

JOURNAL OF LAW & CYBER WARFARE

FOREWORD

Cyber Warfare and the Corporate Environment

By Chris Colvin, Daniel Garrie, and Siddartha Rao

ARTICLES

Cyberwarfare: Attribution, Preemption, and National Self Defense.

By John Dever and James Dever

Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy.

By James E. McGhee

Is Cyber Espionage a Form of Market Manipulation?

By Noah Bledstein

Volume 2 | Spring 2013 | Issue 1

(c) 2012 – 2013. Journal of Law & Cyber Warfare.

All Rights Reserved.

www.jlcw.org

EDITORS

Daniel B. Garrie, Esq., Editor-in-Chief
Siddartha Rao, Esq., Executive Editor

Associate Editors

Stephen Williams, Esq., Editor-at-Large

EDITORIAL BOARD

Alan Roper	Alex Carrillo
Chris Colvin	Dick Crowell
Douglas DePeppe	George Hull
Gus Dimitrelos	James Christiansen
Jeff Bardin	Jonathan E. Turner
Joseph E. Weiss	Larry Ponemon
Noah Bledstein	Patrick Grey
Richard Borden	Roei Haberman
Russell Walker	Thomas A. Johnson
Uma Chandrashekhar	William Spernow
Yoav Griver	

JOURNAL STAFF

Giri Vakkalanka	Kim Kopoff
Margaret Mak	Radhika Tiwari
Renee Almassizadeh	Sarah E. Haines

Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy

By James E. McGhee*

I. INTRODUCTION

Cyber law and policy are all the rage these days. Both are mentioned almost daily in the news. It is reported that China, Russia, Iran and North Korea are bombarding the US with cyber intrusions, both to the DoD networks as well as private networks.¹ Additionally, hacktivist groups like Anonymous and LulzSec are becoming household names. In addition, focused cyber threats have resulted in exposed intellectual property, research and development, military plans, proprietary information and extortion. For instance, when Coca-Cola was negotiating what would have been the largest foreign purchase of a Chinese company; Chinese hackers were inside the Coca-Cola network and were able to obtain details about the negotiations.² Needless to say, Coca-Cola did not make the purchase.

* Mr. McGhee is an operational cyber law 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 do not necessarily represent those of the US Air Force or any other US governmental entity.

¹ Todd Beamon, *Rep. Rogers: China and Russia Conduct 'Vicious' Cyberattacks on U.S.*, NEWSMAX, (May 28, 2013), <http://www.newsmax.com/newsfront/rogers-china-russia-cyberattacks/2013/05/28/id/506756>.

² David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit is Seen as Tied to Hacking Against U.S.*, NEW YORK TIMES

More recently it has been discovered that state actors have been going beyond mere theft and espionage. Now, they are worming their way into more sensitive networks. Iran has engaged in several high-profile distributed denial of service “attacks” on some of the nation’s largest financial institutions. Recently, the Wall Street Journal reported that, “Iranian-backed hackers have escalated a campaign of cyberassaults against U.S. corporations by launching infiltration and surveillance missions against the computer networks running energy companies.”³ This type of activity represents a striking escalation from simply stealing.

Cyber issues have also seized the attention of Congress and the White House. For several years now there has been an attempt to pass some form of cyber-legislation aimed at protecting the United States from cyber-intrusions. The most recent was executive order 13636, Improving Critical Infrastructure Cyber-security, which tasked the National Institute of Standards and Technology (NIST) to develop a voluntary framework for reducing cyber-security risks to critical infrastructure.⁴ It aims to promote voluntary information sharing between the government and those private industries responsible for the nation’s critical infrastructure. If nothing else, it is a step in the right direction. Other than that, nothing substantive has been passed by Congress or is likely to be passed in the near future.

(February 18, 2013), *available at*: <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=1&hp>.

³ Siobhan Gorman & Danny Yadron, *Iran Hacks Energy Firms, U.S. Says*, WALL STREET JOURNAL, May 24, 2013, at 4.

⁴ Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013), *available at*: www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

One of the continuing problems with cyber or dealing with cyber intrusions is the lack of uniformity in concepts, definitions, rules, policy, and law. In many instances, not only is uniformity lacking, but there is simply a void. While the NIST framework may provide uniformity, it is solely focused on critical infrastructure and therefore does not apply to the vast majority of businesses suffering intrusions. This leaves individual states to determine their own concepts, definitions, rules, policy and law regarding cyber. Moreover, cyber is still too new for customary international law to have developed. If we consider Moonlight Maze to be the first major state-on-state cyber incident, then there have only been about fourteen years for such customary law to develop.⁵ The length of time to develop customary international law can vary greatly, but generally takes a significant number of years. The customary law of war has developed over thousands of years, but the practice of limiting conflict evolved primarily in the last 150 years. As a result, there is no general international consensus on how to treat cyber and cyber intrusions. Attempts have been made, however, to create concepts, definitions, rules, policy and law regarding cyber. Some have, to a limited extent, proven useful; others, less so.

One of the main problems with these attempts is that they tend to equate cyber and kinetic strikes as being on the same footing. In other words, they tend to treat them exactly the same. As demonstrated below, this does not always result in clean and easy answers and sometimes leads to absurd results. These attempts also tend to focus on actual cyber-attacks, necessitating inquiry into use of force, armed attack, the United Nations (UN) Charter and the Law of War/Law of Armed Conflict. At this level, the answers are relatively

⁵ Moonlight Maze (1998-2001), probed government and academic computer systems in the United States.

easy, because the US already abides by those rules. The trickier area lies in the realm below use of force, specifically, cyber-espionage. Keeping in mind that there is no international law proscription against cyber-espionage, the question becomes: *can it ever rise to such a level that it threatens our national security? If so, how is it measured? What is it measured against? Who decides? Finally, can victims then respond accordingly or do they have to seek assistance from the proper government authorities? Is it self-defense or hacking back?*

This paper explores three such attempts and discusses the interplay between the Schmitt Analysis, Tallinn Manual and US cyber policy. It attempts to answer whether the Schmitt Analysis remains current and relevant, whether the Tallinn Manual offers anything substantive or new and whether US cyber policy is moving in the right direction. The next section briefly introduces the Schmitt Analysis, the Tallinn Manual and U.S. cyber policy. The subsequent section delves into a more detailed and nuanced discussion of each. The last compares and contrasts all three.

