The University of Cincinnati Intellectual Property and Computer Law Journal

Volume 6 | Issue 1 Article 5

November 2020

Information Crossroads: Intersection of Military and Civilian Interpretations of Cyber Attack and Defense

Carlos Plazas

INFORMATION CROSSROADS: INTERSECTION OF MILITARY AND CIVILIAN INTERPRETATIONS OF CYBER ATTACK AND DEFENSE

I. INTRODUCTION

When the general public hears news stories about "cyberwar" or "cyber-attacks," the image these terms conjure up is of mass destruction to a country's infrastructure. An example is the 2007 movie *Live Free or Die Hard* where a lone wolf actor is able to take control over American electrical infrastructure, media, and even a military jet in midair.[1] These kinds of "cyber-doom" scenarios, where a keystroke destroys the lives of average citizens, bring into question the government's investment of billions of taxpayer dollars on kinetic defense weapons.[2] But what exactly is the current status of "cyberwar," "cyber operations," and "cyber defense?"

The combat domain of the twenty-first century relies on the cyber domain and infrastructure of servers, individual computers, networks, and cyber defense operators.[3] Whether an American fifth-generation stealth fighter patrolling the Russian border with Alaska, or a lone wolf actor looking to cause the most damage possible with a single keystroke, cyber spans the full spectrum of combat. As a country's infrastructure, both civilian and military, becomes more reliant upon the benefits of cyber, it opens itself up to the vulnerability of attack by enemies abroad and at home. On 18 June 2018, the United States Department of Defense published Joint Publication 3-12, "Cyber Operations," to officially set forth how the United States will approach cyber defense and conduct operations against adversaries. According to the publication, ". . . the United States (U.S.) Department of Defense (DOD) is responsible for defending the US homeland and US

[1] Michael Fottrell, Mark Bomback & David Marconi, Live Free or Die Hard (2007).
[2] DOD Releases Fiscal Year 2020 Budget Proposal (2020), https://comptroller.defense.gov/portals/45/documents/defbudget/fy2020/fy2020_press_release.pdf.
[3] Department of Defense, Joint Publication 3-12: Cyber Operations I-1 (2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (last visited Dec. 1, 2020).

interests from attack, including attacks that may occur in cyberspace."[4] A Joint Publication is a regulatory document by the Department of Defense that establishes:

> fundamental principles that guide the employment of US military forces in coordinated and integrated action toward a common objective. It promotes a common perspective from which to plan, train, and conduct military operations. It represents what is taught, believed, and advocated as to what is right (i.e., what works best). It provides distilled insights and wisdom gained from employing the military instrument of national power in operations to achieve national objectives.[5]

The mission of Joint Publication 3-12, *Cyber Operations*, creates legal challenges for two primary reasons. First, cyber combat operations crosses sovereign boundaries, unlike any other kinetic weapon.[6] Second, cyber can operate domestically where the DOD has limited ability to respond to threats due to laws such as posse comitatus, which is the use of federal active-duty troops in a civilian law enforcement capacity.[7]

The DOD considers cyber an important enough domain to create a combatant command just to counter threats within the domain.[8] A combatant command is an organization that takes units from all branches of the US military and directs missions using these joint forces in furtherance of a national interest in that region or domain.[9] An example is the nuclear domain under the control of US Strategic Command (USSTRATCOM).[10] Traditionally, combatant commands are geographic, coordinating joint forces from all the branches of the US Military to conduct operations throughout the globe, the exceptions being USSTRATCOM and US Special

[4] Cyberspace Operations, Department of Defense, Joint Publication 3-12: Cyber Operations I-1 (2018), https://www.jcs.mil/portals/36/documents/doctrine/pubs/jp3_12.pdf.
[5] *Joint Doctrine Publications*, Joint Chiefs of Staff, https://www.jcs.mil/doctrine/joint-doctine-pubs/#:~:text=joint%20doctrine%20pubs-,joint%20doctrine%20publications,train%2c%20and%20conduct%20military%20operations (last visited Dec. 1, 2020).
[6] *Id.* at 1-2.
[7] Use of Army and Air Force as Posse Comitatus, 18 U.S. Code § 1385 (1878).
[8] *Joint Publication* 3-12, at I-2.
[9] *Combatant Commands*, United States Department of Defense Combatant Commands, https://www.defense.gov/our-story/combatant-commands/ (last visited Oct. 5, 2020).
[10] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, A-190 https://fas.org/irp/doddir/dod/jp1_02.pdf (last visited Oct. 5, 2020).

Operations Command (USSOCOM).[11] United States Cyber Command (USCYBERCOM) has existed in some form since the 1990s. In August 2017, President Trump, under the direction of then Secretary of Defense James Mattis, officially directed the creation of USCYBERCOM as a combatant command.[12] With an established combatant command, the US military believes that it can now properly coordinate its cyber forces from all of its branches and further the goal to "defend the US homeland and US interests from attack."[13]

II. BACKGROUND

Joint Publication 3-12 (3-12) covers a myriad of operational capabilities and procedures for the US to conduct cyber operations. However, 3-12 appears to lack legal support for these operations. Understandably, the Joint Chiefs of Staff signed 3-12 over two years ago, yet the words regarding the conduct of cyber operations state:

> DOD conducts Cyberspace Operations (CO) consistent with US domestic law, applicable international law, and relevant USG and DOD policies. The laws that regulate military actions in US territory also apply to cyberspace. Therefore, DOD cyberspace forces that operate outside the Department of Defense Information Network (DODIN), when properly authorized, are generally limited to operating in gray and red cyberspace only, unless they are issued different rules of engagement or conducting defense support of civil authorities (DSCA) under appropriate authority.[14]

The legal support section goes on to say: "[s]ince each CO mission has unique legal considerations, the applicable legal framework depends on the nature of the activities to be conducted."[15]

Nevertheless, the US government bases its ability to conduct Cyber Operations at home and abroad on the Constitution of the United States and Titles 6, 10, 18, 28, 32, 40, 44, and 50 of

