National Security Law Journal

Excerpt from Vol. 4, Issue 1 (Fall/Winter 2015)

Cite as:

Molly Picard, Comment, *Cyberspace: The 21st-Century Battlefield Exposing Soldiers, Sailors, Airmen, and Marines to Potential Civil Liabilities*, 4 NAT'L SEC. L.J. 126 (2015).

ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, homeland security, and national defense.

We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

COMMENT

CYBERSPACE:
THE 21ST-CENTURY BATTLEFIELD EXPOSING SOLDIERS, SAILORS, AIRMEN, AND MARINES TO POTENTIAL CIVIL LIABILITIES

Molly Picard*

In 2015, more than 25 million Americans were affected by the Office of Personnel Management data breaches. These incidents demonstrate a new form of warfare in an emerging battlefield that the United States must defend against: cyber warfare in cyberspace. And as part of that defense in the cyberspace battlefield, the U.S. Department of Defense and U.S. military are active members.

Among the various statutes governing the conduct of U.S. entities in cyberspace is the Computer Fraud and Abuse Act. Originally enacted in 1984 as part of the Comprehensive Crime Control Act, the Computer Fraud and Abuse Act was the U.S. Government's first attempt to legislate in the cyber security field and was designed to combat computer crimes, to secure government information, government computers, and government networks. Now, more than 30 years and several amendments later, the Computer Fraud and Abuse Act has expanded to cover nearly every computer in the world and makes illegal many activities that the average computer user undertakes on a regular basis.

* George Mason University School of Law, Juris Doctor Candidate, December 2016; James Madison University, B.S. in Intelligence Analysis, magnum cum laude, 2013. I would like to thank CAPT Patrick Gibbons, U.S. Navy, Judge Advocate General Corps, for inspiring the topic of my comment, as well as CDR Paul Walker, U.S. Navy, Judge Advocate General Corps, for answering my questions and reviewing my comment. I would like to thank my notes editor, Lauren Doney, for providing insightful and timely feedback throughout the entire process of writing my comment. And, finally, I would like to thank my family and friends for their constant support.

Although the Computer Fraud and Abuse Act contains an exception for the lawful activities of law enforcement and U.S. intelligence agencies, the U.S. military is not a party to the exception. As the cyber security threat to the United States increases and the U.S. military's role in cyberspace evolves, the Computer Fraud and Abuse Act may expose members of the U.S. military active in U.S. cyber defense to personal, civil liabilities for acting in accordance with their orders. To avoid this unfortunate consequence, the Computer Fraud and Abuse Act must be revised and the U.S. military's role in cyber space must be better defined.

INTRODUCTION

> *At one minute out, the Black Hawk crew chief slid the door open. I could just make him out—his night vision goggles covering his eyes—holding up one finger. I glanced around and saw my SEAL teammates calmly passing the sign throughout the helicopter…*
>
> *An hour and a half before, we'd boarded our two MH-60 Black Hawks and lifted off into a moonless night. It was only a short flight from our base in Jalabad, Afghanistan, to the border with Pakistan, and from there another hour to the target we had been studying on satellite images for weeks…*
>
> *Crowded into the cabin around me and in the second helicopter were twenty-three of my teammates from the Naval Special Warfare Development Group… "Five minutes ago, the whole cabin had come alive. We pulled on our helmets and checked our radios and then made one final check of our weapons. I was wearing sixty pounds of gear, each gram meticulously chosen for a specific purpose, my load refined and calibrated over a dozen years and hundreds of similar missions…*
>
> *Now, as the Black Hawk flew to our target, I thought back over the last ten years… A decade after [the 9/11 attacks] and with eight years of chasing and killing al Qaeda's leaders, we were minutes away from fast-roping into Bin Laden's compound.*[1]

A personal account such as this is what most people expect when they think of Soldiers, Sailors, Airmen, and Marines—members of the United States' (U.S.) armed forces—fighting the nation's enemies and providing for the nation's security. In the 21st-century, however, the nation's enemies have evolved. While members of the armed forces still engage in traditional combat described above, a new battlefield is emerging where engaging the enemy involves new weaponry—a mouse, a keyboard, and a computer—and in a new arena—cyberspace.[2] With this new

[1] MARK OWEN WITH KEVIN MAURER, NO EASY DAY: THE FIRST HAND ACCOUNT OF THE MISSION THAT KILLED OSAMA BIN LADEN 1-4 (2012).

[2] Cyberspace is defined by the Department of Defense as "[A] global domain within the information environment consisting of the interdependent networks of

battlefield come new challenges to the legal framework governing the conduct of the members of the U.S. armed forces in securing the nation from enemies, both foreign and domestic.

