Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2008 Proceedings | Southern (SAIS)

3-1-2008

Law and Cyber War

Dennis D. Strouble
Air Force Institute of Technology, dennis.strouble@afit.edu

Mary C. Carroll
National Defense University, carrollm@ndu.edu

LAW AND CYBER WAR

Dennis D. Strouble
Air Force Institute of Technology
dennis.strouble@afit.edu

Mary Cole Carroll
National Defense University
carrollm@ndu.edu

ABSTRACT

The internet has created enormous global changes. People can interact with others anyplace, anytime almost instantly. Much of the infrastructure including energy, healthcare, and telecommunications is interconnected globally. The world has added another domain to international conflicts: Cyber War. In this paper, we explore legal principles which would be involved in a cyber attack. Existing laws of warfare applied in the physical realm do not translate equally as well in the cyber domain. Due to the difficulty of attribution, the invisibility of borders and the need to react quickly, we may need to develop legal principles that allow immediate and appropriate responses. This is an area that needs very careful and thoughtful review

Keywords

Law, cyber war, LOAC, attribution

1. Introduction

The internet has created enormous global changes. People can interact with others anyplace, anytime almost instantly. Much information and knowledge is available to anyone with an internet connection and many countries have public facilities like cyber cafes or libraries that freely provide that connection. Much of the infrastructure including energy, healthcare, and telecommunications is interconnected globally. One discipline struggling to deal with the internetted world is the law. In this article, we explore some fundamental legal issues involved in an attack in cyber space.

In April of 2007, a series of cyber attacks effectively shut down much of the communication infrastructure of the country of Estonia. This was widely reported in the media and often referred to as the "Estonia Cyberwar". Most of the attacks were distributed denial of service attacks where pings and bots were used to spam websites so that the websites were unable to handle the traffic. The attacks continued for weeks and were more sophisticated than generally used methods. The "cyber war" was sparked by Estonia relocating a Soviet-era memorial and war graves in Tallinn. Banks, parliament, government agencies, and news media were the main targets. There was no conclusive evidence to link the attacks to the Russian Government, although there was speculation that the attacks were government sponsored if not government led.

A number of cyber events have involved the United States; among these is "Titan Rain," a series of attacks thought to have been initiated by China against several networks including defense contractors, national laboratories, and NASA. In fact, the United States Military and many private companies have multiple daily attacks on their networks ranging from simple spam to more serious attacks such as denials of service and installing Trojans, virus, and other malware.

Our existing laws make a distinction between an attack by a nation state which may be deemed an act of war and an action by others which is typically determined to be a criminal action. The "classification" of the attacker is just one of a number of factors which influences what organizations are involved and what rules, laws, and policies are applied.

2. Criminal Acts

In 2000, McConnell International produced a report which looked at cyber crime and punishment. They analyzed the current state of the law in 52 nations and found that only a small fraction has amended their laws to cover even a majority of the different types of cyber crimes that needed to be addressed. They found that even though there were initiatives underway, a great deal of work needed to be done. They reported that a major problem was the transnational nature of cyberspace. "Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow." (McCornnell,

2000, p. 1) Things have not changed much since then and there continue to be major issues if a criminal cyber attack involves multiple nations. Several authors have highlighted the urgency of finding an effective solution.

3. Nation State Acts

If an attack is determined to be that of a nation state, then another set of laws, rules, and policies applies.

The United States has well-defined rules of engagement and follows international laws of war in the traditional physical domains (e.g., land, sea, air, and space). The increasing use of information technology has caused a new domain to be added - cyber space.

3.1 United States Code Issues

U.S. Code Title 50 (War and National Defense) put in place restrictions on the intelligence community, all departments of the executive branch are required to keep Congress "fully and currently informed of all intelligence activities." The President must determine in a written finding that the action has "an identifiable foreign policy or national security objective for the United States". The President specifies which agencies are authorized to participate in such actions including the military. Title 50 also applies if the United States is assisting or supplying information to other nations.

Title 10 of the United States Code (Armed Forces), governs military activities. In military operations there is no requirement to report to Congress. However, the War Powers Act of 1973 (Public Law 93-148), does require the president to notify Congress when forces are deployed and provides that they are to be withdrawn within sixty days unless there is a formal declaration of war by Congress. This requirement may not apply if the action is categorized as "preparation of the battlefield".