[11] *Id*.
[12] *U.S. Cyber Command History*, U.S. Cyber Command, https://www.cybercom.mil/about/history, (last visited Nov. 25, 2020).
[13] *Cyberspace Operations*, Department of Defense, Joint Publication 3-12: Cyber Operations I-1 (2018) https://www.jcs.mil/portals/36/documents/doctrine/pubs/jp3_12.pdf (last visited Dec. 1, 2020).
[14] *Id*. at III-11.
[15] *Id*.

the United States Code (U.S.C.).[16] Essentially, the DOD and other agencies tasked with cybersecurity have the power to conduct cyber operations only through Titles 6, 10, 18, 32, and 50. Title 6 deals with domestic security, specifically the role that the Department of Homeland Security plays within the operation of the cyber domain regarding national security.[17] The Department of Homeland Security (DHS) is responsible for securing the nation's domestic cyberspace.[18] DHS and DOD rely upon each other to assist in the cyber defense of the nation. DHS relies upon the assistance of DOD cyber capabilities. On the other hand, the DOD relies on DHS because DOD is limited in its ability to conduct domestic operations, particularly dealing with law enforcement, barring national emergencies such as insurrections.[19] DHS's primary focus is in countering attacks, protecting non-DOD governmental networks, preventing intrusions, and establishing relations with the private sector in support of national cybersecurity.[20] Furthermore, DHS partners with the Department of Justice (DOJ), specifically the Federal Bureau of Investigation (FBI), to provide the information that the DOJ needs for conducting law enforcement investigations and the operations to ensure domestic cybersecurity.[21]

The federal government criminalized cybercrimes through 18 U.S.C. 1030, also known as the Computer Fraud and Abuse Act of 1986.[22] Currently, 18 U.S.C. 1030(a) states the definitions of cybercrimes:

> (1) Knowingly accessing a computer without authorization or exceeding authorization
>
> (2) Obtaining— (A) information contained in a financial record of a financial institution, or of a card issuer; (B) information from any department or agency of the United States; or (C) information from any protected computer;

[16] *Id.* at III-2.
[17] *Id.*
[18] *Id.*
[19] *Id* at III-10.
[20] *Id.*
[21] *Id* at III-11.
[22] Charles Doyle, *Cybercrime: A Sketch Of 18 U.S.C. 1030 And Related Federal Criminal Laws*, https://fas.org/sgp/crs/misc/rs20830.pdf (last visited Dec. 1, 2020).

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States;

(4) knowingly accessing a computer or network with intent to defraud;

(5) intentionally or recklessly cause damage to a network via installation of programs or through invasion of the network;

(6) inhibit the traffic of communication with the intent to defraud;

(7) extortion.[23]

Notably, there are no provisions for cyber terrorism or cyberattacks by foreign entities.[24] Such crimes fall under the law of war and DOD enforcement while the Computer Fraud and the Abuse Act of 1986 concern what DHS and DOJ are targeting at home.[25]

Further, DOD's role in cyber under Title 10 is to "man, train and equip US forces for military operations in cyberspace."[26] From the Secretary of Defense to individual soldiers assigned to a cyber specialty in their respective service, every member of the organization has a responsibility to ensure the mission of safeguarding US information networks.[27] Individuals within this cyberinfrastructure man their posts against would-be attackers, whether they be agents of near-peer competitors, such as China and Russia, or dispersed agents of terrorist networks, such as Daesh, conducting information warfare via social media against the US, its allies, and their interests.[28]

A notable responsibility under Joint Publication 3-12, USCYBERCOM is the sole authority to conduct cyber operations and actions that impact other sovereign nations.[29] As such,

[23] *Id*.
[24] *Id*.
[25] *Id*.
[26] *Joint Publication 3-12* at III-3.
[27] *Id*.
[28] *Id* at III-1.
[29] *Id* at III-5.

geographic combatant commands must relegate themselves to a supporting role for USCYBERCOM assets to conduct operations in the area.[30] The sharing of responsibilities between geographic combatant commands and USCYBERCOM poses issues with cybersecurity. First, unlike standard units, cyber units can see "digital weapons" and these "digital weapons" have the power to create kinetic effects that are often non-attributable.[31]Second, affected nations can take action against conventional forces in the combatant command's geographical theater in response to the cyber-attacks, even though the operation is most likely from the US mainland.[32] This means that an operation may start as a cyber-operation but transition into requiring physical forces and physical attacks in order to achieve mission objectives.

Why is all this law and military infrastructure necessary? In short, why is the cyber domain slowly taking a spotlight in a DOD budget in which large kinetic weapons like aircraft carriers, tanks, and stealth bombers normally dominate? The fear of having years of technological development and billions of dollars spent in achieving military superiority just to see it disappear via cyber-attack powers the DOD's cyberwar machine.[33] The DOD is afraid that even with all its spending on the latest kinetic weaponry it is still vulnerable to adversaries knocking out entire battlefleets with one keystroke, or shutting down the nation's power grid at the click of a mouse.[34] The United States' main concern in cyber is what Professor Sean Lawson describes as a "cyber Pearl Harbor" or a "cyber 9/11" in his book *Cybersecurity Discourse in the United States Cyber-Doom Rhetoric and Beyond*.[35] Professor Lawson and the DOD agree that cyber has the ability to

[30] *Id*.
[31] *Id*.
[32] *Id*.
[33] Sean Lawson, *Cybersecurity Discourse in the United States Cyber-Doom Rhetoric and Beyond*, 13 (Mark Lacy & Dan Prince Eds., 2020).
[34] *Id.* at 61.
[35] Sean Lawson, *Cybersecurity Discourse in the United States Cyber-Doom Rhetoric and Beyond*, 5 (Mark Lacy & Dan Prince Eds., 2020).

cause terrible damage to the United States. However, Lawson takes a different approach from the DOD and argues that the military's view on cyber is filled with "cyber-doom" rhetoric better suited for the movie theater than the Pentagon.[36] Criticism of the DOD's rhetoric stems from two primary camps. First, Lawson notes "the official narrative about who threatens what, how, and with what potential impact shifted over time, but it has done so with very little evidence provided to support the claims being made, thus raising the possibility that cyber threats are a mere fiction."[37] Second, other critics state that "think tanks, security firms, defense contractors, and government leaders who trumpet the problem of cyberattacks as self-interested ideologues who promote unrealistic portrayals of cyber threats for the financial benefit of an emerging 'cyber-industrial complex.'"[38]