In fulfilling their mission to "support and defend the Constitution of the United States of America," the U.S. military regularly ask their members to conduct activities that would otherwise violate federal statutes and criminal codes.[3] For example, "[i]n wartime the role of the military includes the legalized killing (as opposed to murder) of the enemy . . . ."[4] The Computer Fraud and Abuse Act (CFAA) has become an over-encompassing statute that now covers nearly every computer in the world.[5] Without creating an exception to the CFAA, members of the military could personally face civil liabilities for conducting operations in accordance with military orders. The Department of Defense's (DOD) presence in cyberspace has increased in the past few years. This change became apparent with the recent establishment of United States Cyber Command (CYBERCOM), an entity designed to lead the military in the cyber security field.[6] Given the increasing cyber threat that puts

---

information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." JOINT CHIEFS OF STAFF, JOINT PUB. 3-12(R): CYBERSPACE OPERATIONS, at GL-4 (Feb. 5, 2013) [hereinafter JP 3-12], http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[3] *See* Enlistment Oath: who may administer, 10 U.S.C. § 502 (2006). *See also* U.S. CONST. art. 1, § 8, cl. 11 (Congress holds the power "[t]o declare War, grant Letter of Marque and Reprisal, and make Rules concerning Captures on Land and Water . . ."); U.S. CONST. art. 2, §1, cl. 1 ("The executive Power shall be vested in a President of the United States of America"); U.S. CONST. art. 2, § 2, cl. 1 ("The President shall be Commander in Chief of the Army and Navy of the United States…"); U.N. Charter, art. 51 (recognizing every nation's right to self-defense). *See e.g.*, MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 21-25 (Basic Books 5th ed. 2015) (providing reasons as to when certain conflicts are determined to be just or unjust).

[4] STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 404 (Aspen Casebook Series, Wolters Kluwer, 5th ed. 2011) (quoting Memorandum of Law: Executive Order 12333 and Assassination, by W. Hays Parks, *reprinted in* U.S. DEP'T OF ARMY, PAM. 27-50-204, THE ARMY LAWYER para. c. (Dec. 1989)).

[5] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010).

[6] *U.S. Cyber Command*, U.S. STRATEGIC COMMAND, https://www.stratcom.mil/factsheets/2/Cyber_Command/ (last updated Mar. 2015).

industry, intellectual property, and national security at risk, it is important to define the military's role in this emerging cyberspace battlefield to avoid imposing civil liabilities on members of the armed forces who are merely following orders and upholding their mission to support and defend the United States.

The CFAA currently exempts law enforcement and intelligence agencies, enabling them to conduct activities that would otherwise violate the CFAA.[7] Those members of the military assigned to and operating under the authority of an intelligence agency, such as the Defense Intelligence Agency, National Security Agency, or Central Intelligence Agency, are privy to this exemption.[8] In contrast, however, members of the armed forces operating solely under military authority have no such protection. Instead, the military is required to justify each independent cyber operation.[9] Continuing to protect members of the armed forces from civil liabilities, which is done regularly when the United States sends its troops into battle, is essential to the success of CYBERCOM and for regulating the new cyberspace battlefield.

The current statutory framework surrounding cyber security law potentially exposes military personnel operating solely under military authority to civil liabilities for violating domestic laws, primarily the CFAA. To curtail the potential civil liabilities, the CFAA requires an amendment to create an exception for military cyber activities, similar to the exception granted to law enforcement operations and intelligences agencies. Additionally, the CFAA demands a reversion to its original intent of protecting government computer systems and sensitive government information. Finally, because of the indefiniteness surrounding cyberspace, the emerging 21st-century battlefield warrants a clear statutory framework outlining the military's and DOD's roles in cyber security.

---

[7] Computer Fraud Abuse Act, 18 U.S.C. § 1030(f) (2008).

[8] *See id.* (§ 1030(f) specifically grants "an intelligence agency of the United States" the ability to conduct "any lawfully authorized . . . intelligence activity.").

[9] *See*, *e.g.*, Richard Weitz, *Defense Department Prepares for Cyberwar: The Current State of Play*, SECOND LINE OF DEF. (Apr. 12, 2011), http://www.sldinfo.com/ defense-department-prepares-for-cyberwar/.

Section I of this comment introduces the current operating environment (OE) by examining 21st-century national security threats to the United States. In explaining the OE, this comment then defines cyber security and explains the various types of cyberspace activities and cyber security threats. It discusses the military's emerging role in cyberspace and the activities the military conducts in cyberspace.

Section II describes the legal implications of cyber security and cyber operations by examining the international and domestic laws that establish the legal framework governing offensive and defensive cyber security missions.

Section III explains how current U.S. domestic law may expose members of the military to civil liabilities for conducting operations in accordance with military orders because of the overly broad scope of the CFAA and the lack of a clearly defined OE for the military in cyberspace. This analysis begins by examining *Nardone v. United States*. In *Nardone*, the Supreme Court held that a generally applicable statute that did not exempt the government or government agents from liability under the Federal Communications Act of 1934 prohibited the Bureau of Investigations from collecting data that the Federal Communications Act protected.[10] Using this case as well as traditional modes of statutory interpretation, this comment argues that the CFAA does not create an exception for military cyber activities, and because of this, members of the armed forces could potentially face civil liabilities for the military's cyber security activities. Although the CFAA creates exceptions for intelligence agencies and law enforcement operations, similar military actions are not included in the statute's exemption.

Finally, this comment suggests, in Section IV, that given the growing concern over cyber security and the ever-increasing threat to national security from cyberspace, the CFAA should be amended to create an exception for military operations. Additionally, the CFAA should be reverted to its original intent of protecting government computer systems and sensitive government

[10] Nardone v. United States, 302 U.S. 379, 384-85 (1937).

information. Finally, given the present cyber threat and growing cyber field, the military requires a general legislative framework to define the military's role in cyber operations so that the military can proactively address this new, emerging threat.

