

JOURNAL OF LAW AND CYBER WARFARE

- I. North Korea: The Cyber Wild
Card.....1
Rhea Siers
- II. Hack, Attack or Whack; The Politics
of Imprecision in Cyber Law 13
James E. McGhee
- III. A Brave New World: Applying
International Law of War to Cyber
Attacks 42
Noah Simmons
- IV. Strengthening Director Duties of Care for
Cybersecurity Oversight: Evolving
Expectations of Existing Legal
Doctrine.....109
Brad Lunn

Editor-in-Chief

Daniel B. Garrie, *Partner, Law & Forensics*

Associate Editors

Siddartha Rao, *Special Counsel, Law & Forensics*

Samantha Tucker, *Analyst, Pulse Advisory*

Michael Mann, *Associate, Law & Forensics*

Radhika Tiwari, *Analyst, Pulse Advisory*

Tarique Collins, *Associate, Zeichner, Ellman & Krause*

Editorial Board

Christopher Burgess

Founder & CEO, Prevendra

Jean-Claude Knebel

*Consul General of Luxembourg to
New York*

Jack Dever

*Director, Business Intelligence Unit,
General Electric*

Dr. Larry Ponemon

Chairman, Ponemon Institute

Jeremy Kroll

CEO, K2 Intelligence

John Dever

*General Counsel of Defense Firm
Major Reserve, US Army*

Dr. Joseph Weiss

*Managing Partner, Applied Control
Solutions*

Shane Reeves

*Associate Law Professor, US
Military Academy, West Point*

Mitchell Silber

*Executive Managing Director, K2
Intelligence*

Noah Bledstein

*IT Data Privacy Leader at GE
Healthcare*

Retired Major U.S. Airforce

Robert Clark

Cyber Attorney, Army Cyber Institute

Robert Bair

*Lieutenant Commander,
United States Navy*

Ryan Lasalle

*Global Managing Director, Security
Transformation Services, Accenture*

William Spernow

Chief of Security, Virus Inspector

Eric Jensen

Law Professor, BYU

Uma Chandrashekar

*Global Information Security and Privacy
Leader at Edwards Life Sciences*

Vincent Scott

*GBS-ITS Cybersecurity, Proctor &
Gamble Company*

Rhea Siers

*Senior Associate at the GWU Cyber
Security Initiative*

Richard Borden

*Assistant General Counsel, Bank of
America Merrill Lynch*

Professor Michael Schmitt

*Director, Stockton Study of International
Law at the US Naval War College*

Hack, Attack or Whack; The Politics of Imprecision in Cyber Law

James E. McGhee¹

I. Introduction

NATO has a section of their website with a timeline of the history of cyber-attacks.² An intriguing aspect of the list is that many of the events listed are referred to as hacks, without any definitive explanation of why or how they qualify as cyber-attacks. On September 3, 2013, abc NEWS reported that, “U.S. officials confirmed a cyber attack by the Syrian Electronic Army on the Marine Corps recruiting website late Monday in which the pro-Assad collective replaced the normal page with on calling on U.S. servicemen to refuse orders to fight in Syria should they be called.”³ On September 10, 2013, Fox published a story titled,

¹ . Mr. McGhee is an operational cyber attorney with the 24th Air Force, Joint Base San Antonio, Lackland AFB. The views expressed in this Article are those of the author in his personal capacity and does not necessarily represent those of the US Air Force or any other US governmental entity. The author wishes to thank Noah Bledstein for editing and feedback.

² *History of Cyber Attacks*, NATO REVIEW, <http://www.nato.int/docu/review/2013/Cyber/timeline/EN/>.

³ Rhonda Schwartz, *U.S. Confirms Syrian Electronic Army Defaced Marines Website*, <http://abcnews.go.com/blogs/headlines/2013/09/u-s-confirms-syrian-electronic-army-defaced-marines-com/>.

