CHAPTER

13

Legal System Impacts

INFORMATION IN THIS CHAPTER

- Legal Systems
- Key U.S. Laws
- Privacy Impacts
- Digital Forensics

The legal aspects of cyber warfare have been woven throughout this book as they are integral to the discussion of doctrine, ethics, and legal precedence based on similar circumstances. We covered the challenges with defining what a cyber war is and the changing definition of war in Chapter 1. We talked about how the cyber domain compares and contrasts to sea and space issues in Chapter 3. We reviewed aspects of attack versus exploit (espionage) versus defense and the many national policy issues in Chapter 4. This chapter will address the ubiquitous challenges of cyber across both warfare and commercial issues. Then in Chapter 14 we will address the ethical concepts we have codified into law such as the idea of "humane war" or "law of armed conflict" and Bellum Iustum (Just War Theory) that have come out of the lessons from the world wars in Europe. This chapter will address these concepts briefly and discuss how they are impacted and implemented in cyberspace.

First, we must analyze how the current laws, the foundation of which is the Law of Armed Conflict (LOAC), impact cyber warfare. The LOAC arises from a desire among civilized nations to prevent unnecessary suffering and destruction while not impeding the effective waging of war. A part of public international law, LOAC regulates the conduct of armed hostilities. It also aims to protect civilians, prisoners of war, the wounded, sick, and shipwrecked. LOAC applies to international armed conflicts and in the conduct of military operations and related activities in armed conflict; however such conflicts are characterized [1]. Conflicts or wars are divided into two categories: *jus ad bellum* (justification for going to war) and *jus in bello* (how war is fought). The latter, governed by United Nations Charters, the Geneva conventions, and the Hague conventions, has codified many of the existing customary international legal principles for warfare.

http://dx.doi.org/10.1016/B978-0-12-416672-1.00013-1

Next, we need to understand what an act of war and *use of force* are. Within the United States act of war is determined by the president. Use of force has different meanings for governments at war and law enforcement agencies (LEAs)—both center on actions taken whose impact forces the target to do something. This is often measured on a graduated scale or continuum. These acts must be carried out by lawful combatants (someone authorized by a sovereign nation) to fall under these guidelines. There are also noncombatants/bystanders and unlawful combatants/terrorists. These are much easier to identify in a traditional conflict but in an insurgency or in cyberspace they can become illusive.

Because the language used to develop these rules does not easily translate into cyberspace, there is no commonly accepted international understanding on how they will apply to this new war fighting domain. With that said, there have been two recent documents and one speech that have contributed greatly to national and international understanding. The first document is from the NATO Cooperative Cyber Defence Centre of Excellence: *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, published in 2013 and written at the invitation of the Centre by an independent "International Group of Experts." It is the result of a 3-year effort to examine how extant international law norms apply to this "new" form of warfare. The Tallinn Manual consists of "rules" adopted unanimously by the International Group of Experts that are meant to reflect customary international law, accompanied by "commentary" that delineates their legal basis and highlights any differences of opinion among the Experts as to their interpretation in the cyber context [2].

Following are the key conclusions from the manual:

- States may not knowingly allow cyber infrastructure located in their territory to be used for acts that adversely affect other States.
- States may be responsible for cyber operations directed against other States, even though those operations were not conducted by the security agencies. In particular, the State itself will be responsible under international law for any actions of individuals or groups who act under its direction. For instance, a State that calls on hacktivists to conduct cyber operations against other States will be responsible for those actions as if it had conducted them itself.
- The prohibition on the use of force in international law applies fully to cyber operations. Though international law has no well-defined threshold for determining when a cyber operation is a use of force, the International Group of Experts agreed that, at a minimum, any cyber operation that caused harm to individuals or damage to objects qualified as a use of force.
- The International Group of Experts agreed that cyber operations that merely cause inconvenience or irritation do not qualify as uses of force.
- States may respond to unlawful cyber operations that do not rise to the level of a use of force with countermeasures. Countermeasures are actions that would otherwise be unlawful were they not in response to the unlawful actions of another State. As an example, if one State disrupts communications in another, it would be lawful for the target State to respond by conducting disruptive cyber operations of its own.
- A State that is the victim of a cyber "armed attack" may respond by using force. The force may be either cyber or kinetic. In international law, an "armed attack" is a "grave" use of force. Any cyber operation that results in death or significant damage to property qualifies as an armed attack.

- The majority of the International Group of Experts agreed that non-State actors, such as cyber terrorists, are capable of conducting armed attacks, to which the victim State could respond in self-defense. In other words, the matter is not solely one of law enforcement. In certain circumstances, it would be permissible to use force against those cyber terrorists when they are located in other States.
- Under international law, it is possible that a conflict consisting entirely of cyber operations would qualify as an "armed conflict" to which international humanitarian law would apply. This is important because not only does international humanitarian law contain certain protections for individuals and objects during an armed conflict, but it also gives immunity to combatants for certain actions, such as intentionally killing the enemy, which would otherwise be unlawful.
- During an armed conflict, commanders and other superiors may be criminally responsible for ordering cyber operations that constitute war crimes or for failing to stop such operations when committed by their subordinates.
- Although there is no prohibition in international humanitarian law on civilians—such as hacktivists—conducting cyber operations during an armed conflict, if they do so, they sometimes become legitimate targets.
- Not all cyber operations directed against civilians and civilian objects are prohibited during an armed conflict. Instead, international humanitarian law primarily addresses operations that qualify as an "attack."
- The majority agreed that an attack is a cyber operation that causes injury or death to individuals or damage or destruction to objects or which interferes with the functionality of cyber infrastructure in a manner that requires repair. Therefore, these experts would conclude that cyber operations directed against the civilian population or civilian objects are not prohibited by international humanitarian law when they merely cause disruption, irritation, and inconvenience.
- Directing a cyber operation against a civilian is a war crime if it injures the civilian or was likely to do so.
- It is unlawful to use cyber attacks to spread terror among the civilian population.
- Cyber weapons must be the subject of a legal review before they can be fielded on the battlefield.
- It is unlawful to launch a cyber attack that is not directed at a lawful target and which therefore would indiscriminately cause damage to civilians and civilian objects.
- During armed conflict, cyber operations must be employed against a target if they are militarily feasible in the circumstances and would result in less harm to civilians and civilian objects than the use of conventional weaponry.
- The special protections that medical and religious personnel, medical units, and medical transports have under international humanitarian law apply fully with respect to cyber operations directed against them. The same is true with regard to "objects indispensable to the survival of the civilian population" like medical supplies, food stores, and water treatment facilities.