III. CHALLENGES TO CONVENTIONAL COMBAT DOCTRINE IN THE CYBER REALM

A. SOVEREIGNTY

The US military maintains a vigilant presence over America's interest at home and abroad in a myriad of domains that are tangible and understandable to the American citizen such as air, land, and sea. Jane and Joe Doe can understand or at least visualize what they see on CNN when an aircraft enters foreign airspace, or a Special Forces team conducts an operation in another land. Both of those operations fall within the traditional interpretation of invading another nation's sovereignty. Yet, where does a nation's cyberinfrastructure stand regarding sovereignty? Does accessing the aircraft database of Ramstein Air Base from a terminal in Moscow constitute a violation of American sovereignty in the same way a Russian Spetsnaz unit physically on the ground taking pictures of the same information violates American sovereignty? In a 2009 *Air Force Law Review* article, Lieutenant Colonel Patrick W. Franzese writes, "[w]hile not every

[36] *Id.* at 17.
[37] *Id.*
[38] *Id.*

violation of sovereignty will necessarily result in the use of force, state practice evidences that a state can use force to defend its sovereignty."[39] Colonel Franzese collected data evidencing that in 2008, the Pentagon's network saw over six million cyber-attacks, most of which were by individuals trying to gain access to delicate information such as e-mails and Congressional computer access points.[40] Yet, the US is not the only target of cyberattacks. Sovereign nations around the world see attacks in the millions as well, often going past simple information gathering and causing harm on par with kinetic attacks.[41] Estonia, Georgia, and Kyrgyzstan were subjected to cyberattacks that significantly affected Internet service in their banking, governmental, and communication infrastructure in their countries.[42] In Estonia, observers identified that "[t]he main targets were: the Estonian presidency and its parliament; almost all of the country's government ministries; political parties; three of the country's six big news organizations; two of the biggest banks; and firms specializing in communications."[43] These targets are not random; they are critical to a nation's political, economic and communication infrastructure. By weakening these points, an adversary opens the way for additional attacks, whether digital or kinetic.

Sovereignty is a critical component of the cyber warfare equation because sovereignty is one of the highest held beliefs of the United Nations Charter.[44] The United Nations Charter establishes guiding principles and ideas that nations that wish to be part of the organization and work alongside other members must adhere to. Article 2(1) of the United Nations Charter states,

[39] Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist*, 64, Air Force Law Review (2009), https://www.afjag.af.mil/portals/77/documents/afd-091026-024.pdf.
[40] *Id.* at 2.
[41] Sean Lawson, *Cybersecurity Discourse in The United States Cyber-Doom Rhetoric and Beyond*, 25 (Mark Lacy & Dan Prince Eds., 2020).
[42] *Id.*
[43] *Id.*
[44] The Judge Advocate General's Legal Center and School International and Operational Law Department, Law of Armed Conflict Documentary Supplement, 1 (2013).

"[t]he Organization is based on the principle of the sovereign equality of all its Members."[45] To protect that valued sovereignty, the Charter explicitly requests in Article 2(4) that members refrain from the threat or use of force to resolve conflicts.[46] In the aforementioned attacks in Estonia and the US, do cyberattacks fall under this violation of the charter? Specifically, does it constitute use of force under Article 2(4), or an "armed attack" under Article 51 of the Charter allowing the victim of the attack to defend itself proportionally?[47] The answer is not as simple as traditional kinetic attacks. That is why scientists, legal scholars, and military generals are constantly trying to figure out where the line, if any, exists with cyberattacks. A disproportionate reaction to a cyberattack in the form of a kinetic response can create a domino effect where a temporary connection lag spike leads to flag-draped coffins carried out of cargo planes.

Critics of cyberattacks being on par with kinetic weapons argue that placing cyber weapons on par with their kinetic weapons involves flawed reasoning.[48] Thus, critics state that to place cyber weapons on equal footing with kinetic weapons is based on exaggerated cyber-doom capabilities.[49] Professors Jeffrey Biller and Michael Schmitt, in their 2019 legal analysis titled "Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare," concurred with Professor Thomas Rid's critical view of categorizing cyber-weapons on par with kinetic weapons.[50] The scholars fault the poor use of analogies by governmental organizations and conclude that "cyber capabilities cannot logically be categorized as weapons or means of cyber warfare."[51]

---

[45] *Id.*
[46] *Id.*
[47] "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 Measures Necessary to Maintain International Peace and Security." *Id.* at 7.
[48] *Lawson* at 140.
[49] *Id.*
[50] *Id.*
[51] *Id.*

Nonetheless, in 2009, the international community viewed the US and Israeli cyber units' use of the Stuxnet virus to disrupt Iranian nuclear production as the use of a weapon.[52] Conventional American and Israeli units trained and equipped for cyber warfare were eventually credited with the Stuxnet attack, and it achieved its mission to physically harm Iranian centrifuges that aided in the uranium enrichment process.[53] Hypothetically, an operation could carry the same results if a stealth bomber, or a Special Forces team conducts it; however, because it involved combat cyber capabilities, the ability to initially attribute the attack and determine its source and breach of sovereignty flirted along the delicate line of an "armed attack."[54] Stuxnet is an outlier in this regard. Most acts of cyber-sabotage to date have been non-violent, harming neither machines nor human beings.[55]

The polarized opinions regarding cyberattacks and their impacts are not limited to political scholars. There is an ongoing debate between entrenched camps of whether cyber-attacks are "armed attacks.[56] To attempt to bridge the divide between these ideas, the DOD places military cyber capabilities as an instrument that is dependent on the domains of air, land, sea, and space to conduct its operations.[57] Under this theory, DOD is able to appease those in the camp that believe that cyberattacks can only be "armed attacks" when accompanied by "real world" military acts by conducting these joint operations.[58] On the other hand, cyber's ability to permeate through all the domains also gives it the ability to harm through all domains, cause harm regardless of the original platform for an attack, and allow it to remain independent of conventional systems.[59] The one thing