“Hackers Plot 9/11 Cyber Attacks on U.S., Israel.”⁴ The article explains that “Politically-motivated hackers recently announced a call to arms to Muslim hackers aimed at attacking U.S. and Israeli websites on Wednesday, the 12th anniversary of the September 11 terrorist attacks.”⁵ The Markey-Waxman report, based on information gathered through a survey containing 15 questions and sent to more than 150 utility companies, found that the electric grid is the target of numerous and daily cyber attacks.⁶ “Those events range from phishing emails to malware infections to unfriendly probes.”⁷

Thus it is all too clear that any cyber-intrusion, whether mundane or malicious, from a teenager, a criminal or a nation state, regardless of place of origin, is likely to be described as a cyber-attack. However, to a military attorney the term “cyber-attack” actually includes only a small segment of this spectrum of activity. Cyber-attacks must meet certain criteria to justify this designation, i.e., involving damage or destruction to property or injury or death to persons. If we use this definition, arguably, there have only been a handful of actual cyber-attacks that rise to the level of either use of force or armed attack over the past ten years or so. Indeed, some would argue that we have yet to see

⁴ Matt Egan, *Hackers Plot 9/11 Cyber Attacks on U.S., Israel*, Sept. 10, 2013, <http://www.foxbusiness.com/technology/2013/09/10/hackers-plot-11-cyber-attack-on-us-israel/>.

⁵ *Id.*

⁶ Electric Grid Vulnerability, Industry Responses Reveal Security Gaps, A report written by the staff of Congressman Edward J. Markey (D-MA) and Henry A. Waxman (D-CA), May 21, 2013.

⁷ *Id.*

an actual cyber-attack. I can only think of two examples, that if perpetrated against the United States, would likely be considered either a use of force or armed-attack for cyber purposes: Stuxnet and the Iranian attack on Saudi Aramco. We can arguably use these as baselines for future events – we know it when we see it.

If this generalized misuse and mischaracterization was merely the product of our media, it could be forgiven, as a degree of hyperbole can be expected when the goal is to draw in a paying audience. However, our politicians, military leaders and NATO allies have consistently used “cyber-attack” as shorthand for almost every event involving a computer intrusion.

We are actually talking about three separate and distinct terms that should have three separate and distinct definitions; cyber-espionage, cyber-crime and cyber-attack. Yet invariably cyber-intrusions are collectively referred to as cyber-attacks. This over generalization has serious consequences, particularly in a legal context. Where use of military force is in question, how an event is characterized and ultimately defined makes all the difference with regard to who is responsible for responding to the event, what sort of responses are legal and the level of authorization required to respond. Potential liability is also an issue as acts of war resulting in damage are rarely covered by insurance or eligible for compensation from an

aggressor nation, whereas cyber-crimes may be covered and damage caused outside of a conflict is often compensated through a claims process.

There is a larger political context to this imprecision. Describing almost all events as cyber-attacks feeds the popular misperception that we are engaged in an ongoing cyber-war. The laws governing cyber-attacks, or any armed attack, require, indeed, demand that certain thresholds be met before a cyber-intrusion can be labeled and treated as an actual attack. Warfare, whether cyber or otherwise, has traditionally required combatant nation states, or at a minimum, nation state sponsored belligerent groups.

Espionage, whether by a human agent or cyber intrusion is not prohibited under international law, though these activities are almost always criminal acts punishable by the victim's domestic legal code. It is generally understood that all nations engage in espionage against their enemies and their friends, by whatever technical means are available. In the Post- Snowden era it is recognized that the growth of networked communications has resulted in spying on a scale and scope that was previously impossible.

While espionage has always been an expected and, indeed an expected aspect of international relations, the opportunities presented by the growth of cyber networks has brought into focus the differing goals of competing nation states.

While the United States appears to engage in sweeping espionage, it appears to do so solely for military and political intelligence in order to leverage the nation's interests around the world. The difference between China and the United States, for instance, is that China also engages in espionage for economic gain by stealing research and development and intellectual property.⁸

Cyber-crime is the purview of law enforcement (FBI and/or Interpol, depending on the context). It is generally assumed that rogue actors, hacktivist groups and individuals engage in cyber-crime. Typically, most cyber-crimes are defined through statutes or treaties. In the United States there are several laws dealing with cyber-crime, including, among others, the Computer Fraud and Abuse Act (CFAA), the Stored Communications Act (SCA), the Wiretap Act and Pen Register/Trap&Trace. There are also treaties that govern cyber-crime between nations, such as the Council of Europe's (COE) Convention on Cybercrime.⁹

Such a simple and straightforward delineation begs the question, what, exactly do these terms mean? Who decides when cyber-espionage or cyber-crime crosses the line into cyber-attack? How is it decided? What are the

⁸ Noah Bledstein, *Is Cyber Espionage a Form of Market Manipulation*, 2, 1 J. L. & Cyber Warfare (2012).