I. BACKGROUND: SETTING THE SCENE

A. The World Today

According to the May 2010, National Security Strategy (NSS), "[a]t the dawn of the 21st century, the United States of America faces a broad and complex array of challenges to [U.S.] national security."[11] In explaining the evolution of the world environment since the end of the Cold War, the NSS enumerates and advances persistent problems the United States has faced.[12] Specifically,

> [t]he circle of peaceful democracies has expanded; the specter of nuclear war has lifted; major powers are at peace; the global economy has grown; commerce has stitched the fate of nations together; and more individuals can determine their own destiny. Yet these advances have been accompanied by persistent problems. Wars over ideology have given way to wars over religious, ethnic, and tribal identity; nuclear dangers have proliferated; inequality and economic instability have intensified; damage to our environment, food insecurity, and dangers to public health are increasingly shared; and the same tools that empower individuals to build enable them to destroy.[13]

Following the terrorist attacks of September 11, 2001, the United States was forced to recognize the global threat of violent extremist groups that continue to present a risk to U.S. national

---

[11] Press Release, The White House, Office of the Press Secretary, Fact Sheet: Nat'l Sec. Strategy 1 (May 2010) [hereinafter Nat'l Sec. Strategy Fact Sheet], http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
[12] *Id.*
[13] *Id.*

security.[14] Moreover, "[g]lobal power is becoming more diffuse," with new alliances emerging and power shifting throughout other regions of the world.[15]

The Worldwide Threat Assessment of the U.S. Intelligence Community lists counterintelligence, proliferation of weapons of mass destruction, terrorism, transnational organized crime, counterspace, and mass atrocities as major concerns to U.S. national security.[16] Competition over scarce resources also presents grave risks of instability.[17] Additionally, advances in technology accompanied by an increasing reliance on such technology continue to challenge the defense of the United States.[18] With this technology problem, there comes an increasing cyber security threat, which has become one of the gravest concerns to U.S. national security.[19]

B. Cyberspace: Understanding the 21st-Century Battlefield

As Congressman Jim Sensenbrenner explains, "[t]he United States has been the subject of the most coordinated and sustained computer attacks the world has ever seen."[20] Both the U.S. Government (USG) and America's private sector are regularly victims of "military style hacks."[21] Responding to such attacks requires more than international diplomacy as they present serious

---

[14] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, THE NATIONAL INTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA 4 (2014) [hereinafter NATIONAL INTELLIGENCE STRATEGY], http://www.dni.gov/files/documents/2014_ NIS.pdf.
[15] *Id*.
[16] *Annual Open Hearing on Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 10 (2013) (statement for the record of James R. Clapper, Director of National Intelligence) [hereinafter *Worldwide Threat Assessment*], http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pd.
[17] NATIONAL INTELLIGENCE STRATEGY, *supra* note 14, at 4.
[18] *Id*.
[19] *Worldwide Threat Assessment*, *supra* note 16, at 12.
[20] *Investigating and Prosecuting 21st Century Cyber Threats*: *Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 1 (2013) (statement of Rep. F. James Sensenbrenner, Chairman, H. Subcomm. on Crime, Terrorism, Homeland Security and Investigations) [hereinafter Statement of Senator Sensenbrenner].
[21] *Id*. at 2.

challenges to America's national security as well as its businesses and economy.[22] Given the increasing global reliance on computer related technologies, as evident by the more than two billion internet users in 2010, cyber security concerns will continue to increase in number and severity.[23]

The first step to understanding cyber security is understanding the emerging battlefield that is becoming a part of everyday life—that is, understanding the meaning of "cyberspace." The USG defines cyberspace "as the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[24] Because of the world's increasing reliance on cyber technologies, "[c]yberspace [has become]…a key sector of the global economy [and] has become an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks that drive [economies]." [25] Moreover, the United States' key infrastructure industries—"including [the] energy [sector], banking and finance, transportation, communication, and the Defense Industrial Base"—are becoming increasingly reliant on cyber technologies.[26] This increases the risks to the United States as the systems that these industries rely on "may be vulnerable to disruption or exploitation" by enemies of the United States.[27] Unfortunately, while the United States increases its reliance

[22] *Id.*
[23] DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1 (2011), [hereinafter DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE], http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DOD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.
[24] Andru E. Wall, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*, 3 HARV. NAT'L SEC. J. 85, 117 (2011-2012) (quoting JOINT PUB. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 95 (2011)).
[25] DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 23, at 1.
[26] *Id.*
[27] *Id.*

on cyberspace, cyber defense and security have not grown at the same rate.[28]

The concept behind "cyberspace" and its continued operation today, was to increase connectivity and the ability to share information quickly. Advances in cyber technology have made it so that "[s]mall-scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to [the United States'] national security."[29] This potentially means that an individual or a handful of individuals working together can cause huge impacts with a small amount of resources. While the United States successfully defends against a multitude of cyberattacks and intrusions on a daily basis, the cyber field and creative enemies and criminals are designing new technologies at an alarming rate that may outpace U.S. defensive capabilities.[30]

C. Cyber Warfare: Understanding Cyber Attacks

Cyber attacks come in a variety of shapes and forms. Possible scenarios range from "a virus that scrambles financial records or incapacitates the stock market, to a false message that causes a nuclear reactor to shut off or a dam to open, to a blackout of the air traffic control system that results in airplane crashes."[31] All of these scenarios have the potential to cause "severe and widespread economic or physical damage."[32] The resulting damage lies on a spectrum from "merely annoying to destructive," and may aim to "facilitate future criminal, espionage or military activities."[33] Cyber operations may be designed merely to gather information or gain access to a system, or they "can go much further…adversely affecting the functionality of a computer system or even destroying a system