In general, these conclusions show that cyber operations could qualify as use of force but the same rules apply to cyber operations in the physical world. They detail the different aspects of the law and apply it to cyber operations. The first two bullets are important to many countries as it ties responsibility for cyber operations back to the nation-state.

The next influential document is the Department of Defense Cyberspace Policy Report A *Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* November 2011 [3]. Following are extracts from answers to the thirteen specific questions on cyber policy for both DoD and the U.S. Government posed in Senate Report 111-201.

1. The development of a declaratory deterrence posture for cyberspace, including the relationship between military operations in cyberspace and kinetic operations. The Committee believes that this deterrence posture needs to consider the current vulnerability of the U.S. economy and government institutions to attack, the relatively lower vulnerability of potential adversaries, and the advantage currently enjoyed by the offense in cyberwarfare.

   Answer: The President's May 2011 International Strategy for Cyberspace states that the United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these national security and vital national assets as necessary and appropriate.
   Deterrence in cyberspace, as with other domains, relies on two principal mechanisms: denying an adversary's objectives and, if necessary, imposing costs on an adversary for aggression.
   This will be done with like-minded nations.
   Deterrence is a whole-of-government proposition. DoD supports the White House Cybersecurity legislative proposal to protect the American people, U.S. critical infrastructure, and our government's networks and systems more effectively.
2. The necessity of preserving the President's freedom of action in crises and confrontations involving nations which may pose a manageable conventional threat to the United States but which in theory could pose a serious threat to the U.S. economy, government, or military through cyber attacks.

   Answer: The Department recognizes that a nation possessing sophisticated and powerful cyber capabilities could attempt to affect the strategic calculus of the United States. Any state attempting such a strategy would be taking a grave risk. Our efforts focus on the following three areas:
   - First, the Department, in conjunction with the Intelligence Community and Law Enforcement agencies, strives to secure the best possible intelligence about potential adversaries' cyber capabilities.
   - Second, the Department recognizes that strong cyber defenses and resilient information architectures, particularly those connected to critical infrastructure, mitigate the ability of a future adversary to constrain the President's freedom of action. If future adversaries are unable to cripple our centers of gravity, they will be more likely to understand that the President has the full menu of national security options available.
   - Finally, the President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by DoD.

3. How deterrence or effective retaliation can be achieved in light of attribution limitations.

   Answer: The same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage. DoD actively seeks to limit the ability of such potential actors to exploit or attack the United States anonymously in three ways:

   - First, the Department seeks to increase our attribution capabilities by supporting innovative research and development in both DoD and the private sector. This research focuses on two primary areas: developing new ways to trace the physical source of an attack, and seeking to assess the identity of the attacker via behavior-based algorithms.
   - Second, the Department has significantly improved its cyber forensics capabilities over the past several years. The Intelligence Community and U.S. Cyber Command continue to develop a highly skilled cadre of forensics experts.
   - Third, in partnership with the Department of Homeland Security, DoD is expanding its international partnerships to increase shared situational awareness, warning capabilities and forensics efforts.

4. To the extent that deterrence depends upon demonstrated capabilities or at least declarations about capabilities and retaliatory plans, how and when the Department intends to declassify information about U.S. cyber capabilities and plans to demonstrate capabilities.

   Answer: Effective deterrence in cyberspace is founded upon both the security and resilience of U.S. networks and systems, and ensuring that the United States has the capability to respond to hostile acts with a proportional and justified response. The International Strategy for Cyberspace provides a clear statement that the United States reserves the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests in cyberspace.

5. How to maintain control of or manage escalation in cyberwarfare, through, for example, such measures as refraining from attacking certain targets (such as command and control and critical infrastructure).

   Answer: The unique characteristics of cyberspace can make the danger of escalation especially acute. For instance, the speed of action and dynamism inherent in cyberspace, challenges of anonymity, and the widespread availability of malicious tools can compound communications and increase opportunities for misinterpretation. As a result, DoD recognizes the clear importance of steps such as the development of transparency and confidence building measures, in addition to further development of international cyberspace norms, to avoid escalation and misperception in cyberspace. The Department also seeks to prevent dangerous escalatory situations by following the same policy principles and legal regimes in its cyberspace operations that govern actions in the physical world, including the law of armed conflict. Finally, the Department believes that increased transparency minimizes the likelihood that a cyber incident will escalate to a dangerous or unintended level.

6. The rules of engagement for commanders at various command echelons for responding to threats to operational missions and in normal peacetime operating environments, including for situations in which the immediate sources of an attack are computers based in the United States.

   Answer: DoD has implemented rules of engagement for the operation and defense of its networks. In current operations that occur in designated Areas of Hostilities, specific rules of engagement have been approved to govern and guide DoD operations in all domains. DoD's cyber capabilities are integrated into planning and operations under existing policy and legal regimes.

   DoD will continue to work closely with its interagency partners, including the Departments of Justice and Homeland Security, to address threats to the United States from wherever they originate, through a whole-of-government approach. The Department is dedicated to the protection of the Nation, and to the privacy and the civil liberties of its citizens.

7. How the administration will evaluate the risks and consequences attendant to penetrations of foreign networks for intelligence gathering in situations where the discovery of the penetration could cause the targeted nation to interpret the penetration as a serious hostile act.

   Answer: Espionage has a long history and is nearly always practiced in both directions. For the U.S. and many other states, traditional espionage has been a state-sponsored intelligence-gathering function focused on national security, defense, and foreign policy issues. The United States Government collects foreign intelligence via cyberspace, and does so in compliance with all applicable laws, policies, and procedures. The conduct of all U.S. intelligence operations is governed by long-standing and well-established considerations, to include the possibility those operations could be interpreted as a hostile act.

8. How DoD shall keep Congress fully informed of significant cyberspace accesses acquired for any purpose that could serve as preparation of the environment for military action.

   Answer: The Department has been working closely with Congress to improve the reporting schemes for cyberspace operations. DoD will provide quarterly cyber briefings to appropriate Members of Congress and their congressional staff in fulfillment of notification requirements. For sensitive operations that may require out-of-cycle reporting, DoD will ensure that appropriate Members of Congress and their congressional staff receive any necessary additional briefings.

9. The potential benefit of engaging allies in common approaches to cyberspace deterrence, mutual and collective defense, and working to establish norms of acceptable behavior in cyberspace.

   Answer: The President's International Strategy for Cyberspace makes clear that hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners, and DoD has been working actively to clarify those expectations within our alliances.

   To implement that vision, the Department of Defense Strategy for Operating in Cyberspace emphasizes the importance of building robust relationships with U.S. Allies and partners to strengthen the deterrence of malicious cyberspace activity and to build collective cyber defenses.