[52] *Id.* at 60.
[53] *Id.* at 113.
[54] *Law of Armed Conflict Supplement* at 7.
[55] *Lawson* at 114.
[56] *Franzese* at 6.
[57] *Joint Publication 3-12* at 1-2.
[58] *Id.*
[59] *Franzese* at 6.

on which scholars can agree is that cyber has outpaced the current legal capabilities to understand and control the potential for cyber operations.[60]

Does the idea that States maintain sovereignty in the digital realm hold true as much as physical borders? One camp of theorists states that cyberspace should be free from government interference or sovereignty. [61]Such an argument suggests that cyberspace is immune from state sovereignty due to its interconnected and cross-border features.[62] On the other hand, Lt. Col. Franzese explores the idea that there are four reasons why States cannot separate sovereignty from the digital domain. First, although the digital domain does not have a physical embodiment or location, the servers and infrastructure supporting it are within a State's borders.[63] Second, States maintain financial control over corporations or organizations that maintain the support system for cyberspace.[64] Third, States have an interest in the content shared through cyberspace. From child pornography to communication of radical ideas such as Daesh's newsletter, a State has an interest in monitoring the data processed through cyberspace.[65] Fourth, cyberspace has slowly forced States to have a presence in the domain.[66] The current use of telecommuting resulting from the COVID-19 pandemic demonstrates this exact issue. The US military saw most, if not all, of their non-operational activities moved to the cyber domain.[67] For example, organizations held important meetings discussing everything from aircraft maintenance status to courts-martial over home networks with rushed protection methods in place.

---

[60] *Id.*
[61] *Id.* at 9.
[62] *Id.* at 12.
[63] *Id.*
[64] *Id.*
[65] *Id.* at 13.
[66] *Id.*
[67] Defense Department CIO and Joint Staff CIO Brief Reporters on DOD Communication Efforts Regarding COVID-19, https://www.defense.gov/newsroom/transcripts/transcript/article/2147989/defense-department-cio-and-joint-staff-cio-brief-reporters-on-dod-communication/#skip-target (last visited Dec. 1, 2020).

The difficulty of establishing cyber sovereignty is not lost on States. Just recently, during the twentieth century, States had to adapt to two new domains in air and space. Fears about the catastrophic consequences that could come from allowing the domains to be unregulated led the States to come together and identify where the line should be to protect their sovereignty and own survival.[68] Cyber should be no different. Even as there is criticism towards the cyber-doom rhetoric, States and their militaries must take cyber seriously and understand that cyberspace and a country's sovereignty are no longer independent. Much like how countries learned to live under the constant threat of a nuclear umbrella and mutually assured destruction, States must strike a delicate balance to maintain sovereignty while not destroying its ability to communicate and trade with other States.[69]

2. ARMED ATTACKS

Article 49(1) of Additional Protocol I to the Geneva Convention of 1949 defines an "armed attack" as "acts of violence against an adversary, whether in offense or defense."[70] Article 49(3) clarifies the application of attack to mean "air, land or sea warfare."[71] After its ratification and signature by over 173 States in 1977, Additional Protocol I (AP I) attempted to expand on the foundation of the Geneva Conventions from three decades prior in an effort to adapt to an ever-changing world.[72] However, the signatory States could not have predicted the development and revolution that the internet and cyber would bring to the world.[73] AP I's definition of where an armed attack applies remains a binding source of international law at least for those States that are

[68] For example, *see Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, https://www.unoosa.orgoosa, (last visited Dec. 1, 2020), *archived at* https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html.
[69] *Franzese* at 40.
[70] *Jag School Law of Armed Conflict Documentary Supplement* at 210.
[71] *Id.*
[72] *Id.* at 197.
[73] *Id.*

part of the convention.[74] For this reason, even with the advances in DOD's shift to cyber, the unknowns surrounding how to conduct such operations and respond to "cyberattacks" strictly within the cyber domain can scare off funding for more tangible purchases. However, near-peer competitors see this and contrast it with the US's dependence on cyber as a weakness in the US military's armor, because although the capabilities to respond to a cyberattack are there, the legal framework to guide such response is underdeveloped.[75]

Today, cyberspace is a realm that transcends international boundaries at the speed of light, and as Major Graham Todd notes in his *Air Force Law Review* article, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, "unfortunately, law, especially international law, failed to keep pace with the new applications of existing technologies."[76] Maj. Todd further states that "the legal world is being held back by its nuances of wordplay and definitions and allowing technology to dictate the tempo of the law and forcing the community try and fit square pegs in round holes when presented with suspected cyberattacks."[77] Maj. Todd identifies key differences between cyberattacks and traditional kinetic attacks. First, computer networks are a new target category, with computer network attacks capable of providing the same results as striking the traditional target with a kinetic weapon.[78] Second, an attack does not have to use kinetic force and can solely involve a command from one computer to the target system.[79] Third, the intended results are often not kinetic and could simply involve the manipulation of data or disruption of service.[80] Fourth, cyberspace threats are not constrained by

[74] *Id*.
[75]Graham H. Todd, Armed Attack in Cyberspace: Deterring Asymmetric Warfare with An Asymmetric Definition, 66 (2009).
[76] *Id*.
[77] *Id*.
[78] *Id*. at 68.
[79] *Id*.
[80] *Id*.

political boundaries or geography.[81] Fifth, cyberspace attacks can be completed literally at the speed of light.[82] Sixth, the results of some cyberspace attacks, whether intended or not, can be similar to those involving weapons of mass destruction and the cost of acquiring the equipment and expertise to conduct operations in cyberspace is de minimis in comparison to fielding conventional forces.[83] Finally, attributing the attack to the responsible party and determining whether the attack was intentional or accidental is extremely difficult. [84]