Thus there are differing requirements depending on how an action is characterized. "This dichotomy between Title 10 and Title 50 presents even more difficult problems when it comes to activities in the cyber world and in space, which are increasingly vital to the conduct of military, intelligence, and diplomatic activities." (Smith, 2007, p 547)

The United States Air Force is working to address these issues. In a National Press Club event entitled "Victory in Cyberspace," the commander of the new Cyber Command, Lt. Gen. Robert J. Elder recognized the importance of resolving the Title 10 and Title 50 issues when conducting operations in cyberspace (Bejtlich 2007). He also pointed out that while operating under Title 32, the Air National Guard may have more latitude to help local governments and commercial and private organizations with network defense. The reasoning is that under the Posse Comitatus Act (18 U.S.C. § 1385), federal military members and United States National Guard while under federal authority are prohibited from performing in a law enforcement capacity within the United States, except where expressly authorized by the Constitution or Congress. When not in federal service the National Guard is governed by U.S. Code Title 32 (National Guard). One approach might be to add Air National Guard personnel in every state to provide support cyber defense operations.

3.2 The Law of Armed Conflict (LOAC)

The military is required, by policy, to comply with the laws of war in all operations, not just armed conflict.

> "Members of the DoD components comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations." Department of Defense Directive (2006)

The international rules that govern how nations conduct wars are known collectively as the Law of War or The Law of Armed Conflict (LOAC). The purpose is to minimize suffering and unnecessary damage and to regain peace. The Law of War has developed through a series of conventions, primarily The Hague and Geneva Conventions. The LOAC requires that United States military organizations comply with several principles:

1. Necessity: only that degree of force required to defeat the enemy is permitted. In addition, attacks must be limited to military objectives whose "nature, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization at the time offers a definite military advantage";
2. Distinction or Discrimination: requires distinguishing military objectives from protected civilian objects such as places of worship and schools, hospitals, and dwellings;
3. Proportionality: requires that military action not cause collateral damage which is excessive in light of the expected military advantage;

4. Humanity: prohibits the use of any kind or degree of force that causes unnecessary suffering; and
5. Chivalry: requires war to be waged in accordance with widely accepted formalities, such as those defining lawful "ruses" (e.g. camouflage and mock troop movements) and unlawful treachery (for example, misusing internationally accepted symbols in false surrenders) (Waldrop, 2004).

The interpretation of these principles must be determined on a case by case basis. In a thoughtful law review article, CDR Antolin-Jenkins, a Navy JAG Officer, argues that international law allows actions if the cyber attack uses force. It is unclear how far a nation would have to go in a cyber attack to fit within this framework. "Expanding the term "use of force" to encompass cyber attacks which constitute economic aggression is likely to have the effect of opening the door widely to other acts which the United States has long held constitute permissible acts of influence through economic forces." This expanded interpretation of "use of force" might have serious unforeseen and unintended consequences. (Antolin-Jenkin, p. 21**).** It is also unclear how these principles would be applied to actions taken against telecommunication, utilities, health care systems, and other components of the national infrastructure.

Another issue that is raised by the law of war is the status of those who work on cyber defense but are not in uniform. The laws of war give specific protections in terms of status to combatants (e.g. prisoner of war status) that may not be afforded to civilians. Generally the rules apply if the person is wearing identifiable uniform and carrying arms openly. As the U.S. military continues to rely more and more on civilians, both government employees and contractors, their status is unclear (Turner & Norton, 2001). Also the National Strategy to Secure Cyberspace calls on the private sector to respond to cyber threats placing them in an uncertain position. (Hoffman, 2003, p. 421)

4. Difficulties in Attribution

The "classification" of the attacker determines whether military involvement is appropriate. [Depending on who is the attacker, where the attack is coming from, what is being attack and how the attack is being carried out, different rules apply.] In our current internet society, people share information on a daily basis for all type of purposes. Criminals are getting more sophisticated in the use of information technology. Criminals without those skills are finding cyber attacks easier to accomplish. Hacking tools, with video tutorials on how to use them, are available for free. "Script Kiddies" or individuals with little knowledge can find already written code to accomplish their desired actions. These attacks can range from simple vandalism to coordinated attacks against national infrastructure. The roles, responsibilities and applicable rules depend upon attribution – or the "classification" of the attacker. Identification of the cyber attack source requires identification of the physical location of the attacking system (e.g., tracing the attack back and attributing it to a specific IP address), identification of the system(s) controlling the attacking system (in many cases the attacking system is an "agent" of the actual attacker), identification of the individuals responsible for initiating the attack, and, possibly, identification of the organization that is sponsoring the attack (Denning 2005). In rare cases, all four of these elements can resolve to a single individual. More commonly, each of the four elements is a separate entity, significantly complicating the investigation.