10. The issue of third-party sovereignty to determine what to do when the U.S. military is attacked, or U.S. military operations and forces are at risk in some other respect, by actions taking place on or through computers or other infrastructure located in a neutral third country.

Answer: The nature of the DoD response to a hostile act or threat is based upon a multitude of factors, but always adheres to the principles of the law of armed conflict. These responses include taking actions short of the use of force as understood in international law.

DoD adheres to well-established processes for determining whether a third country is aware of malicious cyber activity originating from within its borders. In doing so, DoD works closely with its interagency and international partners to determine:

- The nature of the malicious cyber activity;
- The role, if any, of the third country;
- The ability and willingness of the third country to respond effectively to the malicious cyber activity; and
- The appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.

11. The issue of the legality of transporting cyber "weapons" across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of "overflight rights."

Answer: There is currently no international consensus regarding the definition of a "cyber weapon." The often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult. The interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains. The law of armed conflict and customary international law, however, provide a strong basis to apply such norms to cyberspace governing responsible state behavior. As the President recognized in the International Strategy for Cyberspace, the development of norms for state conduct does not require a reinvention of customary international law nor render existing norms obsolete.

12. The definition or the parameters of what would constitute an act of war in cyberspace and how the laws of war should be applied to military operations in cyberspace.

Answer: The phrase "act of war" is frequently used as shorthand to refer to an act that may permit a state to use force in self-defense, but more appropriately, it refers to an act that may lead to a state of ongoing hostilities or armed conflict. Contemporary international law addresses the concept of "act of war" in terms of a "threat or use of force," as that phrase is used in the United Nations (UN) Charter. Article 2(4) of the UN Charter provides: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state." International legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e., sea, air, land, and space), also apply to the cyberspace domain.

13. What constitutes use of force in cyberspace for the purpose of complying with the War Powers Act (Public Law 93-148).

Answer: The requirements of the War Powers Resolution apply to "the introduction of United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations."

Cyber operations might not include the introduction of armed forces personnel into the area of hostilities. Cyber operations may, however, be a component of larger operations that could trigger notification and reporting in accordance with the War Powers Resolution.

These answers to Congress show a progression of formal and public declarations from both political and military sources. We have Congress formally ask the military a series of questions around what the rules and policies are for cyber warfare. Similar to Tallinn Manual conclusions most of the answers tie to current policies for kinetic warfare. The answers to three, five, eleven and thirteen have specific cyber connotations.

Finally we have the Legal Adviser for the U.S. Department of State Harold Hongju Koh's speech at the USCYBERCOM Inter-Agency Legal Conference at Ft. Meade, MD on September 18, 2012 where he answered some fundamental questions around cyber [4].

Following are extracts from his answers:

Question 1: Do established principles of international law apply to cyberspace? Answer: Yes, international law principles do apply in cyberspace.

Question 2: Is cyberspace a law-free zone, where anything goes? Answer: Emphatically no. Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint.

Question 3: Do cyber activities ever constitute a use of force? Answer: Yes. Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.

Question 4: May a State ever respond to a computer network attack by exercising a right of national self-defense? Answer: Yes. A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.

Question 5: Do jus in bello rules apply to computer network attacks? Answer: Yes. In the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of necessity and proportionality limit uses of force in self-defense and would regulate what may constitute a lawful response under the circumstances.

Question 6: Must attacks distinguish between military and nonmilitary objectives? Answer: Yes. The *jus in bello* principle of *distinction* applies to computer network attacks undertaken in the context of an armed conflict.

Question 7: Must attacks adhere to the principle of proportionality? Answer: Yes. The *jus in bello* principle of *proportionality* applies to computer network attacks undertaken in the context of an armed conflict.

Question 8: How should States assess their cyber weapons? Answer: States should undertake a legal review of weapons, including those that employ a cyber capability.

Question 9: In this analysis, what role does State sovereignty play? Answer: States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict.
Question 10: Are States responsible when cyber acts are undertaken through proxies? Answer: Yes. States are legally responsible for activities undertaken through "proxy actors," who act on the State's instructions or under its direction or control.
Final Question: Is international humanitarian law the only body of international law that applies in cyberspace? Final Answer: No. As important as international humanitarian law is, it is not the only international law that applies in cyberspace.

Unresolved Questions

- 1: How can a use of force regime take into account all of the novel kinds of *effects* that States can produce through the click of a button?
- 2: What do we do about "*dual-use* infrastructure" in cyberspace?
- 3: How do we address the problem of *attribution* in cyberspace?

Similar to the previous two statements we see most of the legal review focuses on how current law covers most of the questions around cyber warfare. Koh's statement was unique in two aspects. First he did not address the need for international cooperation but rather referred to current international laws. Second he listed unresolved issues. So we have looked at official statements from international, U.S. military and U.S state department and in overall find them to agree on the fact that many of the issues around cyber warfare are covered by current laws. This is easier in broad theoretical statements than when applied to the realities of specific cyber conflicts.

As cyber warfare will be conducted over public or commercial networks by actors from both nation-states and independent parties it is important to understand the laws that impact general Internet interactions. First there are some laws that may be applied to impact how cyber conflicts are resolved. One is the concept of due care and/or due diligence. This relates to how much care someone should take to protect their systems. The average person would not leave a handgun unprotected sitting where anyone could take it because they understand their responsibility to secure the gun so it will not be used inappropriately. In many cases today that same person would leave their computer unprotected and not feel responsible if it was used to electronically rob a bank. Responsibility may need to be regulated like the automobile seatbelt law; it might require basic firewall and antivirus protection or the owner of the computer may be liable.

Another legal principle that may be applied to cyber conflicts is the Nuisance Law. There are two types: public and private. A private nuisance is something (such as an activity) that constitutes an unreasonable interference in the right to the use and enjoyment of one's property and that may be a cause of action in civil litigation. A public nuisance is something that unreasonably interferes with the health, safety, comfort, morals, or convenience of the community and that is treated as a criminal violation [5]. If we look at reactive or even proactive attacks, this rule could be applied if governments or individuals took action against that person who left their system unprotected. This concept is tied to the right to self-defense. The challenge is that the computer actually attacking the victim might be a third party system that was compromised and is being used by the attack. In this case a reactive attack could take out

a system in a critical system for a hospital or one that manages an energy grid. It has not been determined how these legal concepts will be applied to cyberspace or if they will be used to address cyber events rather than the traditional systems used to adjudicate LOACs.

Finally, there is the Principle of Neutrality which aims to maintain the confidence of all by not allowing cyberspace to be used to engage at controversies of a political, racial, religious, or ideological nature due to the reliance of all on it. This concept is usually used for peacekeeping or humanitarian missions to support organization like the International Red Cross and Red Crescent Movement.