⁹ Convention on Cybercrime, Budapest, Sept. 23, 2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

distinguishing factors of each? Which laws apply? This paper will examine and provide answers to these questions. The first part will specifically, but briefly define each term, providing definitional granularity. The next part will provide a general examination of the laws that pertain to each term. Finally, the terms will be compared and contrasted showing how they can be easily confused and substituted; each for the other, causing the confusion discussed above.

II. Definitions

A. Cyber Attack

Not to oversimplify, but cyber-attack is nothing more than an attack via cyber means. Of course that begs the question, what is an attack? A kinetic attack is an event that either causes damage/destruction to property or injury/death to people. In short, an event causing violent consequences will constitute an attack. Thus, the focus is on the consequences and not necessarily the means or methods used to create the consequences; it is an effects-based inquiry. A cyber attack, therefore, *should* be a cyber event that causes either damage/destruction to property or injury/death to people. Determining a cyber attack also *should* be an effects-based inquiry, determining whether damage/destruction to property or injury/detach to people has occurred. I highlight “should,” because whether we like it or not, cyber is just different and does not neatly fit into prescribed definitions or an

effects-based inquiry, which will be discussed below.

A formal, governmental definition follows, but in my opinion is not very helpful – “cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains.”¹⁰ It should be noted that the additional terms, degradation, disruption, destruction and manipulation are not further defined. Presumably one has to seek guidance from a dictionary. Doing so provides a vast range of activities, covering an extremely broad swath of deeds. Perhaps it is easier to ask, “What does not constitute a cyberspace attack?” The answer seems to be items that would, at first blush, appear to actually meet the definition above, but the direct denial effects are either *not* hidden or *do not* manifest in the physical domain. Thus, the hinge for cyber attack, under the US definition, rests solely on whether the effects are either hidden or manifest in the physical domain. These terms seem to be mutually exclusive – on one hand the effects are hidden, but on the other they manifest in the physical domain. So, although the second part of the definition seems to be a limitation, it is still incredibly broad, covering either those cyber-intrusions that are hidden *or* those that

¹⁰ Joint Chiefs of Staff, Joint Cyberspace Publication (Joint Publication JP 3-12) (July 5, 2010, incorporating change 1 (Nov. 30, 2011) (hereinafter JP 3-12).

manifest physically. The definition also provides a way for DoD to engage in cyber activities that would not constitute a cyber attack, at least per its own definition thereof. If the direct effect is not hidden or does not manifest in the physical domain, then it would not be considered a cyber-attack per the definition. Ostensibly, this gives military commanders more leeway to utilize cyber as a tool during hostilities.

B. Cyber Crime

Boiled down to its essence, cyber crime is simply committing crime via cyber means; usually theft or fraud or hacking. Individual cyber crimes are defined by statute or treaty. For instance, the CFAA (AKA the “hacker” statute) includes seven substantive offenses: obtaining national security information, accessing a computer and obtaining information, trespassing in a government computer, accessing a computer to defraud and obtain value, damaging a computer or information, trafficking in passwords, threatening to damage a computer.¹¹ The SCA generally prohibits unlawful access to and disclosure of stored information.¹² The Pen Register/trap & trace generally prohibits obtaining and disclosure of meta-data or the data associated with content data.¹³ The wiretap act prohibits the interception of the contents of communications.¹⁴

¹¹ 18 U.S.C. § 1030.

¹² 18 U.S.C. §§ 2701-2709.

¹³ 18, U.S.C. §§ 3121-3127.

¹⁴ 18 U.S.C. §§ 2510-2522.

The COE Convention generally deals with infringements of copyright, computer-related fraud, child pornography, hate crimes and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and Lawful interception.¹⁵

Cyber crime occurs every day around the world on a vast scale. Much of it goes unreported and undetected. Last year cyber-thieves stole \$45 million from numerous ATMs around the world.¹⁶ “In the place of guns and masks, this cybercrime organization used laptops and the Internet,” said Loretta E. Lynch, the United States attorney in Brooklyn. “Moving as swiftly as data over the Internet, the organization worked its way from the computer systems of international corporations to the streets of New York City, with the defendants fanning out across Manhattan to steal millions of dollars from hundreds of A.T.M.'s in a matter of hours.”¹⁷ One of the main issues with cyber crime is the speed at which it occurs. “The difference today is that the dynamics of the Internet and cyberspace are so fast that we have a hard time staying ahead of the adversary,” said Robert D. Rodriguez, a special agent with the Secret Service for 22 years and now the chairman of Security Innovation Network. “And because these crimes

¹⁵ Convention on Cybercrime, Budapest, Sept. 23, 2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

¹⁶ Marc Santora, *In Hours Thieves Took \$45 in ATM Scheme*, N.Y. TIMES, http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?pagewanted=all&_r=0.