The need to fuse information from commercial, governmental, intelligence, and military communities often complicates the investigation and can add a significant amount of delay. In an environment where attacks can occur in less than a second, the need to be in a position to react and respond in a timely fashion cannot be over emphasized (Robb 2007). The investigation team must understand the political boundaries, cultural factors (differences?), and legal jurisdictions where the attack originated, propagated, and targeted. In many cases, the factor (these factors?) can result in barriers that impede or inhibit the investigation. Even in the best of circumstances, it may be impossible to obtain the information needed to attribute the attack quickly enough to enable an immediate response.

Also, it may be impossible to identify the attacker with any degree of certainty as recent events in Estonia have shown. The attackers could be teenage hackers, criminals, commercial interests, patriots acting to support a country, dissidents within the country, terrorists, a nation state or any of these impersonating any of others. There are private citizens in the United States who are monitoring and disrupting Al Qaeda websites. The hackers group, "The Cult of the Dead Cow", after the events of Sept. 11, offered to assist the government in cyber anti-terrorist incidents. If actions of this type are deemed to fall under the laws of war, the consequences for the individuals and actions taken against them are vastly different than if they are found to be criminals (Hoffman, 2003). Much depends upon attribution, and, in a cyber attack, attribution is not an easy task.

Determining the location of the attack may be impossible. A cyber attack may come from hundreds of locations or countries. The actor may have taken over "zombies" around the world or on various satellites in space. Many of these "zombies" might not know or even suspect that their servers or computers are involved. Internet addresses may not determine the location or they may be "spoofed" to show false information. Pinpointing the source of the attack may well affect the actions taken to

counter the attack. "The Internet is quickly making geographic borders metaphorical. Where actions with legal significance consist of streams of electrons taking varying paths among computers all over the world, we need to adjust our laws' conception of 'place.' There are a variety of rules we could adopt to fit events occurring over the Internet into pre-existing categories; there are a variety of alternative models we could adopt instead. Some of the conventional models, though, are clearly unworkable: We don't now have, and seem unlikely to develop, any way to put border guards between computers located in different jurisdictions to examine all of the electrons streaming through. Governments, lawyers, and legal scholars are just beginning to think about these questions in a systematic way" (Litman, 1996).

It may be impossible to classify the actions: Most attackers try to hide the true nature of their attacks. Things that may seem to be innocent or a mere annoyance may conceal malware. Little things done on a large scale may have enormous consequences. "A decade ago, Chinese military theorists like the infamous colonels Qiao Liang and Wang Xiangsui were already hinting at the importance of simultaneously striking multiple infrastructure layers in a confrontation with the U.S. In theory, the breakdown of one system would compound the effects on another, and the crippling of energy, government services, communications, the media, and health care and financial systems would interact in a downward spiral" (Peters, 2007).

5. U.S Response

In setting up the Department of Homeland Security, the President established the National Strategy to Secure Cyberspace. The strategy acknowledged that there are a number of roles for the government, but stated that "In general, the private sector is best equipped and structured to respond to an evolving cyber threat" (Whitehouse webpage, National Strategy to Secure Cyberspace). The private sector has been inconsistent on its ability to protect its own interests and assets. With the interconnectedness of the internet, vulnerability for one entity may create problems for other nodes on the network. Voluntary, individual, defensive measures on the part of the private sector also will not provide the overall protection needed.

There are Federal organizations in place to handle cyber attacks. United States Computer Emergency Readiness Team (US-CERT) is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. National Cyber Response Coordination Group (NCRCG), made up of 13 Federal agencies, is the principal Federal agency mechanism for cyber incident response. In the event of a nationally significant cyber-related incident, the NCRCG will help to coordinate the Federal response, including US-CERT, law enforcement, and the intelligence community.

It is clear, under both international law and national policy, that in a cyber attack on the nation, military components can take whatever passive defensive actions needed. What remain unclear are the active defensive actions or offensive actions that are permitted. Immediately the type and source of the attack must be identified, the proper federal agency must respond in the correct manner. In order for the military to take actions, other than passive defense, it must be determined that the attacker was of a nation state. Otherwise it is a criminal matter and must be handled by law enforcement.