Looking at how the law will impact the cyber domain is further challenged because of the ubiquitous nature of computer systems today. The infrastructure is commercially owned, the systems being used to build botnets can be both privately owned and government systems, every industry is dependent to some degree on the Internet and a typical transaction could span multiple legal jurisdictions. This chapter will look at the legal systems, some U.S. laws that will impact how the government responds, privacy issues, and digital forensics because they are enmeshed with cyber warfare issues.

NOTE

This chapter is not intended as legal advice. We will discuss the laws that exist today and how they relate to cyber warfare to help understand the impacts but it is not intended as guidance or advice. The authors would like to thank Robert Clark for his advice and insight on legal issues throughout the book.

LEGAL SYSTEMS

When examining today's legal systems we have international and nation based law which has four general types of systems: civil law, common law, customary law, and religious law (plus those with a mix, called pluralistic).

International Law has three separate disciplines: (1) public international law, which governs the relationship between provinces and international entities and includes treaty law, law of the sea, international criminal law, and international humanitarian law; (2) private international law, which addresses legal jurisdiction; and (3) supranational law, a legal framework wherein countries are bound by regional agreements in which the laws of the member countries are held inapplicable when in conflict with supranational laws. The sources of international laws are set out in Article 38-1 of the Statute of the International Court of Justice within the UN Charter [5].

Under national system law we have civil law, which is the most widespread type of legal system in the world and has laws that are organized into systematic written codes. In civil law, the sources recognized as authoritative are principally legislation and secondarily, customs. Next is common law. The foundation of common law is "legal precedent"—referred to as "stare decisions," meaning "to stand by things decided." The United States uses a variation of common law which has a several layers, possibly more than in most other countries, and is due in part to the division between federal and state law. Then we have customary law (also referred to as "primitive law," "unwritten law," "indigenous law," or "folk law") that

embodies an organized set of rules regulating social relations that are agreed upon by members of the community. Although customary law includes sanctions for legal infractions, resolution tends to be reconciliatory rather than punitive. Finally we have religious law. The main types of religious legal systems are *sharia* under Islam, *halakha* under Judaism, and canon law under some Christian groups. Islamic law is the most common law governing religious legal systems in use today. It is embodied in the *sharia*, an Arabic word meaning "the right path." *Sharia* covers all aspects of public and private life and organizes them into five categories: obligatory, recommended, permitted, disliked, and forbidden. There are some systems that have mixed or pluralistic law, mixed law consists of elements of some or all of the other main types of legal systems—civil, common, customary, and religious [6]. Each of these systems deals with warfare and the Internet in different ways so it creates a complex situation when one country tries to prosecute a crime with a suspect in a different legal system.

All of these systems base their foundational principles on geography to determine what laws the incident will fall under. For example, if someone trespasses on our property in Texas we can shoot them, in Colorado we cannot shoot them until they break into our house, in California we cannot shoot them unless we feel in danger of losing our life and have no way to escape.

The second issue is that laws are written at a very deliberate pace over years while Internet issues develop at the speed of technological innovation. A prime example is the "I love you" worm in 2000. The investigation tracked the programmer to an individual in the Philippines, but as there were no laws about releasing malware on the Internet no charges were brought against him [7]. There is natural pressure to enact laws based on these events but without careful study laws could be signed that have unintended consequences that are worse than the original problem. The challenge is how do we determine what laws apply to technology that are not addressed in the current set of laws and are not tied to geography?

International

The United Nations is considered by many to be the foundation for international law but there are many treaties, agreements, conventions, charters, protocols, declarations, memoranda of understanding, or on the military side, coalitions that govern how nations interact. The most formal are treaties that are ratified by all sovereign nations involved. Some of these come after major events like the establishment of the North American Treaty Organization (NATO) while others develop over time like Admiral or Maritime Law. Still others are driven by technology like nuclear weapons, biological weapons, and satellites. There are some key lessons that can be learned from maritime law and space law. Let's look at the parallels they have to the cyber warfare.

Maritime Law

Maritime or admiralty law is a system of law concerning navigation and overseas commerce. Because ships sail from nation to nation over seas that no one nation owns, nations need to seek agreement over customs related to shipping. Though maritime law is general in character, only those parts that determine the relations among nations—particularly those

that deal with problems arising on the seas in wartime, such as questions of belligerency and neutrality—are part of the international law proper [7]. Much like the Internet where traffic needs to flow over circuits not owned by the parties sending and receiving the messages, there need to be some rules on how nations act and react to each other and to non-State actors launching attacks from sovereign territory. The responsibility to help ships in trouble could become the Internet responsibility to both protect and prevent hostile cyber actions in their country. Some will argue that most countries don't control the systems we are talking about but that is also true for the shipping industry. Privateering (state sponsorship of privately owned ships used to attack enemy shipping) is not a problem on the high seas today, but as we look at the many cyber incidents that have indicators of state sponsorship, we should examine how Privateering was addressed to make sure we take advantage of lessons learned over history. Piracy is another age-old issue and there are many customs and laws on how they can be dealt with; these principles should be considered as precedents for how to react to criminals on the Internet.

Space Law

Space law is defined as the agreements governing the exploration and use of outer space, developed since the first launching (1957) by humans of a satellite into space. Space law, an aspect of international law, has grown under the aegis of the United Nations. A 1963 UN declaration stated that the exploration and use of outer space would be for the benefit and in the interest of all people; that no sovereignty could be claimed in space; that objects and persons launched into space would be returned promptly and safely if they landed in a foreign country; and that nations launching objects would be responsible for damages caused by them. In 1967, a general treaty went into effect embodying these principles and adding a prohibition on the military use of space and a provision for the inspection of installations on celestial bodies [8]. Like the Internet, space is an area where technology is changing rapidly and geography is difficult to define, so is a good template to look to for methods to develop mutually beneficial treaties. The biggest difference is the cost of entry to this domain is very high so the group of nations is small, while cyberspace has little if any cost barrier. It is imperative we draw from all areas that parallel cyberspace if we want to accelerate the development of cyber law.

The lessons drawn from nuclear and biological were addressed in Chapter 1 and also have some basic principles that can help develop the international legal framework to address cyber warfare issues.