¹⁷ *Id.*

are global, even when the authorities figure out who is behind them they might not be able to arrest them or persuade another law enforcement agency to take action.”¹⁸

C. Cyber Espionage

Much like cyber attack, cyber espionage is nothing more than espionage via cyber means. This begs the question, what, exactly is espionage? Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense of a state. In the United States, one must do so with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.¹⁹ What exactly is “information about the national defense?” It is easier to think of such information as classified information. Each nation has its own information classification system. In the United States we generally only deal with four classifications; top secret, secret, confidential and unclassified. For official use only (FOUO) is often seen and just as often confused with classifications. FOUO, however, is a dissemination control and not a classification. It identifies information which may not be appropriate for public release.²⁰ So, cyber espionage is really just theft of classified national defense information. Of course, as mentioned

¹⁸ *Id.*

¹⁹ 18 U.S.C. §§ 792-798.

²⁰ DoDM 5200.01

above, countries like China also engage in cyber-espionage for economic reasons. So, cyber-espionage can more clearly be defined as theft of classified national defense information *and* persistent and invasive economic espionage on a massive scale.

Traditional espionage required physical intrusion of the sovereignty of another nation to obtain information – whether by the spy or his/her agent and access was much more limited. With cyber-espionage, the risk of capture and/or embarrassment is essentially non-existent due to the very nature of cyber. Today, spies have carte blanche to operate without fear of prosecution and also have, for the most part, unfettered access. Perhaps the worst that happens today is that the spy loses system access upon being “captured.” Of course, the spy simply reestablishes access or gains access to another system. Law enforcement and system defenders are left playing whack-a-mole.

III. Laws

A. Cyber Attack

The laws governing cyber attack are commonly referred to as the law of war or law of armed conflict, which include the United Nations Charter and the Geneva Conventions. Specifically, articles 2(4) and 51 of the UN Charter discuss use of force and armed attack, which are the main areas of concern. Trying to pin down terms and

definitions often requires digging for additional clarification. For instance, what does “use of force” and “armed attack” mean? When, exactly, do cyber intrusions cross those lines?

Despite numerous attempts to do so, i.e., the Tallinn Manual and, the Schmitt Analysis, there is no solid, international consensus when a cyber-intrusion equals a use of force or armed attack to be considered an actual cyber-attack. Although the Schmitt Analysis is widely accepted, it fails to address certain key areas and lacks consistent uniformity.²¹ Tallinn merely suggests certain rules be used in deciding cyber issues during international conflict. Tallinn, however, doesn’t offer much in the way of groundbreaking novelty.²² Cyber is older than Tallinn and states have been utilizing cyber capabilities for some time without gross deviation or violations. Tallinn seems to offer nothing more than recent and current state practice in the absence of customary international law, i.e., what we’ve already been doing. Cyber is still too new for customary international law to have fully developed.²³ It will take many more years to develop.

Article 2(4) under the UN Charter demands that, “All Members shall refrain in their international relations from the threat or use of force

²¹ James E. McGhee, *Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy*, 2 J. L. & Cyber Warfare (2013).

²² *Id.*

²³ *Id.*

against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”²⁴ One can only use force in self-defense if subject to an Armed Attack (or authorized to do so by the Security Council).

Article 51 under the UN Charter states, “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.”²⁵

Despite having two apparently separate thresholds, the position of the United States is that, “the inherent right of self-defense potentially applies against any illegal use of force.... [T]here is no threshold for a use of deadly force to qualify as an ‘armed attack’ that may warrant a forcible response.”²⁶ This has long been its official position.²⁷ Thus, for the United States, the question isn’t whether a cyber intrusion constitutes an armed attack, but whether it constitutes an illegal use of

²⁴ U.N. Charter, art. 2, para. 4.

²⁵ U.N. Charter, art 51.

²⁶ Harold Honhgu Koh, Legal Advisor of the Dep’t of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* <http://www.state.gov/s/l/releases/remarks/197924.htm>.