From these concepts, the most difficult to consolidate with traditional notions of attack is the last point of attribution.[85] When Maj. Todd wrote his article, the difficulty of attribution was present but not as pervasive as it is today. Today, terrorists and State-sponsored cyber forces can rely on cheap Virtual Private Networks, servers located in sovereign territory on the other side of the globe from their insertion point, and training that is becoming easily and economically available to more citizens each day. One just needs to look at the proliferation of smartphones and their capabilities since 2009. However, Maj. Todd's approach is still viable and resonates with firmly held legal beliefs such as negligence and assault.[86]

The analysis breaks down into two questions. First, was a cyber weapon used against the property or persons of a State?[87] Second, did a foreign state knowingly allow an entity under its legal control to use the cyber weapon?[88] Answering these questions raises the additional question of what exactly qualifies as a cyber weapon. The military tries to define "cyber weapon" by using the civilian definition in 18 U.S.C. 1030.[89] The statute defines a cyber weapon based on its ability

[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.* at 69.
[86] *Id.* at 93-94.
[87] *Id.*
[88] *Id.*
[89] *Id.* at 84.

to create cyber "damage" or an "impairment to the integrity of data, a program, a system or information."[90] Legal ambiguity in this definition appears to be the perfect counter to cyber's ability to be unpredictable and ever evolving. Maj. Todd's approach focuses on an offensive rather than a defensive tool.[91] His approach provides the victim of a cyber-attack a more lenient analysis, allowing the victim to retaliate with a stronger legal foundation. [92]Additionally, Maj. Todd's definition forces actors wishing to conduct cyberattacks to consider their use by placing them in a more vulnerable situation, leaving them with fewer options to criticize legally supported counter attacks.[93]

Major Todd's two-part cyber-attack definition, though helpful to States in defining a cyber-attack, nonetheless establishes a dangerous scenario where a cyber-attack can open the door for a kinetic counterattack.[94] Article 51 of the United Nations charter states that a nation still holds its right to self-defense.[95] Part of that right is a nation's ability to counterattack by whatever means it deem proportional to the attack.[96] Consider the Stuxnet attack on Iranian centrifuges: under the proposed definition, the US and Israel both *knowingly* allowed agents under their command to conduct an operation that impaired a system of information, causing physical damage.[97] Thus, Iran could theoretically consider this an armed attack and respond in kind by destroying a target with force proportional to that used, in which case a bomb may fit the bill. The cyber domain and the legal domain are two worlds muddled in their intricacies and ever-changing nature. However, as

[90] *Id.*
[91] *Id.*
[92] *Id.* at 86.
[93] *Id.* at 87.
[94] *Id.*
[95] *Jag School Law of Armed Conflict Documentary Supplement* at 1.
[96] AP I, Art. 51(5)(B): "[A]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" violates the principle of proportionality.
[97] *Lawson* at 113.

one evolves so must the other, and currently, the law is needing to play catch up with the cyber domain.

3. CURRENT DIRECTIVE ON APPLICATION OF CYBER-WEAPONS BY US MILITARY UNITS

Under the two directives of how the United States defines weapons, the use of "Cyber-weapon" as a term is currently incorrect.[98] Department of Defense Directive 3000.03E states that Non-Lethal Weapons "are explicitly designed and primarily employed to incapacitate personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property, facilities, materiel, and the environment."[99] The directive further goes on to say that it does not apply to "[i]nformation operations, cyber operations, or any other military capability not explicitly designed and primarily employed to incapacitate personnel or materiel immediately, while minimizing fatalities, permanent injury, and undesirable damage to property, facilities, materiel, and the environment, even though they may have these effects to some extent."[100] Under this definition and limitation, the use of cyber technologies to attack or defend does not equate to using a weapon. So, what does the military consider cyber if not a weapon?

Department of Defense Directive 3600.01, *Information Operations* states that cyber technology is a "capability."[101] DOD Directive 3600.01 describes the use of cyber technology as the "principal mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities (IRCs) in concert with other lines of

[98] The United States Department of Defense currently defines "weapons" as "non-lethal" under DOD Directive 3000.03e and all other weapons outside the definition of this directive as "lethal."
[99] DOD Directive 3000.03e: Use of Non-Lethal Weapons (April 25, 2013), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300003p.pdf?ver=2018-10-24-112944-467 (last visited Dec. 1, 2020).
[100] *Id*.
[101] DOD Directive 3600.01, Information Operations (May 2, 2013), https://fas.org/irp/doddir/dod/d3600_01.pdf (last visited Dec. 1, 2020).

operations to effect adversaries' or potential adversaries' decision making while protecting our own."[102] The directive defines what the purpose of cyber capabilities are, but the actual process of employing them is much more complex, even in comparison to ordering the drop of a conventional bomb. In 2016, Mr. James E. McGee, then legal advisor for United States Special Operations Command North, published an article titled *Liberating Cyber Offense.*[103] In his article, McGee describes the fundamental pathway that the US military takes when undertaking offensive operations using cyber capabilities.[104] In comparison to its kinetic brethren, cyber operations against a non-DOD network require a much higher level of approval, usually starting at the Secretary of Defense.[105]

Furthermore, McGee elaborates that in order to execute a cyber operation, a combatant or regional commander must have either an execute order (EXORD) already in place for conducting cyber operations against that specific target from the Secretary of Defense, or route the request through the review and approval process for cyber operations (RAPCO).[106] The RAPCO process is usually mired in bureaucracy and interagency procedures that stymie the operation and usually force the commander into opting for their kinetic assets which in turn end up risking actual lives and equipment.[107] Even if an EXORD is in place, and it is coupled with valid rules of engagement, there are still requirements for processing authorization for the cyber operations, getting actual target approval, and deconflicting the area of operation with other assets, which takes more time than conventional kinetic operations.[108]

---

[102] *Id*.
[103]Strategic Studies Quarterly, Liberating Cyber Offense (2016), https://www.jstor.org/stable/pdf/26271529.pdf?refreqid=excelsior%3aefc589906cdc19bbefe3c8332d2adcca (last visited Dec. 1, 2020).
[104] *Id*.
[105] *Id*.
[106] *Id*.
[107] *Id*.
[108] *Id*.