United States Laws

In the United States, cyber incidents can be handled under Criminal Law (Penal Codes, Statutory, and Case Law), Civil Law (Tort, Contract, and Property Law), or Tribunal Law (Industrial, Labor, and Arbitration Law) depending on the circumstances. Penal codes are laws concerning crimes and their punishments and can be used to prosecute malicious cyber acts. Torts are wrongful acts, other than a breach of contract, that injures another and for which the law imposes civil liability. A serious issue related to national cybersecurity is whether or not our critical infrastructure companies are practicing due care/due diligence

for computer security. If they were found to not be compliant then they would assume liability (the accountability and responsibility to another enforceable by civil remedies or criminal sanctions). Finally, tribunal law is a court or forum of justice where a person or body of persons (such as village elders) hear and decide disputes so as to bind the parties [9]. These different systems show the complexity within the United States when it comes to deciding jurisdiction for cyber attacks.

These legal systems need to be modified and enforced to raise the level of defense for the commercial sector today. This raises the argument about whether the government should be using "the carrot or the stick" to motivate industry. Some feel each industry (e.g., energy or finance) should self-regulate as they understand the risks to their business better than the government. Others feel the industries judge risk based on revenue and not on national security so they cannot be expected to implement the appropriate level of security. If the government is to incentivize industry they can offer either something like a tax break for good security practices or penalties for poor practices. Either would require a standard to be followed and audits to validate. If any country hopes to raise their national level of computer network defense they will need to start to impose standards of practice on key industries.

Criminal Law

Generally criminal law is the government against an individual, while civil and tribunal laws are a person against another person. When we look at some of the issues surrounding cyber conflicts we see some actions will be tried in civil court as economic issues, while other attacks can be prosecuted as criminal acts and still others will be moved into foreign or international legal systems. Each of these systems requires a different level of proof. Burden of proof is when the prosecutor must produce sufficient evidence in support of a fact or issue and favorably persuade a judge or jury; it encompasses both the burdens of production and persuasion. The proof is usually offered as evidence. There are three types of evidence: physical evidence, intangible evidence, and direct evidence. Evidence can be obtained by LEA as part of the investigation but often requires some type of court order (mandate from a superior authority) such as a warrant (writ issued by a judicial official authorizing an LEA to perform a specified act required for the administration of justice) or a subpoena (a command for the production of artifact or person).

An example would be to subpoena a hard drive, log files, emails, or documents (note it is not unusual to have a warrant for email files but not the rest of the information on the hard drive). This process is imperative for computer security practitioners to understand, as to take any retaliatory action they will need to be able to defend their actions in a court of law. For many of us this is a foreign concept; the military is not used to collecting evidence—they collect intelligence (which requires different processes and burden of proof), and in the commercial sector the key is detection then mitigation and recovery (focus is fixing the vulnerability and getting back into production—not prosecution). To change the cycle of defenders reacting to each new attack there will need to be a change in how defenders react and start to counteract, use of the legal system is one such method.

Electronic Discovery

The collection of evidence is known as Electronic Discovery (or e-discovery); it is the method used by parties to a civil or criminal action to obtain information held by the other party that is relevant to the action. E-discovery costs are spiraling ever higher, posing a significant challenge for companies faced with litigation and regulatory investigations that require extensive data collection and review. A sample scenario could be when the prosecution requests the email, web traffic, and Microsoft Office documents for 10 key people involved in a case for the last seven years. This would require the IT staff to get the backup tapes (assuming they have them), load them (understanding they may no longer run the same hardware), unencrypt them (if they still have the passwords on file), and extract just the required records under evidentiary process rules (i.e., tagging and tracking who has had access to them). See Figure 13.1, the Electronic Discovery Reference Model, for a general flow chart of the process. It is easy to see how labor intensive this is if everything goes right. For companies which have not developed policies and processes to facilitate this, it never does. These processes are necessary for countries as well as companies who want to track where the threat has been in their network and most government agencies are not funded or required to be able to facilitate this kind of an investigation.

While e-discovery is essentially a narrowed focus of digital forensic investigations, it is important to understand that it must be done by trained personnel who understand both how to conduct an investigation and the technology involved. That said, a good forensic investigator will not limit their investigation to just examination of the technology. They should also use the following techniques:

- Depositions: Sometimes referred to as witness interviews, it is the primary method for interviewing individuals to uncover important concepts and facts.
- Interrogatories: Similar to depositions, but in written form. Instead of a live interview, written questions are presented to a target.
- Document Requests: Sometimes referred to as a Discovery Request or a Subpoena, this is the primary method for obtaining documents and other items.

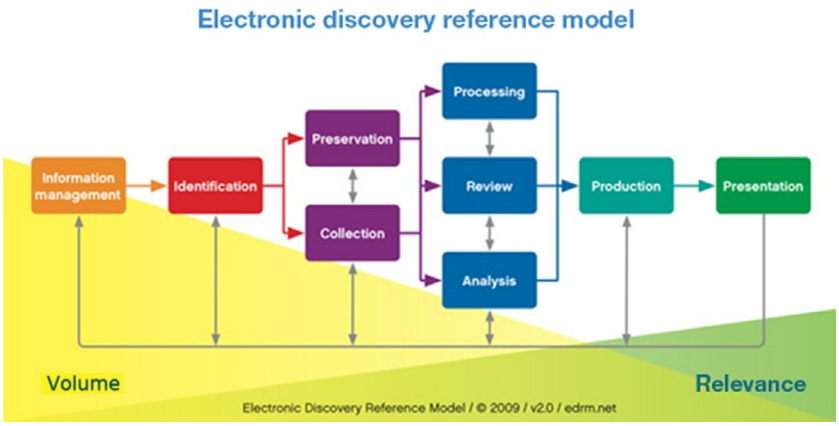

FIGURE 13.1 Flow chart of the steps for e-discovery [7].

Once the case is complete and a verdict of guilt has been issued, it is time to determine punishment (such as a fine or imprisonment) inflicted on an offender through the judicial process. These can serve as a deterrent for other attackers as they see the cost of cyber crime or warfare is higher than the benefits they gain.

KEY U.S. LAWS

In Chapter 4 we touched on the United States Codes that impact cyber warfare: Title 50—Intelligence/Counter Intelligence (DNI), Title 10—War (DoD), and Title 18—Legal (DOJ) which need to be integrated into one process (sometimes referred to as Title 78). We also mentioned the use of Title 32 (National Guard) and Title 14 (Coast Guard) as they have different regulations governing them and can fill different missions the active military forces can't. One major restriction is the Posse Comitatus Act which prohibits search, seizure, or arrest powers to be used by U.S. military personnel. This law states that the U.S. military cannot collect information on U.S. citizens. This has created quite a challenge as it is often difficult to determine which IP addresses and other network/cyberspace information belong to U.S. citizens. The National Guard and Coast Guard don't fall under the same rules and in some cases can facilitate that collection.