²⁷ *See, e.g.*, Abraham D. Sofaer, International Law and the Use of Force, in 82 AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 420, 422 (1988). Sofaer was at the time the State Department’s Legal Adviser.

force and therefore a cyber-attack. What then, is a use of force in the cyber arena?

It turns out that for the United States, the physical effects of a cyber intrusion are key. This should already sound familiar as previously discussed above – a cyber intrusion will constitute a cyber attack if the *effects* are similar to those caused by a kinetic strike. In his speech, Mr. Koh proclaimed, that “[c]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.”²⁸ For him, and the United States, it is merely equating cyber with kinetic: “if the physical consequences of a cyber attack work the kind of physical damages that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.” Mr. Koh goes on to suggest that “[i]n assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues.”²⁹ Using this approach, and only this approach, seems to make the answers very easy. It is not difficult to look at a cyber intrusion and determine whether the physical consequences thereof are similar to a comparable kinetic strike.

²⁸ *Id.*

²⁹ *Id.*

There is no argument amongst nations, or at least no serious argument, that the LOAC applies to cyber. I have also previously argued that this is not a surprise – we have been abiding by the LOAC for many years now while using cyber. Cyber is merely another tool/capability, much like a kinetic tool/capability, that a commander has at his/her disposal to use during conflict.³⁰ To be sure, it is the position of the United States, its allies, the Tallinn Experts and, most other nations that have considered the question.

B. Cyber Crime

Under Title 18 there are several sections dealing with different aspects of cyber crime. Section 1030 is the Computer Fraud and Abuse Act. It imposes both criminal and civil liabilities on a person who intentionally accesses a computer without authorization or exceeds authorized access in using a computer, thereby obtaining information from a computer that is used in or affecting interstate or foreign commerce.³¹ It does not specifically cover use of computers to commit crimes, but address actions impacting or causing loss or damage to computers and data and theft of data. It includes seven substantive offenses: obtaining national security information, accessing a computer and obtaining information, trespassing in a government computer, accessing a computer to

³⁰ See James E. McGhee, *supra* note 21.

³¹ 18 U.S.C. § 1030.

defraud and obtain value, damaging a computer or information, trafficking in passwords, threatening to damage a computer, and involving actions against a protected computer.³² “Protected computer” is a term of art referring to a computer used by the United States Government, a financial institution, or used in or affecting interstate or foreign commerce or communication. In other words, essentially any computer connected to the Internet.³³ It is admittedly broad, confusing and some claim abused by prosecutors.

Sections 2701-2709 codify the Stored Communications Act. It generally prohibits unlawful access to certain stored communications, regulates voluntary disclosure by network service providers of customer communications and records and, creates a code of criminal procedure that government law enforcement officers must follow to obtain stored communications from network service providers. Thus, anyone who obtains, alters, or prevents authorized access is subject to criminal penalties.³⁴ “Stored communications” are wire or electronic communications that are in temporary, intermediate storage incidental to transmission or that have been put in backup protection storage.³⁵ In other words, stored communications are data that are resting, not moving. An “electronic communication service” is

³² *Id.*

³³ *Id.*

³⁴ 18 U.S.C. § 2701-2709.

³⁵ 18 U.S.C. § 2510(17)

any service that provides to users thereof the ability to send or receive wire or electronic communications.³⁶ This is also known as network service providers, including Internet service providers, telephone companies and cell phone service providers.

Sections 3121-3127 cover the pen register/trap and trace. It concerns the real-time collection of addressing and other non-content information relating to communications; in other words, meta-data.³⁷ A pen register records what numbers were dialed from a phone, much like your normal phone bill. A trap and trace device records what numbers called a particular phone, like a caller ID. The parameters include dialing, routing, addressing and/or signaling information and entail almost all non-content information in a communication.³⁸ The definition includes both device and process, making the statute applicable to software as well as physical devices. Finally, it also applies to computer network communications.

Sections 2510-2522 cover the wiretap act. It prohibits the interception of the contents over wire, oral, and electronic communications in transmission by third parties who were not a party to the communication.³⁹ It generally has two purposes – protecting the privacy of wire and oral

³⁶ 18 U.S.C. § 2510(15)

³⁷ 18 U.S.C. § 3121-3127.

