agreements on sharing of data, and not just for cyberweapons tracking.

Other agreements could focus on mandating technology that will aid in managing a cyberweapons threat. An example would be a mandate for countries to use IPv6 instead of IPv4 to enable better attribution of events on the Internet; rogue states could be told that they cannot connect to the Internet unless they use IPv6. Other mandates could stipulate architectures in which attribution of traffic is easier such as minimum requirements on persistence of cached records. Other useful agreements could prohibit less-controllable attacks such as worms and mutating viruses, to achieve better discrimination of military from civilian targets in cyberattacks (Shulman 1999).

Criminal prosecution of a nation's hacker groups by its government could be an important stipulation of agreements. For instance, when Philippine hackers in 2000 launched a virus that attacked computers worldwide and the Philippine government was initially unhelpful, improvements under international pressure were subsequently made by it, both legally and managerially, to enable a better response in the future. Other possible agreements could follow those of traditional arms control, as for instance a commitment to use cyberweapons only in self-defense, or agreed export controls on cyberweapons technology. We do need to make legal distinctions between cybercrime, cyberconflict, cyberespionage and cyberterror as this is necessary when creating a regulatory regime for cyberweapons (Wingfield 2009). One model that could be studied is the Wassenaar Arrangement for export controls, which could be extended to information technology products.

4 Conclusion

Cyberarms agreements have been said to be impossible. But technology is changing that. We can seize and analyze drives on which cyberweapons were developed; we can detect the necessary testing of cyberweapons; we can create incentives for self-attributing and reversible cyberattacks; and we can develop and ratify new kinds of international agreements. While we cannot stop cyberweapons development, we may be able to control its more dangerous aspects much as we control chemical, biological, and nuclear weapons, and limit it to responsible states. It is time to consider seriously the possibility of cyberarms control.

References

Berman P. (2002) "The Globalization of Jurisdiction," *University of Pennsylvania Law Review,* Vol. 151 No. 2, pp. 311-545.

Beverly, R., and Sollins, K. (2008) "An Internet Protocol Address Clustering Algorithm," USENIX SysML Workshop.

Brenner, S. (2010) *Cybercrime: Criminal Threats from Cyberspace*, Santa Barbara, CA, US: Praeger.
Clarke, R., and Knake, R. (2010) *Cyberwar: The Next Threat to National Security and What To Do about It*, New York, US : HarperCollins.

Croft, S. (1996) *Strategies of Arms Control: A History and Typology,* Manchester, UK: Manchester University Press.

Dorf, J., and Johnson, M. (2007) "Restoration Component of Business Continuity Planning," in Tipton, H., and Krause, M. (Eds.), *Information Security Management Handbook, Sixth Edition*, Boca Raton, FL, US: CRC Press, pp. 1645-1654.

Erbschloe, R. (2001) *Information Warfare: How to Survive Cyber Attacks,* Berkeley, CA, US: Osborne/McGraw-Hill, 2001.

Gady, F.-S. (2010, March 24) "Africa's Cyber WMD," *Foreign Policy*.

Gardam, J. (2004) *Necessity, Proportionality, and the Use of Force by States,* Cambridge, UK: Cambridge University Press.

Garfinkel, S. (2006, September) "Forensic Feature Extraction and Cross-Drive Analysis," *Digital Investigation*, Vol. 3, Supplement 1, pp. 71-81.

Garfinkel, S., Roussev, V., Nelson, A., and White, D. (2010) "Using Purpose-Built Functions and Block Hashes to Enable Small Block and Sub-File Forensics," DFRWS, Portland, OR.

Ghernouti-Helie, S. (2010) *A National Strategy for an Effective Cybersecurity Approach and Culture,* New York, US : IEEE Press.

Johnson, P. (2002) "Is It Time for a Treaty on Information Warfare?" in Schmitt, M., and O'Donnell, B., *Computer Network Attack and International Law (International Law Studies Volume 76)*, pp. 439-455, Newport, RI, US: Naval War College.

Hvistendahl, M. (2010, March 3) "China's Hacker Army," *Foreign Policy*.

Libicki, M.(2007) *Conquest in Cyberspace: National Security and Information Warfare,* New York, US: Cambridge University Press.

Malin, C., Casey, E., and Aquilina, J. (2008) *Malware Forensics: Investigating and Analyzing Malicious Code*, Syngress.

Markoff, J. (2010, September 26) "A Silent Attack, But Not a Subtle One," *New York Times*, p. A6.

Mel, H., and Baker, D. (2000) *Cryptography Decrypted, 5th edition,* Boston, MA, US: Addison-Wesley Professional.

Munz, G., and Carle, G. (2007, May) "Real-Time Analysis of Flow Data for Network Attack Detection," *Proc. 10th IFIP/IEEE Intl. Symposium on Integrated Network Management*, pp. 100-108.

O'Neill, P. (2010) *Verification in an Age of Insecurity: The Future of Arms Control Compliance*, New York, US: Oxford.

Price, R. (1997) *The Chemical Weapons Taboo*, Ithaca, NY, US: Cornell University Press.

Rooney, B. (2011, February 4) "Calls for Geneva Convention in Cyberspace," *Wall Street Journal*.

Rowe, N. (2010) "The Ethics of Cyberweapons in Warfare," *Journal of Technoethics*, Vol. 1, No. 1, pp. 20-31 [JTE].

Rowe, N. (2010, July) "Towards Reversible Cyberattacks," *Proc. 9th European Conference on Information Warfare and Security*, Thessaloniki , Greece [ECIW].

Rowe, N., and Garfinkel, S. (2010, May) "Global Analysis of Disk File Times," *Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland CA.

Rowe, N., and Goh, H. (2007, June) "Thwarting Cyber-Attack Reconnaissance with Inconsistency and Deception," 8th IEEE Information Assurance Workshop, West Point, NY, pp. 151-158.

Shulman, M. (1999) "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law,* Vol. 37, pp. 939-968.

Torpey J. (2006) *Making Whole What Has Been Smashed: On Reparations Politics*, Cambridge, MA, US: Harvard University Press.

Trost, R. (2010) *Practical Intrusion Analysis*, Upper Saddle River, NJ, US: Addison-Wesley.

United Nations (1991) *Final Document: Third Review Conference of the Parties to the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction*, BWC/DONF.II/23, Geneva, Switzerland.

USCCU (United States Cyber Consequences Unit) (2009, August) "Overview by the US-CCU of the Cyber Campaign

against Georgia in August of 2008," US-CCU Special Report, downloaded from www.usccu.org.

USGAO (United States Government Accountability Office) (2010, March 5) "Cybersecurity: Progress Made But Challenges Remain in Defining and Coordinating the Comprehensive National Initiative," Washington, D.C., US: Government Accountability Office.

Wayner, P. (2002) *Disappearing Cryptography: Information Hiding: Steganography and Watermarking,* San Francisco, CA, US: Morgan Kaufmann.

Wingfield, T. (2009) "International Law and Information Operations," in Kramer, F., Starr, S., and Wentz, L. (Eds.), *Cyberpower and National Security,* Washington DC: National Defense University Press, pp. 525-542.

Yannakogeorgos, P. (2010, October) "Cyberspace, The New Frontier - And the Same Old Multilateralism," in Reich, S., *Global Norms, American Sponsorship and the Emerging Patterns of World Politics.* Houndsmills, UK: Palgrave.

Yannakogeorgos, P. (2011) "Promises and Pitfalls of the U.S. National Strategy to Secure Cyberspace," Carlisle, PA, US: Army War College.

The views expressed are those of the author and do not represent those of any part of the U.S. Government.