TIP

Words matter, and the legal landscape for all things cyber is rapidly changing so finding the right resource is vital to developing a sound strategy or argument. This includes tracking events from sources like United Nations documents, national military doctrine (for the United States it is being updated almost monthly), international organizations (e.g., Internet Engineering Task Force's Request for Comments) as well as recent court cases and new laws. It is important to develop a set of references or news feeds to keep up to date.

International Trafficking in Arms Regulations

Another often overlooked tool is the International Trafficking in Arms Regulations (ITAR) Title 22—Foreign Relations; Chapter I—Department of State; Subchapter M—International Traffic in Arms Regulations which authorizes the president to control the export and import of defense articles and defense services. The fact that an article or service may be used for both military and civilian purposes does not in and of itself determine whether it is subject to the export controls. This includes sending or taking technical data, articles, or equipment related to computers specifically designed or developed for military application, cryptographic techniques, software designed or modified to protect against malicious computer damage, and electronic equipment which has substantial military applicability. There is a very involved process to determine if something falls under ITAR regulations. This can be used to restrict what technology developed in the United States can be sold to potential adversaries. This is not necessarily an effective technique and has had some unintended consequences in the past but can be a useful part of a larger integrated plan.

U.S. Cyber Related Laws

For the U.S. military the foundation of military law is the Uniform Code of Military Justice (UCMJ). The UCMJ applies to all members of the uniformed services of the United States: the Air Force, Army, Coast Guard, Marine Corps, Navy, National Oceanic and Atmospheric Administration Commissioned Corps, and Public Health Service Commissioned Corps. The current version is printed in the latest version of the Manual for Courts-Martial (2008), incorporating changes made by the President (executive orders) and National Defense Authorization Acts of 2006 and 2007 [10]. These are implemented through a number of regulations and in many cases limit what the military can do by policy rather than technological issues. We will not get into the details in this book but a simple example is that the U.S. Cyber Command may have the resources to help defend against an attack on the U.S. energy grid but they are prevented by law/policy from helping. These issues are being addressed through work between NSA/Cyber Command/Northern Command and Department of Homeland Security but are far from resolved.

There are a number of U.S. Acts and institutions that relate to cyberspace such as the Radio Act of 1912 which regulates private communications, the Computer Fraud and Abuse Act of 1984, the Computer Security Act of 1987, the Foreign Intelligence Surveillance Act of 1978 known for its support of warrantless surveillance and the Amendments of 2008 and the Obstruct Terrorism Act of 2001 (known as the Patriot Act), the Federal Information Security Management Act of 2002, and the 1965 establishment of National Institute of Standards & Technology (NIST) which has responsibility for IT standards and technical assistance. Others that are well known, such as Health Insurance Portably and Accountably Act (HIPPA), Digital Millennium Copyright Act (DCMA), Gramm Leach Bliley Act (GLB) and Sarbanes—Oxley Act (SOX), don't have a direct impact on cyber warfare but are crucial to overall cybersecurity [11]. This is just a sampling of the current laws to understand how they impact cyberspace. There are a larger number of bills in Congress today related to the Internet so this subject matter will be under constant change.

Computer Fraud and Abuse Act

Let's examine a few to see how they can impact cyber warfare. First is the Computer Fraud and Abuse Act of 1984 (18 U.S.C. § 1030: U.S. Code—Section 1030). It states fraud and related activity in connection with computers by someone who has knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the U.S. government pursuant to an executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data can be fined under this title or imprisoned for not more than 20 years, or both [11]. This allows the federal government to take legal action against hackers/attackers. This is complicated by the fact that many of the systems or people involved may not reside inside the U.S. borders but it is a useful tool when it can be applied.

Cyber Security Enhancement Act

The Cyber Security Enhancement Act allows service providers to disclose the contents of communications to "federal, state, or local government entities" in the event that the provider

has a "good faith" belief that "an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." These changes effectively expanded the scope of disclosures possible under the law and lowered the standard by which such disclosures could take place [12]. This allows for both LEA and Intelligence Community (IC) to gather and analyze data to determine who and what is involved in a cyber incident in a timely manner.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act), passed in the wake of the 9/11 terrorist attacks, is the controversial Act that expands the type of information to which law enforcement officials may obtain access and permits service providers to divulge the contents of communications in emergencies. Some sample sections that cause debate are [12]:

- Section 212 of the Act permits service providers to voluntarily release the contents of communications if they reasonably believe that "an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." This provision was further modified by the Homeland Security Act to increase the number of governmental agencies to which service providers may disclose communications and to soften the standard by which communications can be disclosed to a "good faith" belief from a "reasonable belief."
- Section 214 of the Act significantly expands the FBI's electronic surveillance powers under the Foreign Intelligence Surveillance Act (FISA), as well as lowering the standards under which the secret FISA court can authorize the FBI to spy on our phone and Internet communications. In particular, Section 214 makes it easier for the FBI to install "pen registers" and "trap-and-trace devices" (collectively, "pen-traps") in order to monitor the communications of citizens who are not suspected of any terrorism or espionage activities.
- Section 215 allows the FBI to secretly order anyone to turn over business records or any other "tangible things," so long as the FBI tells the secret FISA court that the information sought is "for an authorized investigation. . .to protect against international terrorism or clandestine intelligence activities." These demands for records come with a "gag order" prohibiting the recipient from telling anyone, ever, that they received a Section 215 order.
- Section 217 permits service providers to "invite" law enforcement to assist in tracking and intercepting a computer trespasser's communications.

These amendments make it easier for LEA and the IC to conduct investigations into suspected threat activity.

Federal Information Security Management Act

Finally, under the E-Government Act, the Federal Information Security Management Act (FISMA) was designed to require that all federal agencies conduct a "privacy impact assessment" (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII), designate a Chief Information Officer (CIO), implement an information security program, report on the program's adequacy and effectiveness, participate in annual independent evaluations of the information security program and practices, and develop and maintain an inventory of the agency's major information systems [13]. The first federal CIO, Vivek Kundra, produces an annual FISMA report card

under the Office of Management and Budget. In the past it has not been unusual for agencies to receive a failing grade. In 2003, he told the House Committee on Oversight and Government Reform—"when FISMA was enacted, the Internet and the mobile computing revolution were not as pervasive as they are now. Today, agencies are leveraging technologies and business models such as cloud computing, mobile platforms, social media, and third-party platforms to increase efficiency and effectiveness. For example, the Department of Veterans Affairs contracts with mortgage services to service VA-owned home loans. These new models increase efficiency but leave agencies struggling with the question of how to apply FISMA's requirements in an environment where system and enterprise boundaries no longer define the security points. There are a number of issues that contribute to our vulnerabilities, including: lack of coordination, culture of compliance, lack of an enterprise approach and need to energize national agenda for cybersecurity research and development" [14]. To fix these, the Federal CTO plans to overhaul how FISMA is enacted, moving more authority to the National Institute of Standards and Technology (U.S.) (NIST), developing metrics and real-time situational awareness (moving away from the current static document based Certification and Accreditation programs) as well as tracking return on security investments, increasing cyber skill set, and improving response to attacks. These are foundational to computer network defense of the government.