6. Other International Laws

The recent attacks on Estonia should serve as a wakeup call to all nations to explore the adequacy of the existing United Nations (UN) Charter when applied to cyber attacks (Robb 2007). The world condemnation that a physical attack against Estonia would have evoked did not occur in response to a cyber attack. The UN Charter is most concerned with physical attack when compared to diplomatic sanctions or economic boycotts. However, it was not written to address cyber attacks where the critical infrastructure of a nation could be attacked in seconds

There are other treaties, such as the Outer Space Treaty, Moon Treaty, and the International Telecommunication Convention that also might affect how laws are interpreted regarding cyber attacks but these were either not signed by all of nations, including the United States, or were clearly written without the internet in mind.

7. Conclusions

In this paper, we have identified challenges that would be faced in a cyber attack situation. Existing laws of warfare applied in the physical realm do not translate equally as well in the cyber domain. Due to the difficulty of attribution, the invisibility of borders and the need to react quickly, we may need to develop legal principles that allow immediate response when based on good faith or when the defender is in hot pursuit. This is an area that needs very careful and thoughtful review. This

presentation in this paper is not comprehensive, but should provide the reader some insight into the difficulties that will be faced when significant cyber attacks occur.

8. Disclaimer

The views expressed in this article are those of the authors and do not reflect the official policy or position of the Air Force Institute of Technology, The National Defense University, United States Air Force, Department of Defense, or the United States Government.

References

1. Antolin-Jenkins, V. (2005), "Article, Essay & Note: Defining the Parameters of cyberwar operations: Looking for law in all the wrong places?" *Naval Law Review*, Vol. 51, pp 132-174.
2. Bejtlich, R. (2007). Air Force Cyberspace Report, TaoSecurity, October 12, 2007, http://taosecurity.blogspot.com/2007/10/air-force-cyberspace-report.html
3. Condron, S. (2007), "Getting it right: Protecting American Critical Infrastructure in Cyberspace", *Harvard Journal of Law & Technology*, Spring, Vol 20, No. 2, pp 404-422.
4. Creekman, D. (2002), "NOTES AND COMMENTS: A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China", *American University International Law Review*, Vol. 17, pp 641-674.
5. Denning, D.E. (2005). Cyber Attack Attribution: Issues and Challenges. Center for Terrorism and Irregular Warfare, Department of Defense Analysis, Naval Postgraduate School. http://www.cyberconflict.org/pdf/attribution2.ppt.
6. Department of Defense Directive (2006), Number 2311.01E, DoD Law of War Program.
7. Hoffman, M.H. (2003), "The legal status and responsibilities of private internet users under the law of armed conflict: a Primer for the unwary on the shape of law to come", 2 *Washington University Global Studies Law Review*, Vol. 2, pp 415-426.
8. Hollis, D, (2007), "New Tools, New Rules: International Law and Information Operations", *Legal Studies Research Paper Series, Temple University Beasley School of Law,* No. 2007-15, pp 1-18.
9. Jensen, E. (2002) "ARTICLE: Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense", Stanford Journal of International Law, Vol. 38, pp 207-240.
10. Litman, J. (1996), "SYMPOSIUM: The Internet: Law without borders in the information age" *Wayne Law Review* Vol. 43, pp 95-98.
11. McConnell International, (2000), "Cyber Crime...and Punishment? Archaic Laws Threaten Global Information", http://www.mcconnellinternational.com/services/cybercrime.htm
12. Peters, R. (2007) "Washington ignores cyberattack threats, putting us all at peril" *Wired Magazine*, September 2007, pp 168-169.
13. Robb, J. (2007). When Bots Attack. Wired Magazine, August 23, 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots
14. Smith, J. (2007), "Symposium: State intelligence gathering and international law: Keynote Address", *Michigan Journal of International Law,* Spring, Vol. 28, pp 543-552.
15. The National Strategy to Secure Cyberspace (2007) http://www.whitehouse.gov/pcipb/
16. The National Cyber Security Division of the Department of Homeland Security http://www.dhs.gov/xabout/structure/editorial_0839.shtm
17. Turner, L.L. & Norton, L. G. (2001) "Civilians at the tip of the spear – Department of Defense total force team", *Air Force Law Review*, Spring, Vol. 51, pp 1-110.

18. Waldrop, E. (2004) "Integration of military and civilian space assets: legal and national security implications", *Air Force Law Review*, Spring, Vol. 55, pp 157-231.