II. BACKGROUND

The Schmitt Analysis was first published in 1999 by Michael Schmitt.⁶ In that seminal work, Professor Schmitt identified a number of factors that would likely influence assessments by states as to whether particular cyber operations amounted to a use of force. Professor Schmitt was prescient in tackling the tough cyber questions in the previous century, over thirteen years ago. In 2011, Professor Schmitt published

⁶ Professor Schmitt, J.D., L.L.M., D.Litt., is Chairman of and Professor at the Department of Law, United States Naval War College. Professor Schmitt is also Honorary Professor at Durham University in the United Kingdom and former Dean of the Marshall Center in Germany.

another article, discussing three questions pertinent to international law governing cyber operations.⁷ In that work, he reiterates the factors first identified by him in 1999 as still being relevant to today's discussion regarding international law and cyber. In addition, Professor Schmitt also served as Director of the NATO Cooperative Cyber Defense Centre of Excellence's Tallinn Manual project from 2009 through 2012. The Tallinn Manual was published in early 2013.⁸

The Tallinn Manual consists of "rules" adopted unanimously by an International Group of Experts that are meant to reflect customary international law. Lately much has been heard about the Tallinn Manual in mainstream media as well as military channels. It is touted as a great breakthrough in the quest for international cyber law; the go-to reference for all nations. The common desire is for something in writing delineating international law as it applies to cyber warfare. It offers ninety-five (95) rules for the international use of cyber capabilities. The hoped for goal is a product nations can use to fashion their own legal parameters for international cyber activities. The Tallinn Manual is firmly rooted in the twentieth century development of the law of war (outside the United States more commonly referred to as International Humanitarian Law).

US policy regarding cyber can be traced to the early twentieth century. In a 1918 Joint Resolution, Congress authorized the President to assume control of any telegraph system in the United States and operate it as needed for the duration of World War I. The Communications Act of 1934 formed the Federal

⁷ Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum*, 56 VILLANOVA L. REV. 569 (2011).

⁸ The Tallinn Manual is available at:
<https://www.ccdcoe.org/249.html>.

Communications Commission (FCC) from the Federal Radio Commission and established a broad regulatory framework for all communications, by wire and radio, that has influenced the development of these technologies ever since. The Brooks Act of 1965 gave the National Bureau of Standards (NBS)—now the Department of Commerce’s National Institute of Standards and Technology (NIST)—responsibilities for developing automatic data processing standards and guidelines pertaining to federal computer systems. In 1984, Executive Order 12472 re-chartered the National Communication System (NCS) as those telecommunication assets owned or leased by the Federal government that can meet U.S. national security and emergency preparedness needs. The Department of Homeland Security inherited the NCS in 2003. In 1994, through the Foreign Relations Authorization Act, the Department of State was delegated authority over foreign policy related to international communication and information policy.⁹ Presidential Decision Directive 63 (PDD-63), signed in May 1998, established a structure under White House leadership to coordinate the activities of designated lead departments and agencies, in partnership with their counterparts from the private sector, to “eliminate any significant vulnerability to both physical and cyber-attacks on our critical infrastructures, including especially our cyber systems.”¹⁰ This policy was updated in 2003 with The National Strategy to Secure Cyberspace. It was further augmented later that year in Homeland Security Presidential Directive 7

⁹ See CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 2 (2009), *available* at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

¹⁰ William J. Clinton, Presidential Decision Directive 63/NSC-63 (May 22, 1998) at section II.

(HSPD-7), which assigned the Secretary of Homeland Security the responsibility for coordinating the nation's overall critical infrastructure protection efforts, including for cyber infrastructure, across all sectors working in cooperation with designated sector-specific agencies within the Executive Branch.¹¹ There have been many more updates and supplements and new Presidential Policy Directives as well as HSPDs. These strategies and policies are, by their nature, very broad and thus lacking in actionable directive authority.

III. SCHMITT ANALYSIS

The Schmitt Analysis consists of seven criteria to consider when determining whether a cyber incident/intrusion qualifies as either a use of force or armed attack under the United Nations Charter. First the criteria will be examined as enumerated and explained by Professor Schmitt. Next the factors will be considered in the current e-context in order to determine whether they still offer a useful method to characterize current and emerging cyber threats.

The first is severity, which Professor Schmitt suggests is the most important. The severity of an incident is determined by the harm or damage to individuals and property. Obviously, the more severe the consequences, the more likely the incident/intrusion will be seen as a use of force or armed attack. Those generating only minor inconveniences or irritation will never be so.¹² According to Professor Schmitt, "the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scale, scope, and duration of the consequences will have great bearing on the appraisal of their severity."¹³

¹¹ *Supra* n. 9.

¹² Schmitt, *supra* n. 7.

¹³ *Id.*

The second criterion is immediacy. “The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, states harbor a greater concern about immediate consequences than those that are delayed or build slowly over time.”¹⁴

The third criterion is directness. The greater the attenuation between the initial act and the resulting consequences, the less likely states will be to deem the actor responsible for violating the prohibition on the use of force. Directness examines the chain of causation between the initial incident/intrusion and the resulting consequences. The consequences can either be direct or indirect, depending on the nature of the incident/intrusion.

The fourth criterion is invasiveness. This criterion regards the degree to which a system is penetrated. “The more secure a targeted system, the greater the concern as to its penetration.”¹⁵ Thus, a secure system, such as SCADA systems or classified networks, which is penetrated, is far more invasive than an unclassified public network.

The fifth criterion is measurability. “The more quantifiable and identifiable a set of consequences, the more a state’s interest will be deemed to have been affected.”¹⁶ In other words, what is the measure of damage done as a result of the consequences? Can we put numbers on the cost or the dead or the amount of property damaged or destroyed?

The sixth criterion is presumptive legitimacy. Acts which are not forbidden are permitted; absent an

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

express prohibition, an act is presumptively legitimate.¹⁷ Therefore, those things that are strictly prohibited would tend more towards a use of force or armed attack, whereas those things that are not strictly prohibited would tend not to be.

The seventh and final criterion is responsibility. “The law of state responsibility governs when a state will be responsible for cyber operations. Responsibility lies along a continuum from operations conducted by a state itself to those in which it is merely involved in some fashion. The closer the nexus between a state and the operations, the more likely other states will be inclined to characterize them as uses of force, for the greater the risk posed to international stability.”¹⁸

Examining these factors in light of the current cyber threat environment, *how does one determine the severity of a cyber incident/intrusion if the sole concern is harm or damage done to either property or individuals?* Particularly, if the cyber event does not create similar effects that a kinetic strike would create? One of the key problems with insisting on using old rules, criteria and policies is that, on one hand they attempt to equate cyber events with kinetic events. For example, if a cyber event and a kinetic event both cause the same amount of harm or damage to either property or individuals, it is conceptually easy to claim that they should be treated the same. The rules apply in the same manner. To be sure, Professor Schmitt has stated, “Accordingly, cyber operations that directly result (or are likely to result) in physical harm to individuals or tangible objects equate to armed force, and are therefore uses of force.”¹⁹ On the other hand, cyber can create the same overall effects without causing lasting physical

¹⁷ *Id.*

¹⁸ Schmitt, *supra* n. 7.