³⁸ *Id.*

³⁹ 18 U.S.C. § 2510-2522.

communications and delineating uniform circumstances and conditions under which the interception of wire and oral communications may be authorized. There are five requirements to meet the elements of the statute: 1) the intentional 2) interception 3) of the contents 4) of a wire, oral, or electronic communication 5) by use of a device.⁴⁰ A wire communication is an aural transfer over wire, cable, or other like connection; in other words, a transfer containing a human voice. Electronic communications generally include those communications if it is neither carried by sound waves nor can be fairly characterized as one containing the human voice.

The COE Convention is broken into several titles – each dealing with certain categories of offenses, delineated in articles. Title 1 covers offenses against the confidentiality, integrity and availability of computer data and systems. It includes articles dealing with illegal access, illegal interception, data interference, system interference and misuse of devices. Title 2 covers computer-related offenses and includes articles covering computer-related forgery and computer-related fraud. Title 3 covers content-related offenses. Its article deals with offenses related to child pornography. Title 4 covers offenses related to infringements of copyright and related acts.⁴¹ It

⁴⁰ *Id.*

⁴¹ Convention on Cybercrime, Budapest, Sept. 23, 2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

was ratified by the United States, by unanimous consent, in August 2006. It entered into force in the United States on 1 January 2007.

C. Cyber Espionage

It is generally accepted that acts which are not explicitly forbidden under international law are presumptively legitimate. This is true for propaganda, psychological warfare or, most importantly for espionage to include cyber espionage. Although the Geneva Conventions do discuss spies, they do so in the context of armed conflict, but not for conflicts not amounting to armed conflicts. Professor Schmitt has stated that, “Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state’s territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace.”⁴² Of course, such a declaration begs the question; can cyber espionage ever constitute a use of force? It is difficult to conceive a scenario where it would, but perhaps in extreme circumstances it may. Since espionage is not generally prohibited under international law, one must look to domestic law.

The United States, as well as most other countries, has a criminal statute that criminalizes

⁴² Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum*, 56 VILLANOVA L. REV. 569 (2011).

espionage. Title 18, sections 792-799 covers various crimes, constituting espionage. The crimes include, harboring or concealing persons, gathering, transmitting or losing defense information, gathering or delivering defense information to aid a foreign government, photographing and sketching defense installations, use of aircraft for photographing defense installations, publication and sale of photographs of defense installations and disclosure of classified information.⁴³ “Classified information,” means information which, at the time of a violation, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution.⁴⁴

Title 18, Section 1831 covers economic espionage and outlaws, generally, theft, copying or duplicating, receiving, buying or possessing trade secrets either intending or knowing that it will benefit any foreign government, foreign instrumentality, or foreign agent.⁴⁵ Section 1832 proscribes converting a trade secret to the economic benefit of anyone other than the owner thereof.⁴⁶ The problem with espionage statutes is that one has to have jurisdiction over the person committing the offense. While true of any criminal statute, it is of particular concern with cyber espionage. If there is no physical penetration, and there would not

⁴³ 18 U.S.C. § 792-799.

⁴⁴ 18 U.S.C. § 798(b).

⁴⁵ 18 U.S.C. § 1831.

⁴⁶ 18 U.S.C. § 1832.

necessarily be with cyber-espionage, then the cyber-spies really have nothing to worry about. Moreover, if one can't even identify/attribute the specific perpetrator, then there is no body to have jurisdiction over.

IV. Juxtaposition

It should be clear by now that the terms cyber attack, cyber crime and cyber espionage are separate and distinct. Each refers to a particular set of cyber intrusions, having its own definitions and laws. Depending on how the cyber intrusion is defined, it could fall within the purview of either law enforcement (cyber crime or cyber espionage) or the military (cyber attack). Therein lies the rub – trying to determine how to define a particular cyber intrusion in the first place.

Despite the clear and distinct definitions of each kind of cyber intrusion, it is often difficult to determine, initially, just which kind it is. Most, if not all, cyber intrusions look alike, even to those trained to detect them. There is very little to distinguish a true cyber attack from a cyber crime or cyber-espionage – the tactics, techniques and procedures are essentially the same. Indeed, the only difference between them is the intent of the actor, which will likely be unknown, and a keystroke. For instance, it would be impossible to discern the true nature of a phishing scheme at first blush. Perhaps it is a criminal organization attempting to steal user names and pass words for

identity theft. Maybe it is a prelude to an attack or other use of force; an attempt to gain administrative privileges to shutdown the network. It could also just as easily be an act of espionage.