---

[28] *Id*.
[29] *Id*. at 2.
[30] *Id*.
[31] Oona A. Hathaway et al., *The Law of Cyber-Attack* 100 CAL. L. REV. 817, 822-23 (2012) (internal citations omitted).
[32] *Id.* at 823.
[33] Gary D. Brown & Owen W. Tullos, *On the Spectrum of Cyberspace Operations*, SMALL WARS JOURNAL (Dec. 11 2012), http://smallwarsjournal.com/print/13595.

or component."[34] Some broad categories of attacks include access operations, disruption operations, and cyber attacks.[35]

"Access operations enable other cyber activities by providing entry to an adversary computer system," which is necessary before any other cyber activity, such as information gathering or attacks, can take place.[36] An attacker may gain access to computers or information systems "by installing software programs, defeating security measures, injecting malicious code or other exploitation of a system's vulnerabilities," and include actions to maintain or regain access previously obtained.[37]

In 2008, an access attack occurred when Operation Buckshot Yankee used universal serial buses (USB) programmed with a virus to gain access to sensitive information.[38] When a user inserted the USB into a port on a classified DOD network computer connected to the Internet, the actors were able to gain access to information on the networks being used by the computer. "Operations like this can be designed to facilitate espionage or the destruction of a system, or anything in between."[39]

A second example, Operation Aurora "gained and maintained access into Google's network for many months," which gave the actors, "a treasure trove of information [on] companies that were doing business with Google."[40] The attack permitted access to a large quantity of information, and was believed to have originated in China for purposes of industrial espionage.[41]

And in 2009, operation GhostNet was able to "turn on an infected computer's microphone and video recording systems [ ] to capture new information, or [ ] to exfiltrate data from the computer

---

[34] *Id.*
[35] The following examples were excerpted from *On the Spectrum of Cyberspace Operations*, by Gary D. Brown & Owen W. Tullos. *See id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Brown & Tullos, *supra* note 33.
[40] *Id.*
[41] *Id.*

system."[42] Believed to have originated in China, the attack gained unauthorized access to computer systems in over 100 countries.[43]

Another type of operation is a cyber attack, which may be defined as an activity that "has effects in the real world beyond the cyber system itself" such as "actions in cyberspace whose foreseeable results include damage or destruction of property, or death or injury to persons."[44] In 2009, the Sayano-Shushenskaya Russian hydroelectric power plant suffered a serious accident. Workers shut down a dam's damaged turbine for maintenance; but a computer operator located at a separate control facility from the dam turned the turbine back on.[45] "The operator's electronically delivered command for increased activity caused the damaged turbine to spin out of control, killing 75 people and causing over $1 billion damage."[46] While this was an accident, it demonstrates the potential damage to infrastructure if individuals seeking to cause harm gained access to critical infrastructure computer systems.[47]

Cyber disruptions are a third type of cyber operations that "interrupt the flow of information or the function of information systems without causing physical damage or injury."[48] Cyber disruptions can interfere with a government's ability to communicate with its people or can include the distribution of false information through an "official electronic message system" that advocates for actions to be taken against the target government.[49] An excellent example of a cyber disruption is the 2010 incident named Operation Cupcake. Al Qaeda in the Arabian Peninsula (AQAP) published an online version of the magazine *Inspire*.[50] "[T]he British government

---

[42] *Id.*
[43] *Id.*
[44] *Id.* (noting that this definition differs from DOD's, which will be explained in the following section).
[45] Brown & Tullos, *supra* note 33.
[46] *Id.* (noting that this definition differs from DOD's, which will be explained in the following section).
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *See id.*

replaced the bomb-making instructions in the online publication with cupcake recipes," which lasted for several days.[51]

Another example of a cyber disruption occurred on July 4, 2009. Both the United States and South Korea suffered an attempt to "jam traffic on over two dozen government and commercial systems, including financial networks."[52] While the effects lasted only hours to a few days, such an attack could be replicated and cause further, lasting impacts.[53]

A third example occurred in 2007, when "[c]yber actions [in Estonia] shut down the Government's ability to communicate and froze the financial sector for about a month."[54] The attackers were motivated by a civil dispute—the Estonian government wanted to move the statue of a Soviet soldier and the perpetrators disagreed with this decision.[55] "Estonia heavily relied on cyberspace for communications and commerce, and experienced significant disruption of its communication and economic systems."[56]

And, finally, when Russia invaded Georgia in 2008, the nation simultaneously launched traditional military attacks and a cyber offensive. Georgia's web and telecommunications systems suffered a cyber disruption that prevented "many government computer-based activities in the early days of the Russo-Georgian conflict."[57] Georgia's civilian communications, financial systems, and media were also degraded by the cyber operations.[58]

As these examples suggest, "[c]yberwarfare is no longer the future of warfare—it is the present and the future."[59] Currently cyberspace is filled with "minor skirmishes, a silent cyber arms race,

[51] Brown & Tullos, *supra* note 33.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] Brown & Tullos, *supra* note 33.
[58] *Id.*
[59] Wall, *supra* note 25, at 115.

and major intelligence gathering."[60] These small, precursory actions may be setting the stage for larger cyber wars in the future; early stages of cyber activity demonstrates that countries are eager to learn as much as possible about U.S. critical infrastructure and information systems.[61]

In 2015, the U.S. Office of Personnel Management (OPM) suffered two separate, but related cyber security incidents that resulted in the disclosure of personnel data of 4.2 million current and former federal government employees and the background investigation records of 21.5 million current, former, and prospective federal employees and contractors.[62] OPM discovered malicious activity on the OPM network, which permitted the source of the incidents to steal information from the OPM-maintained background investigation databases.[63] The USG has yet to reveal the source of these cyber security incidents, and OPM, DHS, and the Federal Bureau of Investigation continue to investigate, assess the full impact, and assist with the remedial efforts following the incidents.[64] Although this collaborative team assessed that the attack is no longer active, the USG has not stated how the source gained access or for how long the attack went undetected.[65] This massive data breach demonstrates the potential impact of an access attack and highlights the pertinence of cyber security to the United States.