¹⁹ *Id.*

damage or damage at all. For instance, if a cyber event and a kinetic strike both take out a power grid, plunging an area into darkness; the overall effect is the same. However, the kinetic strike would necessarily cause harm and damage to property and likely to individuals as well. By comparison the cyber event would not necessarily cause any physical harm or lasting damage at all. Moreover, the cyber event may very well be reversible. Thus, two events that cause the exact same consequence would, in fact, be treated differently under the old rules and, I submit, the Schmitt Analysis. Under the latter example, there is no physical harm or lasting damage and therefore, under the severity criterion, no use of force and certainly not an armed attack.

The next criterion is immediacy. With a cyber event, the intended effects may not become apparent for days, weeks or even months, as occurred with Stuxnet. A kinetic strike usually produces an instantaneous effect. A key question, therefore, is, when does the cyber event actually take place? Is it the point of insertion or the moment of “attack?” If we apply existing standards I believe Professor Schmitt would answer that the actionable event occurred at the moment of attack. Professor Schmitt has stated, “the introduction into a state’s cyber systems of vulnerabilities that are capable of destructive activation at some later date would not constitute a threat of the use of force unless their presence is known to the target state and the originating state exploits them for some coercive purpose.”²⁰ To be fair, he qualifies his statement by suggesting that a threat must be communicated in order to qualify under the UN Charter. I don’t necessarily disagree from a technical, legal point of view. That, however, simply begs the question, what constitutes a communication? Doesn’t the act of introducing destructive vulnerabilities

²⁰ *Id.*

designed for subsequent activation into another country's systems constitute a threat? Isn't the threat communicated by the mere insertion? If not, and we have to wait for the activation of such "devices", then when does the clock start for determining whether the effects are of immediate concern? If we look at Stuxnet, the "attack" consisted of at least three waves over 10 months and, took time to evolve.²¹ The initial insertion into Iranian systems, however, was months, and perhaps even years earlier. Can semi-autonomous delayed effect cyber capabilities register on the immediacy criterion continuum for meeting use of force or armed attack?

To add further confusion into the mix, Professor Schmitt's statement above, "likely to result" seems to be in contradiction to his other statement, "capable of destructive activation at some later date." If the destructive capability is known, then doesn't that fall within the "likely to result" category even without an overt communication from the adversary? If so, doesn't that qualify as a use of force? Let's look at a non-cyber example to illustrate the point. Assume a situation in which a criminal places a bomb in a house. The person is aware of, but unable to remove it and the bomb can be remotely activated. The criminal makes no overt threat to the family. Is this nonetheless a threat to the family? Clearly, the answer is yes. How is the introduction of a cyber vulnerability into control systems different? Is not the threat inferred?

The next criterion is directness. Here the cause and effect in the chain of causation needs to be understood. With kinetic strikes, the cause and effect are intimately related—the strike directly causes the damage or destruction. With cyber, the effects can be very indirect and attenuated. Cyber events may have third or fourth order effects that cause the measurable harm or

²¹ Falliere et al., W32.Stuxnet Dossier (Symantec, February 2011).

damage. Furthermore, cyber capabilities may have the ability to hide the cause or make it appear as if another cause is to blame. By examining the power grid shut-down by a cyber event further, assume that the perpetrator of the event was sophisticated enough to make it appear as if the shut-down was simply the result of either faulty equipment or operator error or even an act of God—lightning strike. Thus, the ultimate cause is extremely difficult or even impossible to discern. Most serious cyber events will be sophisticated enough to either hide the cause or shift the blame. If not, attempting to trace back the entire causal chain from second, third, fourth order effects and beyond may prove too difficult and time consuming to allow response within a reasonable window. Realize that simply because something is difficult it does not mean it is unworkable. However, when time is of the essence and with cyber it always is, the difficulty and timeliness of making a determination is a paramount concern. How far can this go down the rabbit hole before the subsequent effects are deemed too remote and too indirect? Would all of the subsequent victims be Mrs. Palsgraf?²²

The next criterion is invasiveness. Here the concern is with the security of the system penetrated and the depth of insertion by the adversaries. For instance, an intrusion into the public-facing website of a major bank is not nearly as invasive as a root-level intrusion into their internal network. Many of our financial institutions have recently been bombarded with DDoS (Distributed Denial of Service) events, which many

²² *Palsgraf v. Long Island Railroad Co.*, 248 N.Y. 339, 162 N.E. 99 (N.Y. 1928) is a seminal case in tort law, establishing the concept of proximate cause and foreseeability, limiting liability to the consequences of an act that could reasonably be foreseen rather than every single consequence that follows.

believe stem from Iran. Despite the increasing magnitude, at present these are more of a nuisance than a threat and the technique does not put sensitive information at risk. On the other hand, Chinese intrusions into DoD systems or Russian intrusions into SCADA systems would be extremely invasive. Professor Schmitt, however, cautions against applying this criterion too liberally because cyber exploitation is a ubiquitous tool of cyber espionage. He states, “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. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.”²³ Since it is virtually impossible to decide whether a cyber event is a prelude to an attack, an actual attack, a mere probe or espionage, until the ultimate event, how is this criterion useful at all today? Once again, one needs to wait-and-see the effect to make a proper determination. This means one will have to watch as an enemy pilfers information and exfiltrates it to know whether it is indeed espionage. Similarly, one will have to wait for an attack to begin before taking any response because one is unable to decide on a legally appropriate response without first knowing what *kind* of cyber event is playing out. By that point, it will be too late. On one hand, Professor Schmitt declares the intent of the adversary needs to be known before any action takes place. On the other, he states that disabling cyber security mechanisms to monitor keystrokes does not constitute a use of force. How does one know their intent in the latter scenario? The reality is that one does

²³ Schmitt, *supra* n. 7.

not unless the adversary announces their intent or one is already engaged in a declared armed conflict. Therefore, with cyber exploitation obfuscating our ability to make a determination, this criterion also offers little value in making such determinations.

The next criterion is measurability. It should go without saying that kinetic strikes are much more quantifiable and identifiable than the consequences of cyber operations. Kinetic strikes will likely result in damage or destruction to structures and to injury or death. Cyber consequences may not cause the same sort of easily recognizable results, yet they still produce the same ultimate effect as kinetic strikes. It may prove difficult, if not impossible, to measure, with any degree of accuracy, the subsequent consequences of a cyber event. Must one resort to trying to quantify the second and third order effects of a cyber event? Is it even possible to do so? Let us revisit the power-grid shutdown and examine the consequences thereof. A cyber event shuts down a power grid inside the United States, but causes no physical damage to any property. However, assume that it is sophisticated enough to merely act as a switch and simply turn off the power. The immediate effect is loss of power and is measurable by the number of people without power. The second and third order effects are much harder to measure. Perhaps physically weakened or elderly civilians die due to either lack of heat or lack of cooling, depending on the weather. Perhaps there is an increase in traffic fatalities due to lack of signaling lights. Maybe small children also die due to lack of operating medical services. Maybe looting occurs and property is damaged and people are injured. Can it be said that these are *direct* effects of the cyber event that can be quantified? This criterion is very similar to directness and the unforeseen victim discussion above. It is important to note that with

the kinetic strike, causing the exact same result—loss of power—the focus is only on the direct effects, namely, the damage and destruction to property and injury or death to individuals. One would not necessarily look any further, because it is not needed. With cyber, one necessarily will be forced to do so, just to balance the criterion equation. Once again there is an inconsistency. On one hand equating cyber with kinetic events that cause the same effects and similar amounts of damage would result in similar measurability when applying the same rules and analysis. On the other hand, applying the same rules to cyber events that cause the overall same effects, but without necessarily creating the same measurable event yields different results. Treating cyber differently, on its own, may yield no measurable effects at all. Measurability, therefore, is not necessarily a good gauge, especially where the cyber event causes no actual physical harm or destruction.