A cyber attack, therefore, *should* be a cyber event that causes either damage/destruction to property or injury/death to people. Determining a cyber attack also *should* be an effects based inquiry. However, the effects-based model, while useful for kinetic strikes, is not as useful for cyber intrusions. Moreover an effects-based model necessarily means we actually have to wait for the consequences to manifest before we can determine just what happened. In other words, we won't know what *kind* of cyber intrusion took place unless and until we can review the consequences. Therefore, we won't know who should respond or even how.

It can be argued that cyber intrusions happen so quickly that the consequences will manifest almost immediately and thus the effects-based model still works. However, consider the Stuxnet event as the most recent example of a true cyber attack. The "attack" consisted of at least three waves over 10 months and, took time to evolve.⁴⁷ The initial insertion into Iranian systems, however, was months, and perhaps even years earlier. It is uncertain whether the Iranians would have recognized Stuxnet for what it was had they detected it earlier; attack, crime or espionage. It is

⁴⁷ Falliere et al., W32.Stuxnet Dossier (Symantec, Feb. 2011).

certain, however, that they would not have waited for the consequences to manifest before taking action.

While it may prove convenient to compare cyber-intrusion effects to kinetic event effects, the comparison breaks down for those cyber intrusions that do not cause damage/destruction to property or injury or death to people. While the overall effect may be the same, the cyber intrusion may not cause any physical damage/destruction to property or injury/death to people. For instance, if a cyber intrusion and a kinetic strike both shut down a power grid; the overall effect is the same – loss of power. However, the kinetic strike would necessarily cause damage/destruction to property and also likely injure or kill individuals while the cyber-intrusion would not.⁴⁸ Moreover, there would still be some question of just what kind of cyber intrusion it was. Maybe it was a theft or espionage event that went badly.

How then to compare them? Is there a better method to determine whether a cyber intrusion rises to the level of attack? Should we instead use a combination of methods – effects-based and a non-effects based model?

I propose that analysts look at the sophistication of the cyber intrusion to help determine what kind it is. For instance, Stuxnet and

⁴⁸ See James McGhee, *supra* note 21.

the subsequent cyber-injections, i.e., Duqu, and Flame, were all highly sophisticated. In fact, it has been suggested that Flame is so complex that it may take up to ten years to fully analyze it.⁴⁹ However, it has also been suggested that Flame was not specifically designed as a cyber attack weapon, but rather an incredibly specialized cyber espionage tool. This may or may not prove to be absolutely true since its complexity will take years to unravel. In any event, the more complex and sophisticated the cyber intrusion, the more likely it is to be a weapon for cyber attack.

I also agree with Mr. Koh that the target and location of the event are important factors to consider. For instance, intrusions into supervisory control and data acquisition (SCADA) systems are more likely a cyber attack or preparation for one. These systems are industrial control systems, monitoring and controlling industrial processes. They include power generation, water treatment, oil and gas pipelines, chemical processing facilities, electrical power transmission and civil defense siren systems. There is little or no reason for a benign actor to perpetrate a cyber intrusion into a SCADA system. While one may argue that cyber-spies are just as likely to poke around in SCADA systems, it should be noted that most countries use the same or similar systems. So, there really shouldn't be

⁴⁹ Kim Zetter, *Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers*, WIRED, May 28, 2012.

anything of interest for cyber spies to steal that their countries don't already have.

Additionally, I agree that the actor behind the cyber-intrusion is an important factor. Cyber intrusions from certain countries or certain organizations are more likely to constitute a cyber attack or prelude thereto. Some may argue that attribution makes it difficult, if not impossible, to identify the actor. I think attribution is overrated as a concern. I'm not alone in my opinion. Leon Panetta has stated, "In addition to defending the department's networks, we also help deter attacks. Our cyber adversaries will be far less likely to hit us if they know that we will be able to link to the attack or that their effort will fail against our strong defenses. The department has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack. Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America."⁵⁰

I'm not suggesting that these factors alone would provide justification for a retaliatory strike

⁵⁰ Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City
<http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

rising to the level of an armed attack, without more evidence. I am, however, suggesting that a limited strike merely to stop the cyber intrusion would be justified, without waiting for the consequences of an effects based inquiry. Perhaps sending a stop command or severing the command and control nodes would be all that is needed.