D. United States Cyber Command

In response to the growing threat of cyber warfare and the growing concern over cyber security, the DOD established U.S. Cyber Command (CYBERCOM). CYBERCOM is a sub-unified command nestled under the control of U.S. Strategic Command (STRATCOM). CYBERCOM is a topic-focused command, which

---

[60] *Id.*
[61] *Id.*
[62] OFFICE OF PERS. MGMT., CYBERSECURITY RESOURCE CENTER: CYBERSECURITY INCIDENTS (last visited Nov. 06, 2015) https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened.
[63] OFFICE OF PERS. MGMT., CYBERSECURITY RESOURCE CENTER: FREQUENTLY ASKED QUESTIONS (last visited Nov. 06, 2015) https://www.opm.gov/cybersecurity/faqs.
[64] *Id.*
[65] *Id.*

joined other Combatant Commands (COCOMs) such as U.S. Central Command (CENTCOM), U.S. Special Operations Command (SOCOM), and U.S. Africa Command (AFRICOM). COCOMs become the lead for the military and focus specifically on their respective topic or geographical areas. CYBERCOM's mission is to:

> Plan[], coordinate[], integrate[], synchronize[] and conduct[] activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to [the U.S.] adversaries.[66]

This mission is broad and grants CYBERCOM wide authority to take both defensive and offensive actions in cyberspace.[67] More specifically, DOD has identified three focus areas for CYBERCOM: "[d]efending the DODIN [Department of Defense Information Network], providing support to combatant commanders for execution of their missions around the world, and strengthening [the U.S.'s] ability to withstand and respond to cyber attack[s]."[68] CYBERCOM intends to improve "DOD's capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace."[69]

Furthermore, DOD has identified five key strategic initiatives for CYBERCOM to accomplish. The strategic initiatives are as follows:

> (1) DOD will treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential; (2) DOD will employ new defense operating concepts to protect DOD networks and systems; (3) "DOD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-

---

[66] *U.S. Cyber Command*, U.S. STRATEGIC COMMAND (last updated Mar. 2015), http://www.stratcom.mil/factsheets/2/Cyber_Command/.
[67] *See id.*
[68] *Id.*
[69] *Id.*

> government cybersecurity strategy; (4) DOD will build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity; and (5) DOD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.[70]

Thus, through CYBERCOM, DOD aims to improve training, education, and techniques, as well as establish partnerships with the private sector and international partners in order to meet the cyber security demands of cyberspace.

DOD is increasing its focus on cyberspace and exploring strategic objectives that will enable it to encounter 21st-century threats. DOD recognizes that "[d]evelopments in cyberspace provide the means for the US military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the OE, and can be leveraged to ensure the nation's economic and physical security."[71] Because cyberspace has created a paradox where both the "prosperity and security" of the United States "have been significantly enhanced" by cyberspace, yet cyberspace has "led to increased vulnerabilities and a critical dependence on cyberspace," [72] DOD, through CYBERCOM, is attempting to synchronize offensive and defensive measures in cyberspace in support and defense of the United States.

CYBERCOM operates under the authorities of the Secretary of Defense (SECDEF) and integrates defensive and offensive operations by synchronizing the activities of the COCOMs, Joint Staff, Office of the Secretary of Defense, the individual military branches, other government departments, and agencies.[73] DOD must conduct cyber operations in accordance with U.S. domestic law, applicable international law, relevant USG and DOD policies, and during times of armed conflict, DOD operations must follow the law of armed conflict by complying with the "fundamental principles of military necessity, unnecessary suffering, proportionality, and

---

[70] DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 23, at 10 (quoting the 2010 National Security Strategy).
[71] JP 3-12, *supra* note 2, at v.
[72] *Id*.
[73] *Id*. at vii-x.

distinction."[74] Thus, it is crucial to understand the legal framework that governs cyberspace. Military cyber operations that may be in conflict with this framework present serious issues for the DOD.

II. THE CURRENT LEGAL FRAMEWORK IN CYBERSPACE

The law regulating cyberspace is neither clear nor precise. To understand the legal framework that governs cyberspace, and the actions that violate this framework, it is important to understand both international legal concepts and domestic laws. "While cyber operations must satisfy both international and domestic law, the elements of analysis differ. An action may be permissible under international law, but face domestic legal or policy restrictions."[75] While domestic law usually controls in U.S. courts, international legal principles often inform domestic law principles.[76] Section II is divided into three parts. Part A explains how customary international law generally applies to cyberspace. Part B outlines the domestic legal framework. Finally, Part C describes CFAA in detail

---

[74] *Id*.

[75] Brown & Tullos, *supra* note 33.