The next criterion is presumptive legitimacy. This criterion, much like invasiveness, must be applied with caution. If you recall, acts which are not explicitly forbidden under international law are presumptively legitimate. This is true for propaganda, psychological warfare or, most importantly for cyber- espionage. Here one runs into the exact same problem as with invasiveness. Namely, it is virtually impossible to decide whether a cyber event is a prelude to an attack, an actual attack, a mere probe or espionage, until the ultimate event. Otherwise, one is left guessing and playing catch-up after the fact. In addition, today's cyber environment is populated with many non-state actor adversaries. Thus, presumptive legitimacy is not a good indicator for them because their acts are considered to be criminal. The problem, however, is determining the actor in the first place. Attribution plagues us once again. Even if the point of origin can be determined that

is not definitive evidence of either state or non-state actor involvement. Unfortunately this is true even when the point of origin appears to be a government computer system. In the current cyber environment, presumptive legitimacy is only beneficial if one knows not only the intent of the actor up front but also the actor's identity. As discussed, knowing either is almost impossible in cyber, at least up front.

The final criterion is responsibility or, to be more precise, state responsibility. The more closely related an action is to a state, the more likely it will be seen as a use of force or armed attack. Professor Schmitt tells us that, "responsibility lies along a continuum from operations conducted by the state itself to those in which it is merely involved in some fashion."²⁴ While true, the practical utility of this standard in the current cyber environment is questionable. As discussed, it is very difficult to determine the intentions behind specific cyber events. Even if an event appears to be traceable to a specific country this is no guarantee that that country is responsible for or even condones the activity. However, international law allows some leeway, with regard to attribution. Professor Schmitt writes that, "So long as the victim-state has taken reasonable steps to identify the perpetrator of an armed attack, cyber or kinetic, and has drawn reasonable conclusions based on the results of those efforts, it may respond forcefully in self-defense."²⁵ In the rapidly evolving cyber landscape, a standard of care for reasonable efforts does not exist, and is unlikely to solidify in the foreseeable future. "That a state drew the wrong conclusion is of no direct relevance to the question of whether it acted lawfully in self-defense. Its responses are assessed as of the time it took

²⁴ *Id.*

²⁵ *Id.*

action, not ex post facto.”²⁶ The assessment only has to be reasonable for the victim to take action against a cyber-intrusion that arises to either a use of force or armed attack. The difficult question is, even with this leeway, does existing technology support a “reasonable” determination? Although the ability to unmask one’s adversaries is increasing, so is the ability of the adversaries to hide, spoof or cover their identity. Similarly, this criterion presents the same problems that presumptive legitimacy presents regarding unmasking the adversary.

To be fair, Professor Schmitt recognizes the limitations of his Analysis. He states: “The criteria are admittedly imprecise, thereby permitting states significant latitude in characterizing a cyber operation as a use of force, or not.”²⁷ He has suggested that the factors are useful but not determinative, and they should not be applied mechanically. Rather, they need to be applied holistically according to the relevant context—that is, which factors are important and how they should be weighted will vary on a case-by-case basis. Moreover, the factors are not meant to be exhaustive, though they are often treated as such.²⁸ The framework is more useful for post hoc forensic analysis of particular cyber-attacks than for characterizing real-time operations.²⁹ He also writes that, “In light of the grave consequences that cyber operations can cause without physically harming persons or objects, this interpretation may seem wholly unsatisfactory. Nevertheless, it is the extant law.”³⁰ Finally, he admits that, “The legal analysis ... should strike most readers as unsatisfactory.

²⁶ *Id.*

²⁷ *Id.*

²⁸ Schmitt, *supra*, n. 23.

²⁹ *Id.*

³⁰ Schmitt, *supra* n. 7.

Clear fault lines in the law governing the use of force have appeared because it is a body of law that predates the advent of cyber operations.”³¹

In light of the above, the Schmitt analysis is still useful for states, but only to determine if an event that has already transpired met the threshold of use of force or armed attack. This has real value as it allows a state to go to the UN Security Council for proper action or take action on its own, i.e., self-defense. It can also justify countermeasures once a proper determination is made. However, if the response is too far removed from the actual event/intrusion, it may appear more like reprisal than a legitimate response. The Analysis is lacking, however, when considering current, on-going cyber operations. The problem is that current and on-going cyber operations are precisely what states and private industry are most concerned with characterizing today. His analysis was novel, groundbreaking and relevant at the time it was first proposed and for several years thereafter. As today’s cyber realm has blossomed and moved to the forefront of our military, commercial and political lives, the relevance of this analysis is less clear.

In its day, the Schmitt Analysis worked and worked well. Ten years ago a cyber intrusion was rarely recognized until the effects manifested and alerted the victim. Using the Schmitt Analysis to determine whether those effects constituted a use of force or armed attack proved useful. Today, robust network defenses often discover such intrusions as they happen. The key now lies in making a Schmitt Analysis determination concurrent with the cyber intrusion. In the operational world this is referred to as law at the “speed of need.” Moreover, today an intrusion is just as likely to originate with a non-state actor like Anonymous or Lulzsec or

³¹ *Id.*

some other rogue or terrorist group. If true, then the Schmitt Analysis has no utility because it does not apply to non-state actors. Additionally, the vast majority of intrusions do not rise to the level of use of force or “armed” attack, but are exactly the events that our government and businesses deal with daily. While it may be true that the “black swan” or Pearl Harbor-like cyber event is worrisome, it has been reported that events of this magnitude have already been experienced, but in the context of cyber espionage rather than cyber-warfare. Thus, it is time for a new set of rules or an update of the Schmitt Analysis.

IV. TALLINN MANUAL

The Tallinn Manual consists of ninety-five rules meant to reflect customary international law as it applies to cyber. It was released by NATO’s Cooperative Cyber Defense Centre of Excellence in March 21, 2013 and is the product of a three-year project. The rules were developed by an “International Group of Experts,” including distinguished legal academics and practitioners, supported by a team of technical experts. USCYBERCOM, the International Committee of the Red Cross, and NATO each provided an observer.³² Upon its release, the Manual caused quite a stir in the media and military channels. Despite its own admonitions not to use it as an authoritative document or settled law, many are in fact doing so.