Additionally, Joint Publication 3-60, *Targeting*, Section A(2)(3) limits the use of cyber capabilities when targeting suspected enemies.[109] Specifically, the issue with targeting in the cyber domain is determining how far the damage can extend and in turn the harm it can cause to civilians as collateral damage.[110] McGee states:

> [I]n assessing incidental injury or damage, remote harms and lesser forms of harm—such as mere inconveniences or temporary losses—need not be considered in applying the proportionality rule. In the case of a power plant supporting civilian infrastructure, this can mean outlining effects against unintended targets, including hospitals, religious sites, orphanages, or other places that might be on a restricted or no-strike target list.[111]

Furthermore, the United States has taken Professor Harold Koh's concepts during his speech at the 2012 CYBERCOM legal conference and codified them as part of their law of war manual.[112] Professor Koh stated that cyber operations can be considered "armed attacks" under the UN Charter Article 2(4), which states, "[i]f the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force."[113] It is within this realm of contradiction that cyber capabilities dwell. Not quite a weapon, yet still in the realm of an armed attack; safer and theoretically easier to use, yet much more complicated to employ in combat.[114]

IV. CURRENT CHALLENGES TO CYBERSECURITY

A. CONSOLIDATING DOMESTIC INFORMATION SHARING AND HOMELAND DEFENSE

In the event of cyberattacks and actual cyber conflict, the true casualties will not be the cyber operators at the front lines of DOD's fight, but the individual American citizen. 2014 saw

[109] Joint Publication 3-06 Targeting I-1, https://www.justsecurity.org/wp-content/uploads/2015/06/joint_chiefs-joint_targeting_20130131.pdf (last visited Dec. 1, 2020).
[110] *McGee* at 49.
[111] *Id*.
[112] *Id*. at 50.
[113] *Id*.
[114] *Id*.

attacks against private civilian companies such as Target, eBay, Home Depot, J.P. Morgan Chase, Sony Pictures, and Anthem.[115] Further investigation into these attacks and additional breaches in 2015 divulged that over 43% of American corporations had been victims of cyberattacks in one form or another.[116] These companies are seeing sophisticated attacks on par with those that the military faces from its near-peer competitors.[117] The close ties between the private and public sectors in America make it so that an attack against a civilian company can have far-reaching effects on its defense industry. One such example is the 2015 data breach of defense contractor Lockheed-Martin.[118] Lockheed provides the United States military with hundreds of weapon systems, most notably for the 2015 hack are the F-22 and F-35 fighter jets.[119] These two aircraft are the only true fifth-generation stealth fighters in the world, and have capabilities that the US relies on to achieve air dominance over any adversary.[120] The 2015 hack saw information regarding these aircraft transferred to an unknown source, but most defense experts believe Chinese cyber operators or Chinese sponsored actors are responsible.[121] The primary evidence behind suspicion of Chinese interference is the resemblance of China's newest J-20 fighter to the F-22 and F-35 as well as the rapid improvements to J-20 from prior to the attack.[122]

---

[115] *2014: A Year of Mega Breaches*, Ponemon Institute, 1, (January 2015) available at http://www.ponemon.org/local/upload/file/2014%20the%20year%20of%20the%20mega%20breach%20final3.pdf (hereinafter "Ponemon Institute - 2014") (noting breaches at CHS Community Health Systems, Michael's Stores, Nieman Marcus, and Staples).

[116] *Is Your Company Ready for A Big Data Breach?*, Ponemon Institute, 1, (September 2014), available at http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf (Hereinafter "Ponemon Institute - Big Data Breach").

[117] Cybersecurity and Information Sharing: Legal Challenges and Solutions, 3, https://kmjas.jag.af.mil/moodle/pluginfile.php/32853/mod_resource/content/2/crs_-_cybersecurity_and_information_sharing_legal_challenges.pdf.

[118] Andrea Shalal, *Big U.S. Data Breaches Offer Treasure Trove for Hackers*, Reuters, https://www.reuters.com/article/us-cybersecurity-usa-china/big-u-s-data-breaches-offer-treasure-trove-for-hackers-iduskbn0om0n920150607 (last visited Oct. 5, 2020).

[119] Lockheed-Martin, https://www.lockheedmartin.com/en-us/products.html.

[120] *Id*.

[121] *Shalal* at 1.

[122] Jared Keller, *China's J-20 Stealth Fighter Is Built on Stolen F-35 Technology*, Yahoo! News (Oct. 18, 2019)., https://news.yahoo.com/chinas-j-20-stealth-fighter-010000654.html.

The interdependent nature of the federal government's defense infrastructure and the civilian corporate market makes the sharing of information and experiences between them regarding cyberattacks vital for mutual survival.[123] Current cyber information sharing has three lines of attack: dissemination of information from the federal government to private entities, dissemination among the private entities, and transfer of information from private entities to the federal government.[124] Although the methods share similarities, they have different challenges regarding legal frameworks and technical difficulties such as differing security clearances for forwarding information.[125]

1. SHARING INFORMATION FROM THE FEDERAL GOVERNMENT TO PRIVATE ENTITIES.

The federal government's infrastructure relating to the receipt and compiling of information regarding cyber-attacks and capabilities is robust and has the most legal clarity regarding roles and responsibilities.[126] The Department of Homeland Security's Office of Intelligence and Analysis (I&A), is an entity under Section 201 of the Homeland Security Act of 2002.[127] I&A is empowered to "access and receive" information and intelligence from agencies of government at all levels, state and federal, as well as from private actors.[128] I&A's principal mission is to "identify and assess […] terrorist threats to the homeland […] and actual and potential vulnerabilities to the homeland."[129] The second step of I&A's mission is to gather all of the information relating to the suspected attack, process it, and disseminate it to agencies of the federal

[123] Andrew Nolan, Cybersecurity and Information Sharing: Legal Challenges and Solutions, 3, https://kmjas.jag.af.mil/moodle/pluginfile.php/32853/mod_resource/content/2/crs_-_cybersecurity_and_information_sharing_legal_challenges.pdf.
[124] *Id.* at 5.
[125] *Id.* at 5-6.
[126] *Id.* at 7.
[127] *Id*.
[128] *Id*.
[129] *Id*.