[76] *See* DYCUS ET AL., *supra* note 4, at 163. When at war, the U.S. is bound by the principles of *jus in bellum*, which governs conduct when at war. *See*, *e.g.*, Geneva Convention Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135. The U.S. is bound by the Geneva Conventions and Hague Conventions as a signatory. *See generally* Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention (XI) relative to certain Restrictions with regard to the Exercise of the Right of Capture in Naval War, Preamble, Oct. 18, 1907, 36 Stat 2396. Furthermore, the United States is bound by the concept of *jus ad bellum*, which limits when a nation may engage in war. This concept is largely inferred from the U.N. Charter, which stipulates when a nation may use military force. *See generally* U.N. Charter, arts. 42, 43, and 51. Together, these international concepts shape how and when the U.S. engages in war. The U.S. is bound by these concepts based on treaties and signed international agreements. However, if Congress creates statutes contrary to these concepts, then the U.S. statutes rule under the "last in time" principle. *See* Comm. of U.S. Citizens Living in Nicaragua v. Reagan, 859 F.2d 929, 929 (1988). Furthermore, the U.S. does not believe itself to be regulated by customary international law or by international concepts that have not been adapted into U.S. statutes or made law through the treaty process. *Id*. at 936. Thus, while the United States' policies toward engaging in war and the United States' conduct once in war have been shaped by international law, the United States'. places what has been codified in treaties and statutes above international law.

and examines the potential civil liabilities that could arise under the statute against members of the armed forces. CFAA is a domestic policy of particular concern for the DOD.

A. Traditional International Law

The end of World War II brought a wave of international treaties attempting to define permissible uses of force and the laws governing conduct when nations are at war.[77] The international community was largely concerned with establishing and maintaining peace, and limiting the use of force to situations where it was the only means capable of resolving disputes and reinstating international peace and security.[78] One area in which these international agreements have become inadequate is in determining "how to address attacks that have little or no direct physical consequences, but that nonetheless cause real harm to national security," such as attacks in cyberspace.[79] While nation states have fallen short of claiming that a cyber attack would give rise to the requisite armed attack necessary for justifying a response using military force under Article 51 of the United Nations (U.N.) Charter, there is a general consensus that cyber attacks are an increasing threat to national and international peace and security.[80]

International legal concepts regarding the use of military force necessarily involve two concepts: *jus ad bellum,* or the international laws concerning a nation's right to wage war, and *jus in bello*, or the laws governing armed conflict once it has begun.[81] Understanding how these concepts relate to cyber security first requires a basic understanding of these concepts and how cyber security concerns differ from the pre-computerized world that existed when these concepts were formed and codified in international treaties and agreements.

---

[77] *See* Hathaway, *supra* note 31, at 840 (refencing the Geneva Conventions and the U.N. Charter).
[78] *See* DYCUS ET AL., *supra* note 4, at 210-12 (explaining that even when use of force is permissible, it must be limited only to effectuate legitimate political goals).
[79] Hathaway, *supra* note 31, at 840.
[80] *See id*.
[81] DYCUS ET AL., *supra* note 4, at 211, 234.

1. Jus ad bellum

Jus ad bellum incorporates the understanding expressed in the U.N. Charter for when nation states may go to war. Article 2 of the U.N. Charter states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations" in order to preserve international peace and security.[82] The prohibition against the use of force has two general exceptions: member nations are permitted to use force when they are taking part of collective security operations and "[when use of force] actions [are] taken in self-defense."[83] Thus, the crux of the debate is whether a cyber attack is analogous to an armed attack, thus enabling a state to respond in self-defense.[84] Because not every offensive action taken by one party against another rises to the level of an armed attack, it is questionable as to whether cyber attacks may amount to the use of force required to trigger a permissible use of force in response.[85] Additionally, determining the degree or the severity of a cyber attack's impact and whether it justifies taking reciprocal, defensive actions is no easy feat.[86]

Moreover, the United States has recognized that the international law principles of necessity and proportionality apply to cyber attack responses.[87] These principles limit the use of force, making responsive military actions a possibility only as a last resort when all diplomatic means have failed, and these principles require that an appropriate response be no more excessive in force than what is absolutely necessary to achieve legitimate political objectives.[88] The challenge again comes down to determining what is the appropriate degree of responsive action to a cyber incident and

[82] U.N. Charter, art. 2, para. 4.
[83] Hathaway, *supra* note 31, at 843-44 (outlining the exceptions to the authorization of use of force located in U.N. Charter Articles 39 and 51).
[84] *See* U.N. Charter art. 51. *See also* Hathaway, *supra* note 31, at 844.
[85] Hathaway, *supra* note 31, at 844-45.
[86] *See generally id.* at 845-49.
[87] *Id*. at 849.
[88] *See* DYCUS ET AL., *supra* note 4, at 234.

whether and at what point military force may be used in such a response.[89]

2. Jus in bello

When a state launches an armed attack, and the attack was sufficient to justify a response, the international law concept of *jus in bello* governs conduct during an armed conflict.[90] *Jus in bello* emphasizes four key principles that comprise an overarching guide to acceptable conduct in armed conflict: necessity, proportionality, distinction, and neutrality.[91] "Necessity relates to the concrete military advantage" that a military action attempts to gain, and if the actions do not advance the military's objective, they may be unnecessary and therefore prohibited.[92] Proportionality deals with the relation between the military advantage sought by the attack and the resulting harm caused to civilians; if the "incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof," far exceeds the military advantage, the response may be inappropriate and prohibited.[93]

The principle of distinction restricts the victims of attacks to military targets, and places relatively strict limits on who can perpetrate and who can be the target of responsive actions.[94] Distinction in responding to or conducting cyber activities is an interesting consideration. Under international law, civilians are not supposed to be the intended targets of military actions; however, because enemies are no longer clearly defined and computer systems are intertwined, the principle of distinction presents a unique challenge for responding to cyber attacks.