Boiled down to its essence, the Manual answers a fundamental question; does international law apply to cyber activities? Not surprisingly, the answer is yes. Next the Tallinn authors attempted to dissect how international law applies to cyber. They discuss the customary, international rules, norms and laws applicable to traditional conflict as applied to cyber and

³² See *supra* n.8.

make determinations regarding whether those rules, norms and laws are equally applicable when using cyber capabilities.

In answering the overarching question, the Tallinn Group looked at the International Court of Justice's Nuclear Weapons Advisory Opinion, where the Court considered whether the prohibition on the use of force governed the use of nuclear weapons.³³ The Court opined that the rules governing the use of force, "apply to any use of force, regardless of the weapons employed."³⁴ The Group concluded that since the rules apply to nuclear weapons, cyber is not so different and that the rules also apply to cyber. The Court also determined that international treaty and customary law that predated nuclear weapons governs their employment; thus so too with cyber. Finally, the Group considered the Martens Clause from the 1899 Hague Convention II, "[i]n cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."³⁵ Therefore, even in the absence of treaty law, humanitarian customs still apply. This is hardly controversial. In essence the Group seems to be restating well understood standards of state practice in the kinetic realm, and then restating the standards based on their understanding of what constitutes cyber. Indeed, Professor Schmitt reminds one that international law requires a legal review of

³³ Legality of the Threat or Use of Nuclear Weapons, 1996 I.C.J. 226 (May 14, 1993) (Advisory Opinion).

³⁴ *Id.*

³⁵ Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8 1977, 1125 U.N.T.S. 3 (hereinafter Protocol 1).

weapons prior to fielding, “which *confirms the fact* that cyber weapons, as with other new weapons are subject to preexisting law.”³⁶ (Emphasis added) To be sure, Air Force Instruction 51-402, implements international law and mandates such a review.³⁷

The introduction to the Manual describes and delineates what it does and does not do. It spells out, with great particularity, its application and non-application to certain areas of law and conflict. Of note, the Group limits their discussion to use of force and armed conflict. Cyber activities that do not rise to the level of either, which includes espionage, are not discussed. The Group focused on cyber-to-cyber operations, excluding kinetic-to-cyber operations and likewise excluding traditional electronic warfare attacks, like jamming.³⁸ Their rationale for excluding discussion on those topics is that they are already well understood under the law of armed conflict. This ignores the overlap and fusion of electronic warfare and cyber warfare capabilities, an issue of great interest within the military Services.

The Manual is additionally divided into two major parts, Part A and Part B. Part A discusses International Cyber Security Law and Part B discusses The Law of Cyber Armed Conflict. The parts are broken down into chapters and sections and each section encompasses the rules, discussing the details and answering the pertinent questions to arrive at the 95

³⁶ Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13 (2012), available at: http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.

³⁷ Secretary of the Air Force, Air Force Instruction 51-402, Legal Reviews of Weapons and Cyber Capabilities (July 27, 2011), available at: <http://www.fas.org/irp/doddir/usaf/afi51-402.pdf>.

³⁸ See *supra* n.8.

rules. For instance, Chapter One discusses states and cyberspace, including sovereignty, jurisdiction and state responsibility. Chapter Two discusses the use of force, including its prohibition and self-defense. Chapter Three, under Part B, discusses the law of armed conflict generally. Chapter Four discusses the conduct of hostilities, focusing on attacks. Chapter Five discusses certain persons, objects, and activities, including medical, religious, detained, children and cultural property, the natural environment and collective punishment. Chapter Six discusses occupation and Chapter Seven discusses neutrality.³⁹

Let's look at some of the rules as enumerated and explained by the Group. Following that, exploring them in the context of whether they offer anything new and substantive or whether they merely restate current practice.

Rule one reads, "A state may exercise control over cyber infrastructure and activities within its sovereign territory."⁴⁰ The experts agreed that, "although no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."⁴¹ Likewise, the experts declared that, "it is the sovereignty that a State enjoys over territory that gives it the right to control cyber infrastructure and cyber activities within its territory. Accordingly, cyber infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace is subject to the sovereignty of the territorial state."⁴²

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

While it is true that no state exercises control over cyberspace it makes perfect sense to declare a state exercises control over those things within its sovereign territory. This revelation is not surprising. Certainly states exercise control over all infrastructure within their sovereign territory, whether government owned or privately owned. For instance, the government regulates dams, power plants, buildings, roads, telephony, etc. and, has been doing so for many years. In this context there is little difference between normal, old-fashioned infrastructure and cyber infrastructure. Both are composed of physical components residing within sovereign territory. Likewise traditional activities that occur within the sovereign territory of a state have been controlled or regulated for many, many years. Cyber activities occurring within the sovereign territory of a state are not sufficiently different from traditional kinetic activities that different rules should apply. Phone and other wire communications are a classic example of “traditional” activities that have been controlled and/or regulated by states. Cyber is a variation on the same theme. Smart-phones are a prime example of both old and new technologies converging in one device. Both technologies, however, are regulated and controlled. Therefore, it stands to reason that the same rules would apply to cyber activities and infrastructure as for traditional activities and infrastructure. The most that this rule provides is, perhaps, definitional granularity between cyberspace itself and cyber infrastructure.

Rule two provides, “Without prejudice to applicable international obligations, a State may exercise its jurisdiction: (a) over persons engaged in cyber activities on its territory; (b) over cyber infrastructure located on its territory; and (c) Extraterritorially, in accordance with international law.”⁴³ Jurisdiction

⁴³ *Id.*

encompasses the authority to prescribe, enforce, and adjudicate. It extends to all matters, including those that are civil, criminal, or administrative in nature. From a legal perspective, jurisdiction is determined by physical or legal presence of a person or object within the sovereign territory. This is known as either in personam or in rem jurisdiction. In other words, a state can exercise jurisdiction over the activities of persons located within the state and also over objects within its territory.

This is long established state practice. Several U.S. laws, namely the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, have resolved many of these tricky jurisdictional issues long ago. Moreover, aspects of copyright and patent law have also answered some, if not all, of these types of jurisdictional questions. Attribution in the cyber realm makes it difficult to determine, with legal accuracy, who or what is behind a cyber event. In some cases, it is even difficult to determine the origin of the event. Even so, attribution is more of a technical issue than a legal one. Besides, as our technology has evolved, the existing laws mentioned above have maintained their applicability regardless of the difficulty in applying them. This rule simply expands on rule one—if a state has control over certain things, people and objects, then legally, it should also have jurisdiction over them. It should not surprise anyone that a state exercises jurisdiction over persons engaged in non-cyber activities within its territory or jurisdiction over non-cyber infrastructure. Why then would a state not also have jurisdiction over persons engaging in cyber activities within its territory or over the cyber infrastructure being utilized? Indeed, the examples mentioned above prove that the United States has been doing just that.