NOTE

When talking about the value of regulations, a good analogy is the local fire department. They have two roles. The firefighters react to fires that are going on in real time while the fire marshal conducts inspections to make sure fires don't get started. The fire codes are pivotal to keeping the number of fires down and the amount of damage done to a minimum. So the value of implementing cybersecurity standards is preventive and will save money in the long run.

Standards to Support Cybersecurity

We will briefly touch on some enabling standards that organizations can use to quantify and measure their security posture. To develop a solid security system, we can look to the International Organization for Standardization (ISO) 27,000 family of Information Security Management System (ISMS) standards and the Information Technology Infrastructure Library (ITIL) model. These can be supported by Capability Maturity Model Integration (CMMI) for documentation and Six Sigma for cost effectiveness. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) by Software Engineering Institute, Carnegie Mellon University is a set of tools and processes for risk-based cyber strategic assessment and planning. Control Objectives for Information and Related Technology (COBIT) by Information Systems Audit and Control Association (ISACA) is a good auditing system. Some industries like North American Electric Reliability Corporation have developed a set of best practices like Industrial Automation and Control System Security Committee of the Instrumentation, Systems, and Automation Society (ISA) SP 99. When looking at systems we can see if they have been through Common Criteria evaluation. These are just a sampling of the resources that are available to organizations today.

PRIVACY IMPACTS

Privacy can have a major impact on cyber warfare: the government must balance national security against the rights of the citizens. There are issues of expectation of privacy in the home and workplace, generational attitudes, constant technological advancements not covered by current laws, and basic human rights of freedom that cyber warfare tactics, techniques, and procedures must take into account. Examples are the move to state/national identity badges, and the use and tracking of biometrics that could enable aspects of national security but impinge on individual privacy rights.

The United States has a number of laws related to privacy. There are indirect references throughout in the Constitution but no declaration of a right to privacy. When we look at congressional statutes we have the Privacy Protection Act, Telecommunications Act, Health Insurance Portability and Accountability Act (HIPAA), Right to Financial Privacy Act, Identity Theft and Assumption and Deterrence Act, and Children's Online Privacy Protection Act. On the other side of the coin, we have Freedom of Information Act and Patriot Act that start to curtail privacy rights in the name of national security. These laws must be kept in constant tension to achieve the right equilibrium between security and freedom.

Electronic Communications Privacy Act

A good example of this balance is the Electronic Communications Privacy Act (EPCA) of 1986 (18 U.S.C. § 2510-22) which as amended protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically. ECPA has three titles: Title I which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or "procurement of any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title II, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses. Title III, which is called the Pen Register and Trap and Trace Statute, requires government entities to obtain a warrant before collecting real-time information, such as dialing, routing, and addressing information related to communications. The ECPA was significantly amended by the Communications Assistance to Law Enforcement Act (CALEA) and the Patriot Act to facilitate national security investigations [11].

DIGITAL FORENSICS

Forensics is the discipline of science dedicated to the systematic gathering and analysis of evidence to establish facts that can be presented in court. The key to forensics is understanding exactly what happened (not why) and determining who did it. Digital forensics is applying this discipline to computer devices and networks. The most difficult goal in this field is determining attribution (ascribing the actions of an incident to a specific person or

organization). This discipline is key to national security for Computer Network Defense. Although the evidence may not end up in a court of law it may be what is needed to authorize a counterattack (virtual or physical).

Let's start with an analogy. In America many places have a beat cop. These are the policemen who patrol a specific set of blocks; they may spend the morning working a traffic accident and an armed robbery investigation, then in the afternoon take care of a domestic disturbance call and write up a vandalism incident. Their job is to enforce the laws within their neighborhood. If one day while walking along they see a man in the alleyway lying on the ground bleeding from a knife stuck in his chest they would immediately call for an ambulance and start basic life saving procedures. If these failed and the man died they would change their priority to preserving evidence to support a criminal investigation. They would call for homicide detectives who would bring along the Crime Scene Investigation (CSI) team. These folks are trained in collecting and analyzing evidence to support the investigation and be able to present it in a court of law. The beat cop could help the detectives with simple tasks like canvassing the area for witnesses but generally they go back to their normal duties. In the virtual world system, administrators are the beat cops for the local network. They ensure the normal operation of the systems and monitor for abnormalities. If they detect a problem they will work to fix it until they determine it is an intrusion. In most organizations the sys admins will work with management to determine if they want to rebuild the system or investigate to facilitate a prosecution.

The problem with just rebuilding is the threat will simply use the same method to regain entry so some analysis is normally warranted but it may not be in accordance with evidentiary rules. If the decision is to investigate then a determination needs to be made if the organization's leadership just wants to know what happened or if it could end up in court. With the possibility of going to court comes the need for specialized skills and qualifications (often in the form of certifications). The systems involved must be treated as evidence. The investigation must be documented and the conclusion must stand up to legal standards. The tools and methodologies used must be able to stand up to review by the opposition. The investigator must be able to present the findings in an understandable way and justify their conclusions. Much like the cop trying to save a life the sys admin can damage evidence if they go too far before calling for help. Also like the beat cop they are not well equipped to testify in a court of law.

WARNING

One note for those who watch the *CSI* TV show, the last thing a digital forensic investigator would do is log into the computer. That is actually destroying evidence.

Digital forensics is similar to physical forensics but there are some key differences: first, it is a much newer discipline and in many cases both the judge and jury have difficulty understanding it (compared to something like DNA evidence which is in the common public understanding today); second, it is very transitory (it is important to baseline the evidence as computer systems are in a constant state of change); and finally, it is not a skill set that many LEA officers have (compared to the amount of training they get in handling and analyzing physical evidence). This brings up the challenge of live vs. static analysis. There will be times when the system cannot be pulled offline to analyze so it must be done live, which requires unique tools and procedures.

There are four basic steps to the computer forensics:

1. Preparation—this is where Tactics, Techniques, and Procedures (TTPs), tools, and documentation methodology are developed
2. Acquisition—this is where the collection, preservation, and review of the evidence is done
3. Analysis—this is where the investigator constructs the events into facts about what was done and if possible who did it
4. Reporting—this is where all the documentation is presented in a format that facilitates the decision needed (this is different in court vs. intelligence activities)

These very simple steps do not reflect the complexity of most investigations. A simple investigation of a laptop could involve network devices it communicated with and mobile devices (e.g., external hard drive, memory sticks, or a Blackberry) that were attached to it. Each of these requires different forensic knowledge and tools.