Lastly, the concept of neutrality pertains to nation states that declare neutrality in a conflict. This declaration of neutrality, however, does not keep independent actors from using the

[89] *See* Hathaway, *supra* note 31, at 848-50.
[90] DYCUS ET AL., *supra* note 4, at 211, 234.
[91] *See* Hathaway, *supra* note 31, at 850-55.
[92] *Id*. at 850.
[93] *Id*.
[94] *Id*. at 851-52.

information systems and networks of a neutral state to launch an attack.[95] Thus, the neutrality principle raises questions over how much control a nation state must maintain over its networks, especially if it is a neutral state, and who, then, becomes responsible for the use of the networks in a cyber attack launched from a neutral nation.[96]

While customary international law establishes a legal framework for traditional armed conflict, cyberspace challenges the concepts of *jus ad bellum* and *jus in bello*. The principles may very well be adaptable to cyberspace. However, finding the necessary armed attack that warrants a response using military force may prove more difficult in the context of cyber warfare. Further complicating the issue is the difficulty of defining an appropriate response to a cyber attack of sufficient magnitude while considering the four key principles governing armed conflict once it begins.

3. Countermeasures

The international concept of countermeasures provides more definitive guidance on responding to a cyber security incident. The principle states, "when a state commits an international law violation, an injured state may respond with a countermeasure."[97] Cyber attacks that may not rise to the level of an armed attack may still violate international customary law and may warrant an appropriate countermeasure.[98] Countermeasures, however, are intended only to coerce the state committing the act that is violating international law to cease its unlawful activities; and once the unlawful activities have stopped, the use of countermeasures must also stop.[99] For example, if a nation was hacking a government computer network in order to obtain information, the victim of the attack may be able to launch a counterattack; however, once the initial aggressor ceases the attack, the response must also cease. Additionally, if countermeasures must comply with the four key

[95] *Id*. at 855.
[96] *Id*.
[97] Hathaway, *supra* note 31, at 857.
[98] *Id.*
[99] *Id*. at 857-58.

principles of *jus in bello*, appropriate responses may be rather limited and difficult to define.

4. International Law in the United States

Generally, the U.S. is bound by the concepts of *jus in bello* and *jus ad bellum* where these concepts have been incorporated into U.S. law through treaties, statutes, and the adoption of international agreements such as the Geneva Conventions, Hague Conventions, and U.N. Charter.[100] When, however, the United States creates a statute governing the same matter as an international agreement or treaty, the "last in time" principle governs, where a statute that supersedes an international agreement does away with the United States' responsibility to act in accordance with the superseded policy.[101] Furthermore, when the United States wishes to enter a conflict, the branches of the USG disagree on whether the President, acting under the Commander in Chief power alone and regardless of Congress's war powers or international agreements, may introduce the military into combat, for how long, and what actions the President can authorize. [102]

While international organizations such as the U.N. and North Atlantic Treaty Organization (NATO) have discussed the need for cooperation in cyberspace, the international community only reached a mere general consensus declaring that more discussion is warranted for determining a legal standard for cyberspace. [103] Depending on the target or type of attack, aviation law, law governing outer space, and maritime law may provide further guidance on international legal concepts governing cyberspace.[104]

---

[100] DYCUS ET AL., *supra* note 4, at 234-35.
[101] *Id.* at 185-89.
[102] *Id.* at 267-75 (citing presidential use of the Commander in Chief power in entering Vietnam).
[103] Hathaway, *supra* note 31, at 860-64; *see also* OFFICE OF THE PRESS SEC'Y, THE WHITE HOUSE, PPD-21, PRESIDENTIAL POLICY DIRECTIVE – CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013), http://www.whitehouse.gov/ the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (explaining that it is U.S. policy to cooperate with international partners on cyber security matters).
[104] Hathaway, *supra* note 31, at 868-73.

Currently, however, international legal concepts provide nothing more than a collection of laws that may only apply under specific contexts. International legal principles were established well before the modern concept of cyber security was a concern, creating similar problems to those regarding the application of international law to conflicts involving terrorist organizations and other non-state actors.[105] While perhaps establishing a starting point, international law does not currently provide a legal standard for cyberspace. This is especially problematic given international law's control over armed conflict and the fact that most modern rules of war were adapted from customary principles of international law.

Thus, while some international legal concepts bind the United States, the applicability of international law is muddled by modern conflicts, including cyber security, where the international law has not yet been developed, and the disagreements over engaging in conflict are unsettled.