Rule nine states, “[A] State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible state.”⁴⁴ Some of these terms require definitions to fully understand stated rule. “Countermeasures are necessary and proportionate actions that a ‘victim-State’ takes in response to a violation of international law by an ‘offending State’ to induce compliance with international law by the offending State.”⁴⁵ An internationally wrongful act occurs when, “conduct consisting of an act or omission: (a) is either attributable to a state under international law; and (b) constitutes a breach of an international obligation of the state.”⁴⁶

Rule nine adds cyber to an accepted definition. States have always been authorized to resort to countermeasures. Now they may do so using cyber countermeasures. It is helpful to think of cyber as one of many tools in a toolbox of national power that sovereign states have at their disposal. Under international law, states have an obligation to ensure weapons they anticipate using are lawful. Though internal mechanisms for ensuring compliance can vary, in general once a weapon has been reviewed for compliance with the Law of Armed Conflict (“LOAC”), and its use is found to be lawful, it may be added to a nation’s arsenal. Likewise, once a cyber capability has

⁴⁴ See The Tallinn Manual, *supra* n. 8.

⁴⁵ *Id.*

⁴⁶ Draft Articles on Responsibility of States for Internationally Wrongful Acts, pt. 2, Arts. 28–41, in Report of the International Law Commission on the Work of Its Fifty-third Session, UN GAOR, 56th Sess., Supp. No. 10, at 43, UN Doc. A/56/10 (2001), *available at*: http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, reprinted in JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION’S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES (2002).

been reviewed for compliance with the LOAC, and found to be in compliance, it also may be provided to operational units for use. The LOAC review is not a substitute for a subsequent review of the contemplated use of a weapon in a specific operation; however it is a necessary predicate safeguard. Granted, countermeasures are not the same thing as responses to either a use of force or armed attack. Cyber-countermeasures are, nonetheless, tools that remain an available option. It would make little or no sense to allow states to use cyber in response to use of force and armed attacks, but to limit the tools available for lesser offenses.

Rule twenty states, “[c]yber operations executed in the context of an armed conflict are subject to the LOAC.”⁴⁷ This, however, begs the question, when *aren’t* cyber operations subject to LOAC? The most obvious and relevant answer is, when the operation is conducted as espionage.

Cyber-capabilities are tools to be used by military commanders just like any other tool or weapon they would use. New cyber capabilities undergo a capabilities review, just like kinetic weapons do. Therefore, it stands to reason that the same rules apply to cyber capabilities as to traditional kinetic weapons. To be certain, US commanders and their allies have been doing so for many years now. It is particularly noteworthy that the Tallinn Group specifically excluded discussing traditional electronic warfare like jamming because those rules are already well established. Cyber is not so different from those “traditional” methods and means that the rules would somehow be different or inapplicable. It is fair to suggest that cyber warfare is closely related to, and may have grown from electronic warfare. Cyber is much broader and encompasses many

⁴⁷ See The Tallinn Manual, *supra* n. 8.

more activities, but the underlying character of the activities is the same. It is accepted that, *any* operation executed in the context of an armed conflict is subject to the LOAC. It makes no difference what it is called or how it is defined. States cannot evade their duties and obligations under the LOAC by calling their operations by another name. It is DoD policy that, “[m]embers of the DoD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations.”⁴⁸ It should be noted that this is not new policy, merely the restatement of long-standing US policy.

Rule thirty defines cyber-attack as, “a cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”⁴⁹ It is generally understood that the focus, in defining an attack under the law of armed conflict, is whether the act produces violent consequences. Namely, whether any property was damaged or destroyed or whether individuals were harmed or killed. Therefore, it is not the act itself, but rather the subsequent consequences thereof that matters. The problem is that this rule fails to address the value of intangible property in a networked world. If a cyber operation prevents fuel from being delivered to aircraft and the aircraft are thus unable to complete a kinetic operation, is this an “attack.” It would seem so, though no injury, death, damage or destruction of objects occurred.

Thus, the Tallinn definition of cyber-attack is no more than the definition of attack with cyber tacked-on. It fails to address the central issue raised by the new

⁴⁸ Directive No. 2311.01E: DoD Law of War Program, U.S. DEP’T DEF. 2 (May 9, 2006), *available at*: <http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf>.

⁴⁹ See The Tallinn Manual, *supra* n. 8.

technical context. Of course, if one labels something as an attack, it must meet the definition of one. For instance, one could define a school as a building or other structure wherein people meet and are taught various subjects in a learning environment. To define a girls-school, one would simply state the same thing, but merely tack-on “girls”. Thus, a cyber-attack and a traditional kinetic attack are essentially the same thing, creating the same violent consequences. It is merely the manner in which they are initiated that differs. Although this rule states the obvious, it does create a situation where a cyber event and a kinetic event can be labeled different things even though they bring about the exact same result. A cyber event that shuts down a power grid may do so without causing any harm or damage at all, whereas a kinetic event, causing the same thing certainly causes damage and destruction. One would be an attack, but the other would not under this rule.

Rule forty-nine explains that, “[c]yber-attacks that are not directed at a lawful target, and consequently are of a nature to strike lawful targets and civilians or civilian objects without distinction, are prohibited.”⁵⁰

Once again the Tallinn Group merely substitute “cyber-attack” for traditional “kinetic” attack to reach a commonsense conclusion. Furthermore, US military commanders and their allies have been complying with this rule for some number of years now. Lawyers are embedded with operational and tactical units, carrying out attacks, to specifically provide legal advice regarding distinction. To be sure, international law requires that lawyers be available to offer such advice. Additional Protocol I (API) to the Geneva Convention states, “The High Contracting Parties at all times, and the Parties to the conflict in time of armed conflict, shall ensure that legal advisers are available, when necessary, to advise

⁵⁰ *Id.*

military commanders at the appropriate level on the application of the Conventions and this Protocol and on the appropriate instruction to be given to the armed forces on this subject.”⁵¹ Even though the United States has not ratified API, US rules also dictate that commanders have legal advice. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5810.01D, directs Combatant Commanders to, among other things, “Integrate legal advisers into planning sessions and conferences for military operations and exercises to enable them to provide advice concerning domestic and international law, including the law of war, compliance.”⁵² In other words, this rule informs that the traditional, core principles of the law of war; namely, distinction, apply to cyber-attacks as they do for any attack. Cyber certainly predates the Tallinn Manual and cyber capabilities used in and during war also predates the Tallinn Manual. Nonetheless, US commanders and allies have been abiding by the LOAC even when using cyber tools to create kinetic-like effects. Indeed, the Tallinn Group has noted in Rule twenty that LOAC applies to cyber. Rule forty-nine then, is simply providing more, unneeded details, namely noting the principle of distinction is also applicable to cyber.