For physical acquisition here are some tips: first create a cryptographic hash digest of the original media (MD5/SHA-1). A hash is a one-way mathematical algorithm that when run against a file or hard drive creates a bit string signature or message digest. If anything in the file or on the hard drive changes, the message digest changes. This allows copies of files to be used in court as authentic original evidence. The investigator can keep one copy and work on others and never change the original. Next comes the collection of the relevant specimens, which must be validated with the hash digest.

Then using forensics tools like Encase, Forensic Tool Kit, or Helix, analyze the evidence and document everything done and found. These tools will do much of the discovery but in every investigation there may be specific issues that call for unique tools such as developing scripts. Cell phones are a good example of when a new tool may need to be added to the investigator's tool kit. There are open source tools but be careful as they may not stand up in court as well.

Finally, develop a report of the findings based on a standard template which can facilitate the ability to accurately testify months or years later on the findings. It is important to keep all notes and logs of the investigation as cases can go from analytical to a court case years later and you will need to be able to recall specifics based on your records.

WARNING

There is no program that will act as a dummy or wizard program to facilitate an untrained individual conducting a digital forensic investigation both because every investigation is unique and because only a trained and certified investigator should be in charge. An investigation done by unqualified personnel will result in compromised results and be unusable.

Certification

There are a number of computer forensics certifications. Generally they are broken out by vendor sponsored or LEA supported. Under vendor certifications the major certifications are by the vendor who sells the tool like the EnCase Certified Examiner Program for those who have mastered their software, AccessData Certified Examiner (ACE) by AccessData for their software, the Forensic Toolkit and GIAC Certified Forensic Analyst (GCFA) by the SANS (not

tool based). For the LEA sponsored certifications the major certifications are: International Association for Computer Investigative Specialists (IACIS) which has the Certified Forensic Computer examiner (CFCE) and the Certified Electronic Evidence Collection Specialist Certification (CEECS). The International Society of Forensic Computer Examiners which has the Certified Computer Examiner (CCE). DoD has the Cyber Crime Center which has the Certified Digital Media Collector (CDMC), Certified Digital Forensic Examiner (CDFE), and Certified Computer Crime Investigator (CCCI) certifications. There are a number of other vendors, training programs, certifications, and organizations. This was just meant to be a sampling of what is being done.

One interesting trend in this area is the development of laws governing the field. Some states require certifications while others are moving to require a Private Investigators license. At issue here is the standard for an Expert Witness Qualification where a witness (such as a medical specialist) who by virtue of special knowledge, skill, training, or experience is qualified to provide testimony in a court of law. For many areas it is easy to determine what an expert is, but in the digital investigation world there are very few people with law enforcement training to understand due process and digital forensic skills to understand how to extract and analyze data and no common standard to determine what the qualifications are for an expert.

SUMMARY

The president must determine whether a particular cyber attack against the United States is of such scope, duration, or intensity that it is an "armed attack" and whether the initiation of hostilities is an appropriate exercise of our right of self-defense [14]. This will require a clear standard to be measured against and these standards need to be established now so they become the standard we can use.

This chapter has reviewed the different legal systems and some of the current laws that can impact how cyber warfare is conducted. The importance of these can be found in the overlap with Chapter 1 and definitions, Chapter 3 on the cyber battlefield, Chapter 4 on doctrine, and Chapter 14's coverage of ethics. We discussed the need to balance methods to fight the interconnected cyber crime, espionage, and warfare with the right to privacy. Finally, we dove into the need for digital forensics to support cyber warfare. The goal was to show that cyber is ubiquitous and cannot be divided into clean areas of nation-state, commercial, and military. They use the same infrastructure, involve many of the same systems, and the second and third order effects bleed over into what for a traditional armed conflict would be unrelated areas of the law.

Finally at the time of publishing there were a number of laws being proposed. Most centered on information sharing and protecting privacy. While many of these bills stand little chance of being passed there is another option—relook at the way current laws are being enforced and/or interpreted.

References

[1] Force, US Air. AFPAM36–2241 professional development guide. Air Force e-Publishing, http://www.e-publishing.af.mil/?rdoFormPub=rdoPub&txtSearchWord=36-2241&client=AFPW_EPubs&proxystylesheet=AFPW_EPubs&ie=UTF-8&oe=UTF-8&output=xml_no_dtd&site=AFPW_EPubs&btnG.x=14&btnG.y=10; 2009.

[2] Tallinn Manual on the International Law Applicable to Cyber Warfare by the NATO Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/249.html; 2013 [accessed 17.02.13].

[3] Department of Defense Cyberspace Policy Report A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 November 2011, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf [accessed 17.02.13].

[4] Harold Hongju Koh the Legal Adviser, U.S. Department of State speech to USCYBERCOM Inter-Agency Legal Conference 2012, http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/?utm_source=rss&utm_medium=rss&utm_campaign=harold-koh-on-international-law-incyberspace [accessed 17.02.13].

[5] Agency, Central Intelligence. Field listing – legal system. Fact book, https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html; 2010 [accessed 17.02.13].

[6] Burke L. Love bug case dead in manila. Wired, http://www.wired.com/politics/law/news/2000/08/38342?currentPage=all; 2010 [accessed 17.02.13].

[7] Encyclopedia, Columbia. Library, http://www.answers.com/; 2010 [accessed 17.02.13].

[8] N/A. Law dictionary. Find law, http://dictionary.lp.findlaw.com/; 2010 [accessed 17.02.13].

[9] The electronic discovery reference model, http://edrm.net/ [accessed 17.02.13].

[10] DoD. Uniform code of military justice, http://www.ucmj.us/; 2010 [accessed 17.02.13].

[11] U.S. Department of Justice. Information sharing. Federal statutes, http://it.ojp.gov/default.aspx.

[12] Foundation, Electronic Frontier. Statutory protections. Internet law treatise, http://ilt.eff.org/index.php/Privacy:_Statutory_Protections#The_Cyber_Security_Enhancement_Act; 2010 [accessed 17.02.13].

[13] U.S. Department of Justice. Information Sharing. Federal Statutes, http://it.ojp.gov/default.aspx [accessed 17.02.13].

[14] Kundra V. Federal information security testimony. CIO.Gov, http://www.cio.gov/pages.cfm/page/Vivek-Kundra-Testimony-Federal-Information-Security; 2010 [accessed 17.02.13].