It is interesting to surmise why cyber is so confusing despite the clear differences. Perhaps it is deliberate. It is well known that General Alexander, recently retired, dual-hatted as the Director National Security Agency and also Commanding General of United States Cyber Command, built a cyber empire⁵¹. It is therefore in the interest of our politicians and military commanders to define cyber attack as broadly as possible. This gives them the greatest leeway and the greatest power to deal with all things cyber. Take recent proposed cyber legislation as an example. Most proposals include sharing of information between private businesses and government, ostensibly to facilitate greater defense throughout both business and government.⁵² However, privacy advocates cry foul over what they see as significant government intrusion into private networks/records, i.e., government overreach.

⁵¹ James Bamford, *NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar*, WIRED, Jun. 12, 2013, <http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/all/>.

⁵² Electronic Frontier Foundation, *Cyber Security Legislation*, <https://www EFF.org/cybersecurity>.

Moreover, it is primarily the responsibility of the Department of Homeland Security (DHS) to defend the homeland, which includes cyber events.⁵³ In other words, DHS has both the authorities and responsibility, but they lack the required capability. It has been suggested that DHS will look to and call upon United States Cyber Command Commander, presently Admiral Rogers, in the event a cyber intrusion rises to the level of cyber-attack. The approval authorities for taking any offensive cyber action are very high. Perhaps this is because any offensive cyber action/intrusion is generally considered a cyber attack.

So far most businesses have been holding their own when dealing with cyber intrusions. It does not appear that they are in any need of protection from big brother – yet. Recent distributed denial of service attacks (DDOS), aimed largely at big banks, have proven unsuccessful.⁵⁴ Although initially some of the banks suffered shutdowns for extended periods of time, they have since be able to withstand the onslaught. I suspect that if they do suffer another major incident, then they'll call for help. Of course, I think it also depends on the business. For instance, if a SCADA system or the Federal Aviation Administration is attacked or shut down, then it seems right and

⁵³ Department of Homeland Security, *Cyber Security Overview*, <https://www.dhs.gov/cybersecurity-overview>.

⁵⁴ Nicole Perlroth & Quintin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0.

proper for the government/DoD to be involved from the get-go. If banks and other businesses are otherwise sufficiently protecting themselves, I see no need for government, specifically DoD, involvement, especially if the cyber intrusions are below use of force/armed attack, which makes the definition thereof, most important.

V. Conclusion

The term cyber attack has become ubiquitous in our everyday lives to the point we no longer understand the differences between an attack, crime and espionage. We just assume that any cyber-intrusion is the same as cyber attack. The general public gets the impression, from our politicians and media that we are under constant bombardment of cyber attacks. I've become convinced too that even our politicians no longer know the difference – if they ever did. This can have many negative consequences because it leads to confusion over roles and responsibilities. We end up with policy makers trying to dictate cyber policy to operators and net defenders, without knowing just what they are talking about. For instance, Representative Mac Thornberry (R-Texas) argued that the president should get input from congress on the government's use of computer viruses and other offensive cyber weapons. He argued that congress should have an opportunity to shape the rules for how and when U.S. hackers attack enemy systems. He stated, "The more you

have them sorted out ahead of time, the smoother things will go when the electrons start flying.”⁵⁵ I and most others in the cyber field would say that the operators and net defenders should be the ones providing input on what they can and can’t do and what they want and need the authority to do. The top-down approach doesn’t work very well when the folks making the rules don’t know the technical capabilities. We need a more generic and benign phrase that more clearly and closely describes the event.

I propose that all cyber events should initially be labeled as cyber intrusions. Once a more detailed analysis of the event provides additional evidence of its true nature, it can be further labeled as a cyber attack, cyber crime or cyber espionage. For instance, while it is true that the United States suffers thousands of cyber intrusions every day, it is not correct that we suffer a true cyber attack every day. Education of our leaders and active engagement with media outlets in this matter will help, but we must also engage each other. Far too many people who should know better continue to mischaracterize cyber intrusions. This reinforces the misperceptions of the general public, media and our leaders. Before we can have a serious conversation about cyber attack, we must all understand exactly what it is and what it isn’t.

⁵⁵ Brendon Sasso, *President should consult with Congress on rules for cyberattacks*, Rep. Thornberry says, THE HILL, Oct. 8, 2013, <http://thehill.com/blogs/hillicon-valley/technology/327237-president-should-consult-with-congress-on-rules-for-cyber-attacks-rep-thornberry-says>.