Rule ninety-one declares that, “The exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited.”⁵³ In other words, one can’t deliberately target cyber infrastructure in a neutral state/territory or within the control of a neutral state, if also within neutral territory.

⁵¹ Protocol I, *supra* n. 35.

⁵² CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 5810.1D, IMPLEMENTATION OF THE DoD LAW OF WAR PROGRAM (30 April 2010) at para. 6f(2).

⁵³ See The Tallinn Manual, *supra* n. 8.

This is a well-established rule, customary in nature, in the kinetic realm. Its application, therefore, in the cyber realm is not startling. Indeed, it is wholly expected. Moreover, US and their allies have been in compliance for many years. Once again, this coincides with the principle of distinction. US commanders have been complying with the principles of the law of war for every tool they use, including cyber capabilities. To be sure, the use of cyber capabilities is so constrained, due to these issues and concerns, that the approval authority for their use is incredibly high.

Using the Tallinn manual one must consider equating cyber intrusions with kinetic strikes, amounting to use of force or armed attack. Thus, using the same rules for both seems to work. However, as has been demonstrated above, all cyber intrusions are not the same as kinetic strikes and therefore, the same rules cannot apply to both equally. Focusing on cyber intrusions falling below use of force precludes the application of the rules applicable to kinetic strikes.

Despite being over 250 pages and taking approximately three years to complete, the Manual really offers little new or surprising. It is an exercise of academic debate, essentially restating what has been practice for some time by the United States, but failing to address the central issues raised by the emerging technical landscape. The Manual “codifies” that practice by substituting-in the term cyber. Achieving international law for cyber is a complex challenge and will take many nations agreeing over a substantial period of years. The Manual would better serve practitioners by listing and discussing those rules which the Group could not reach a consensus. This is the work which needs to be done by the international law community in order to address the emerging cyber landscape. These are the questions that remain to be answered as

technology increases and cyber becomes even more conventional and widespread. The Manual's usefulness lies with the discussion of the rules and the rational. It allows legal advisors and practitioners to engage in spirited debate in those areas where the Group could not agree. This will help guide future debates and help answer some of the harder questions.

V. U.S. POLICY

Current US cyber policy, concerning cyber intrusions, cyber defense, and cyber offense, can generally be divided between Joint Publication (JP) 3-12 and Presidential Policy Directive (PPD) 20. PPD 20 is more of a whole-of-government approach while JP 3-12 is focused on DoD. Combining both produces a general overview of current US cyber policy. A few unclassified terms will be discussed that are solely those within JP 3-12. No discussion of PPD 20 will occur to avoid potential security issues. I do not mean to suggest that these two documents are the only ones providing guidance on US cyber policy. That is certainly not the case. Rather, they focus more on the relevant issues discussed throughout this paper and provide a means to compare and contrast.

First the list of unclassified definitions will be identified. A discussion on whether those definitions are helpful or whether they hinder our understanding of cyber will follow. Finally there is a review on clear distinctions and some contradictions between the terms used and others previously discussed.

Countermeasures:

That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. In

cyberspace, countermeasures are intended to identify the source of a threat to the Department of Defense information networks and use nonintrusive techniques to stop or mitigate offensive activity in cyberspace. Countermeasures are a subset of defensive cyberspace operations response actions.⁵⁴

Cyberspace: “A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers.”⁵⁵

Cyberspace attack: “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.”⁵⁶

Cyberspace intelligence, surveillance, and reconnaissance: “Activities conducted in cyberspace that synchronize and integrate the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations.”⁵⁷

Cyberspace defense: “Actions normally created within Department of Defense cyberspace for securing, operating, and defending the Department of Defense

⁵⁴ 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).

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Id.*

information networks. Specific actions include protect, detect, characterize, counter, and mitigate.”⁵⁸

Cyberspace operations as: “The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”⁵⁹

Defensive cyberspace operations as: “Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net centric capabilities, and other designated systems.” It defines defensive cyberspace operations response action as, “Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems.”⁶⁰

Offensive cyberspace operations: “Cyberspace operations intended to project power by the application of force in or through cyberspace.”⁶¹

It is reasonable to suggest that the definitions above are not very helpful for practitioners. It is a fair assessment to suggest that some of them are detrimental to what the overarching policy should be. Some hinder one’s actions by defining too broadly, while others don’t go far enough. Moreover, there appear to be some internal inconsistencies as well.

For instance, let’s look at the definition of countermeasures again. Countermeasures seek to impair the operational effectiveness of enemy activity. At first blush that sounds suspiciously like disruption or manipulation, which would qualify as an attack too. The second part informs one that countermeasures use nonintrusive techniques to stop or mitigate offensive

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ JP 3-12, *supra* n. 54.

⁶¹ *Id.*

activity in cyberspace. Now it appears that the definition contradicts itself. On one hand, impairment seems to require some positive action against the enemy—impairment. Indeed, countermeasures go beyond the perimeter of the network. On the other hand, nonintrusive seems to indicate just the opposite. Unfortunately, nonintrusive is not further defined anywhere nor is impair. Finally, it has been noted that the countermeasures are a subset of defensive cyberspace operations response actions. Response actions again infer taking some action outside one's own networks, presumably nonintrusive—whatever that means. Without clear definitions of all pertinent terms, one is left with nothing more than a circular definition that confuses more than it clarifies.

Next consider cyber-attack and cyber effects together, because one is informed that the attack creates the effects. First, the definition states that an attack creates various effects and then several examples are provided. However, the definition does not tell one whether those listed effects are the only effects allowed or whether more exist. To remedy that, one needs an additional definition specifically defining those effects as manipulation, disruption, denial, degradation, or destruction. Ostensibly, this tells one that the list is all inclusive. It is also known that those items are incredibly broad, meaning that almost anything in cyber could constitute an attack by this definition. However, the second part articulates that the denial must either be hidden or manifest itself in the physical domain. So, despite the apparent broadness of the first part, the second part provides limitation. This limitation, further defining an attack, can be used to claim an action is *not* an attack. For instance, one can advise their commander that she may take an action that is not hidden or will not manifest itself in the physical domain and it is therefore

not an attack. Therefore, the approval authority for taking such an action may be a lot lower, allowing greater leeway. Now, perhaps one deliberately placed this “loophole” into the definition to allow for flexibility. Or, perhaps it was an oversight. In either case a “loophole” exists.