and state governments as well as private entities.[130] A division of the National Plans and Programs directorate known as the National Cybersecurity and Communication Integration Center (NCCIC or Center) further supports I&A's role.[131] Where I&A's role is primarily to analyze and warn through information provided to it, NCCIC monitors traffic 24/7 to warn organizations, public and private, of threats to their infrastructure or about attacks going on against similar actors.[132] Congress codified NCCIC's functions to include: "serving as an 'interface' for the 'real-time' 'sharing of information related to cybersecurity risks, incidents, analysis, and warnings between Federal and non-Federal entities.'"[133]

As strong as I&A and NCCIC's security infrastructure appears, its power and that of DHS is not limitless. First, for the government to provide a private entity information regarding threats in the cyber domain, it must generally do so voluntarily as directed by 6 U.S.C. §143(1) and §121(d)(6)-(8).[134] Under current law, DHS is limited to this voluntary exchange of information between the private sector and the government, which raises the question of its effectiveness relying solely on voluntary reports.[135] The statute, 6 U.S.C. §121(d)(11) states that information in DHS's possession "is protected from unauthorized disclosure and handled and used only for the performance of official duties."[136] This means that unless the organization deems it an official duty to disclose the information to private parties, then it will remain with DHS, thus hindering the ability for the government and private entities to coordinate cyber-defense actions.

2. SHARING INFORMATION FROM PRIVATE ENTITIES TO THE FEDERAL GOVERNMENT

[130] *Id*.
[131] *Id*.
[132] *Id.* at 8.
[133] *Id*.
[134] *Id*.
[135] *Id.*
[136] *Id*.

Homeland cyber-defense is the US government's responsibility through DOD and DHS.[137] However, one cannot overlook the interconnected nature of the private entities with the government, and the impact that a cyber-attack on private organizations can have on the federal government. Currently, private organizations can transfer information relating to cyber-attacks and threats voluntarily to DHS.[138] In theory, this process is good, but legally there are underlying private concerns for organizations relating to dealing with the government.[139] First, when a company transfers information from its database to one that is controlled by the federal government, the information is accessible through a Freedom of Information Act request, which may divulge information that the company may not want competitors, investors, or the media to see.[140]

Additionally, by sharing information with the government, private organizations risk the security of their intellectual property. After sharing cyber-intelligence with the government, there is a presumption that a company waives its intellectual property rights associated with the information due to the voluntary disclosure.[141] There is a difficult balance in this realm between the law of trade secrets, which aims to secure a company's place in the hierarchy through the collection of information and technological development to achieve a competitive advantage, and a company's desire to maintain security in the organization.[142] In other words, by trying to protect themselves from cyber-attacks, by sharing cyber-information with the government, private companies are risking key tenets of intellectual property information protection.[143] The disclosure demonstrates that the company (1) has destroyed the independent value because the information

[137] *Joint Publication 3-12* at I-1.
[138] *Nolan* at 7.
[139] *Id.* at 34.
[140] *Id.* at 35.
[141] *Id*.
[142] *Id.* at 36.
[143] *Id*.

is now generally known and (2) is no longer the subject of the company's efforts to maintain the information's secrecy.[144]

3. RECONCILING CONCERNS AND DIFFICULTIES THROUGH FEDERAL LAW

In his 2015 article, "*Cybersecurity and Information Sharing: Legal Challenges and Solutions*," Mr. Andrew Nolan proposes a solution to the sharing of cybersecurity information between entities by breaking down the bureaucracy of the government's approach to cyber-security into three distinct areas.[145] He proposes creating a stronger legislative body of law aside from the Homeland Security Act and tackling the cyber-information by identifying what type of information the government should receive, who can receive the information, and proper use for the information.[146] The issue with the proposals is finding the balance between information gathering, government involvement, and government use.[147] If the scope of the legislation is too broad, the amount of information may be too much for the government to process, and the government may overlook actual threats to the nation's cyber-infrastructure.[148] On the other hand, if the scope is too narrow, then there may be insufficient evidence to pinpoint the attack's target and method of harm.[149] The difficulty in identifying the correct intercept between the private and public sectors is most apparent in the realm of liability.[150] A company may be acting in its and the nation's best interests by providing cyber-information to the government. However, if DHS, and perhaps even DOD, find evidence of federal and state law violations by the company when reviewing the information, questions may arise about who is at fault and why a private entity is

[144] *Id*.
[145] *Id.* at 44.
[146] *Id.* at 45.
[147] *Id.*
[148] *Id*.
[149] *Id*.
[150] *Id.* at 48.

facing charges for doing their part in homeland defense.[151] The answers to such questions were not clear in 2015 when Nolan wrote the article. However, Nolan best describes the interplay by stating: "without some assurances with regard to liability, the potential exists that a private entity may simply refuse to participate in information sharing, reasoning that any amorphous benefits that could be realized would simply not cover the cost of liability."[152]

B. FUTURE OF CYBERSECURITY LEGISLATION

Senior Specialist in Science and Technology, Eric Fischer, wrote his 2013 article, "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions" in hopes of identifying how to reconcile the amorphous, and dispersed nature of cybersecurity with a more centralized and focused approach of federal legislation.[153] Fischer studied ten broad areas Congress explored to improve the cybersecurity infrastructure of the government.[154] Fischer states four areas of focus out of his ten that demonstrate the intersection of private and public interest: "national strategy and the role of government, protection of critical infrastructure (including the electricity grid and the chemical industry), cross-sector coordination, and international efforts."[155] As such, their regulatory framework is in the direst need of clarification to bring forth the most effective and legal cyber protection enterprise.[156] Fischer specifically recommended the legislature tackle these issues by amending already existing regulations to the cyber domain.[157]

1. NATIONAL STRATEGY AND ROLE OF GOVERNMENT AND PROTECTION OF CRITICAL INFRASTRUCTURE

[151] *Id.* at 48.
[152] *Id.* at 49.
[153]Eric A. Fischer, Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions (2013), https://kmjas.jag.af.mil/moodle/pluginfile.php/34396/mod_page/content/32/flrs2013.pdf (last visited Dec. 1, 2020).
[154] *Id.* at 1.
[155] *Id*.
[156] *Id*.
[157] *Id.* at 20.