Lastly, consider offensive cyberspace operations. The definition is short so simply restated here: Cyberspace operations intended to project power by the application of force in or through cyberspace. Once again descriptive terms are not further defined. What, exactly does “project power” mean? What is an “application of force?” Even if force was defined it would not mean much outside of DoD channels. Use of force in international law is not completely settled even regarding kinetic strikes. Use of force in the cyber context is much more difficult to discern and certainly not settled. The US definition, however, seems to imply that any offensive action the US takes would necessarily include some use of force. So, the US makes it easy on their enemies by declaring what is being done is a use of force and difficult on itself for the very same reason. Moreover, there is an apparent disconnect between the definition of cyber-attack and offensive cyberspace operation. One would think that all attacks would be offensive and that all offensive cyberspace operations would be an attack. That, however, is not the case. An offensive cyberspace operation, that is either not hidden or does not manifest in the physical domain, would not be considered a cyber-attack. A cyber-attack that does not rise to the level of application of force would not be considered an offensive cyberspace operation.

Finally, compare some of the US policy definitions with those of the Tallinn manual and Professor Schmitt. Bear in mind that the rules developed by the Tallinn Group presumably reflects consensus as

to the applicable law currently governing cyber conflict. In other words, the rules do not reflect best practice or preferred policy, but the law as it currently stands.⁶² Note the fact that so many differences and discrepancies exist. If there is general agreement, at least from the Tallinn Group, on the law as it currently stands, then why do the views cited seem so divergent?

The US policy definition of cyber-attack is not clear or concise. It does, however, broadly include those things not normally associated with a traditional understanding of kinetic attack—manipulation, disruption, denial, degradation, or destruction. This is especially true if one tries to equate cyber-attack with kinetic attack. The Manual definition makes clear that a cyber-attack is an act of violence either against a person or object and that the focus is on the consequences and not the initiating act itself. Thus, the consequences of a cyber-attack must generate some violence to some person or thing. Notably, the Manual definition includes attacks on data if the consequences manifest as violence against either a person or thing. Moreover, the Manual also indicates that interference with functionality of a physical thing constitutes an attack, *if* restoration of the functionality requires replacement of physical components. This is perhaps where the two definitions diverge greatly. The US policy definition only requires manipulation or disruption, which presumably applies to data; in other words, if one limits the scope of an operation to affecting data that is a cyber-attack. Clearly this is not the case under the Manual definition because there is no violent consequence to either people or things.

Comparing the Schmitt analysis to both the Manual and US policy definition adds to the confusion. Professor Schmitt focuses on harm to people or things,

⁶² See The Tallinn Manual, *supra* n. 8.

which is in line with the Manual's focus on violent consequences. However, Professor Schmitt's criterion of severity is a sliding scale—the more severe the consequences the more likely it is a use of force. So it appears there are three separate and distinct definitions when use of a cyber capability would constitute an attack. US policy only requires manipulation or disruption of data. The Manual requires some physical manifestation of the consequences and Professor Schmitt requires some level of severity based on scale, scope, and duration. Thus, it is possible to arrive at separate and contradictory answers of whether an event constitutes an attack. Changing data to reflect something different to the observer than what is actually there would be an attack under US policy (manipulating data), but clearly would not under both the Manual and Schmitt analysis (no physical manifestation and no harm).

An additional discrepancy arises when considering the introduction of malware into an adversary system. The Manual suggests that, “the introduction of malware or production-level defects that are either time-delayed or activate on the occurrence of a particular event is an attack.”⁶³ Professor Schmitt, however, states that, “the introduction into a state's cyber systems of vulnerabilities that are capable of destructive activation at some later date would not constitute a threat of the use of force unless their presence is known to the target state and the originating state exploits them for some coercive purpose.”⁶⁴ US policy tends to align with the Manual, but for a different reason—insertion into an adversary system would likely constitute manipulation. Thus, it isn't difficult to imagine a scenario where insertion of malware or

⁶³ *Id.*

⁶⁴ Schmitt, *supra* n. 23.

vulnerabilities into an adversary's system would yield different answers depending on which definition one chooses to use.

Thus, current US cyber policy is based on terms that are not well defined and, the meaning of the terms is not consistent with the extant law as defined by the Tallinn Group. Some of the terms contradict others and some add layers of unnecessary constraint. Based on this context it is clear that US cyber policy is definitely not moving in the right direction. Instead of taking the lead and crafting a bold and workable cyber policy, the United States is instead immersed in wordsmithing in an apparent attempt to appear as if they are doing something while really accomplishing nothing substantive. This confusion over terms is even evident in the media, which compounds the problem, not only for us, but also for our allies and even our adversaries. For instance, a recent article in the Washington Post indicates that, "China on Wednesday again denied that it has used cyberattacks to steal U.S. military and business secrets, after new accusations were leveled in May 2013."⁶⁵ Of course China is not using *cyber-attacks* to steal information. They are engaging in cyber-espionage to steal. Undoubtedly there is a misunderstanding between cyber-attack, cyber-espionage and cyber-crime which only contributes to the problem and sows confusion.

VI. CONCLUSION

It is clear that our adversary's growing cyber capabilities are a real and continuing threat to the United States and indeed, the world. Without meaningful, useful concepts, definitions, rules, policy and law there will continue to be a struggle in a vain search for

⁶⁵ William Wan, *China Again Rejects Hacking Allegation*, WASH. POST, at 7, May 30, 2013.

consensus. Despite the attempts discussed in this article, the legal community has not achieved anything even approaching accord. One cannot be so naïve to believe that all nations will agree, but hopeful that if just a handful of influential nations could at least agree on some basic and fundamental concepts, definitions, rules, policy and law, then the rest may follow suit. It may be argued that the Tallinn Manual did just that. Presumably the NATO nations agreed with the rules delineated in the Manual—several key nations. However, as this article points out, those rules are not necessarily in line with either US policy or respected cyber intellectuals like Professor Schmitt and certainly not with other non-NATO nations like China or Russia.

If we continue down this path, issuing a hodge-podge of cyber concepts, definitions, rules, policy and law, an international law of cyber warfare will not develop. Instead, additional cyber intrusions are only getting worse and becoming more dangerous. Likewise, if the U.S. continues to hamper itself with convoluted and, sometimes contradictory concepts, definitions, rules, policy and law, it will fail to take the lead in this field and risk becoming irrelevant. Emerging and re-emerging powers may take charge. Countries like China or Russia or India or Brazil may prove to be the leaders in this area, and most assuredly they will not have the United States best interests at heart.

Without doubt the United States has the potential to lay the groundwork for a workable international legal structure. Professor Schmitt has already contributed significantly, but it is time to build on his early work in the field. The Tallinn Group has also contributed to global understanding as well. Likewise, their contributions must also be further developed. The United States and NATO can't simply dictate to the rest of the world. It has been hinted that

Russia plans to develop its own “anti-Tallinn” manual. If true, then a separate coalition will form around Russia. Two competing groups of cyber concepts, definitions, rules, policy and laws will then exist. At that point, it will almost be impossible for customary international cyber law to develop. Others with diverse views and opinions must be included, if we ever hope to develop the cyber arena in a meaningful way. At the very least, the definitions should align and be consistent with rules. The rules should align with the policy. The policy should align with broad concepts. Concepts should align with the law. Unless and until this is addressed, one cannot expect any consensus either.