The thought that a law from the mid-nineteenth century influences the government's role in cybersecurity may be unfathomable. The underlying principles of some of these statutes still have the effect of restricting the capabilities of the government to properly handle cybersecurity issues, in short proving the government with nineteenth-century tools to handle twenty-first-century problems.[158] The main legislation regarding military law enforcement of civilian issues is the Posse Comitatus Act of 1879 (18 U.S.C. § 1385), which "restricts the use of military forces in civilian law enforcement within the United States, unless it is within a federal government facility."[159] Violations of the Act involve the direct use of military forces; additionally, the use of military force is "pervasive" in the civilian law enforcement operation.[160]Advocates for revision of the Act state that the Act's language in turn binds the hands of DOD in implementing its technology and intelligence on foreign actors in support of civilian law enforcement.[161] Furthermore, as cyber-attacks have the ability to permeate between interconnected networks, what may start as a criminal attack on civilian organizations may turn into an issue of national defense.[162] A strict interpretation of the Act would lead to two separate, uncoordinated investigations that may hinder the abilities of civilian and military cyber-defense.[163] The spirit of the Act is to prevent the image of active-duty military troops in civilian cities.[164] As such, the proposed amendments are mostly aimed at allowing remote assistance through clarifying when the U.S. military can operate domestically regarding cyber threats to the information infrastructure, most of which is privately owned.[165]

[158] *Id*.
[159] 18 U.S.C. § 1385.
[160] *Fischer* at 21.
[161] *Id*.
[162] *Id.* at 22.
[163] *Id*.
[164] *Id*.
[165] *Id*.

In addition, the National Security Act of 1947 (50 U.S.C. 401) created the National Security Council, the Central Intelligence Agency, and the procedures for access to classified information.[166] The reason the Act is important is that most cybersecurity and cyber-defense issues that involve the federal government require a security clearance.[167] Security clearances are a significant barrier to improving cybersecurity sharing of information regarding cyber-attacks.[168] In the past, Congress has attempted to pass legislation facilitating the transfer of information between civilian and military cyber-security enterprises.[169] As private firms augment the military in this regard, it would make sense to amend the Act to allow for more efficient communications, strengthening overall cyber-defense.[170]

2. CROSS-SECTOR COORDINATION AND INTERNATIONAL EFFORTS

Congress has also looked outside the federal government and its abilities to augment national cyber-defense with private industry and international partners.[171] First, Congress has looked at possible updates to the Freedom of Information Act (FOIA, 5 U.S.C. § 552).[172] FOIA allows private individuals and organizations to request information within records of the federal government, aside from a few exceptions.[173] Three key exceptions deal with cybersecurity information: information classified for national defense or foreign policy, data specifically exempt from disclosure by a statute, and trade secrets.[174] As such, FOIA's essential purpose of assisting

[166] *Id.* at 27.
[167] Exec. Order No. 13467 (July 2, 2008), Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information: Section 1.3(g) states that "'covered individual' means a person who performs work for or on behalf of the executive branch, or who seeks to perform work for or on behalf of the executive branch." As such, individuals employed either by the military or executive agencies such as the department of justice (FBI) require a security clearance.
[168] *Fischer* at 27.
[169] *Id*.
[170] *Id*.
[171] *Id*.
[172] *Id.* at 29.
[173] *Id*.
[174] *Id*.

private individuals is its own downfall in trying to aid in coordination between civilian companies and the government.[175] As the government attempts to encourage the private sector to share sensitive cybersecurity information with the federal government, the private sector becomes increasingly concerned that their own records may become government records subject to FOIA requests.[176] A possible solution would be to not archive the information and simply treat it as single-use by deleting the information as soon as the cyber threat has been handled, or to mark it as classified, further supporting the need to amend the National Security Act.

American national cybersecurity is becoming more dependent upon international partnerships as the internet becomes increasingly global.[177] For example, the State Department Basic Authorities Act of 1956 (22 U.S.C. § 2651a), an act originally intended for counterterrorism and HIV/AIDS response coordination, contains language that under certain interpretations provides for cybersecurity positions within the Department of State.[178]Additionally, the Communications Act of 1934 (47 U.S.C. §151) grants power to the Federal Communications Commission (FCC) to regulate domestic and international commercial communications.[179] Fischer identifies possible updates to the Act in order to respond to the current information enterprise by saying, "the act should be revised to give the FCC more of a role in cybersecurity, especially given the growing merging of information and communications technology (ICT) and their increasing importance in the U.S. economy. In fact, a number of other countries have more unified governance of ICT than the United States."[180]

V. CONCLUSION

[175] *Id*.
[176] *Id*.
[177] *Id.* at 28.
[178] *Id*.
[179] *Id.* at 26.
[180] *Id*.

The more one digs into cybersecurity and cyber-defense, the more questions and ambiguity arise. The Department of Defense principally heads modern American cybersecurity operations to ward off potential threats to the nation.[181] The law regarding the use of cyber capabilities is a mixture of attempting to adapt kinetic warfare treaties and doom-theory ideas hoping to prevent loss of life caused by keystrokes.[182] In its application of cyber capabilities, the defense apparatus of the United States as well as our near peer rivals and competitors, is ahead in some respects but still relies on the civilian sector for support.[183] As such, legislation is trying to catch up to both camps, the civil defense and military national defense, to properly address the needs of the nation, both in security and their own private interest.[184] The Department of Defense says it best in Joint Publication 3-12: "Cyberspace, while part of the information environment, is dependent on the air, land, maritime, and space physical domains," but the corollary is likewise applicable: "air, land, sea and space are their own environments (whether they be civilian or military) but they are all dependent on cyber."[185]

[181] *Joint Publication 3-12* at I-1.
[182] *Lawson* at 2-3.
[183] *Doyle* at 1.
[184] *Fischer* at 4-5.
[185] *Joint Publication 3-12* at I-1.