B. Domestic Law

In *2001: A Space Odyssey*, H.A.L., an artificially intelligent computer takes over a space ship sent on an outer space mission to find extraterrestrial life.[106] At its debut in 1968, the idea that a computer might be able to manipulate and take control of a mission and then kill human beings likely seemed far-fetched and revolutionary. Rather than reality, this likely seemed like the wild dream of a science fiction fanatic. Yet, some 46 years later, the threat posed by cyberspace, or the "global domain within the information environment consisting of the interdependent network of information systems [107] infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," is quickly approaching a risk level

[105] *See* DYCUS ET AL., *supra* note 4, at 234-35.
[106] *See* 2001: A SPACE ODYSSEY (Metro-Goldwyn-Mayer 1968).
[107] Where information systems are defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." ERIC A. FISCHER, CONG. RESEARCH SERV., R42114 FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 1 (2013).

similar to that of H.A.L.[108] Rather than having a clearly defined statutory scheme for dealing with an increasingly complex cyber security environment, the current legal framework is a hodgepodge of more than 50 federal statutes, some dating back to the 1800's.[109] These statutes attempt to govern 10 broad themes that are particularly relevant to the cyber security interests of the U.S. and its citizens:

> national strategy and the role of government, reform of the Federal Information Security Management Act (FISMA), protection of critical infrastructure (especially the electricity grid and the chemical industry, information sharing and cross-sector coordination), breaches resulting in theft or exposure of personal data such as financial information, cybercrime offenses and penalties, privacy in the context of electronic commerce, international efforts, research and development (R&D), and the cybersecurity workforce.[110]

As cyberspace continues to present an increasing threat to the U.S., legislators have been grappling to resolve issues relating to the key themes of cyber security and the current legal framework governing cyberspace. To some extent, the White House, the Senate, and the House of Representatives have been unable to agree on which agency should lead the nation's cyber security; currently that responsibility rests with DHS, at least for the time being.[111] Rather than having a clearly defined, ascertainable standard for infrastructure protection, the White House has promulgated a

---

[108] *Id*.
[109] *Id*. at 1-2, 21, 52.
[110] *Id.* at 4-5 (formatting omitted).
[111] *See id*. at 9-10. *See also* U.S. DEP'T OF HOMELAND SEC., BLUEPRINT FOR A SECURE CYBER FUTURE: THE CYBER SECURITY STRATEGY FOR THE HOMELAND SECURITY ENTERPRISE 2 (2011), http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf; PDD-21, *supra* note 103 (explaining that DHS is the lead on protection of critical infrastructure while the Department of Justice and the Federal Bureau of Investigation take the lead on counterintelligence and counterterrorism efforts related to critical infrastructure).

regulatory framework aimed at ensuring the United States' critical infrastructure, with DHS in charge of regulating those safeguards.[112]

Moreover, the "size, skills, and preparation of the federal and private-sector cybersecurity workforce," has concerned national-level policy makers, who have attempted to address issues such as education and training through legislative efforts.[113] "The need for improvements in fundamental knowledge of cybersecurity and new solutions and approaches . . . [to address] topics such as detection of threats and intrusions, identity management . . . , and supply chain security," have been recognized in many recent legislative actions.[114] Without a cohesive approach to operational security, managing threats and ensuring that agencies comply with national standards presents serious challenges to those responsible for securing cyberspace.[115] Furthermore, legislating in the cyber world presents complex policy issues because there are close ties between federal and private sector cyber systems, especially related to private-sector-owned critical infrastructure and the information sharing environment.[116]

In this mix of authorities granting permission to various agencies and departments, there is a complex framework governing cyberspace.[117] Furthermore, with the potential number of players involved—DHS, DOD, Congress, the Intelligence Community, the private sector, just to name a few—managing the web of applicable authorities, statutes, and regulations is cumbersome. While recognizing that cyber security is a major concern for U.S. national security and the importance of protecting critical infrastructure, cyber security frameworks are complicated by the mass of federal

---

[112] *See generally* THE WHITE HOUSE, REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE 1-9, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act.pdf.

[113] FISCHER, *supra* note 107, at 10.

[114] I*d.* at 11.

[115] *See also id.* at 52-61 (including a table with federal statutes deemed by CRS to have cyber security provisions).

[116] *Id*. at 13-15.

[117] *See id.* (summarizing the federal statutory framework governing cyber security).

statutes that may apply to cyberspace.[118] Further complicating the issue are statutes like the CFAA; a law designed to increase the U.S. cyber security, but one that may create liabilities for actions taken by U.S. military personnel.

C. The CFAA and Its Developments over the Years

The CFAA finds its origins in the Comprehensive Crime Control Act of 1984, which was Congress's first attempt to legislate for the emerging cyber threat.[119] The CFAA emerged in 1986 after Congress investigated problems associated with computer crimes and attempted to legislate the developing cyber security field.[120] It was designed to be "a tool for law enforcement to combat computer crimes."[121] In its current form, the CFAA

> outlaws conduct that victimizes computer systems. It is a cyber security law. It protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws.[122]

The legislative history indicates that Congress intended these provisions to provide "'a clearer statement of proscribed activity' to 'the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access.'"[123]

---

[118] *See generally* Nat'l Security Strategy Fact Sheet, *supra* note 12, at 2; NATIONAL INTELLIGENCE STRATEGY, *supra* note 14, at 4; *Worldwide Threat Assessment*, *supra* note 16, at 2.

[119] H. MARSHALL JARRETT, ET AL., COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION, PROSECUTING COMPUTER CRIMES 23 (2010).

[120] *See id.* at 1-3.

[121] Statement of Senator Sensenbrenner, *supra* note 21, at 2.

[122] CHARLES DOYLE, CONG. RESEARCH SERV., R 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS (2010) (text excerpted from the Summary located before the table of contents).

[123] JARRETT ET AL., *supra* note 119, at 1.

Because of the way that the CFAA evolved throughout the years, a "statute… designed to criminalize only important federal interest computer crimes potentially regulates every use of every computer in the United States and even many millions of computers abroad."[124] The USA PATRIOT Act amended the CFAA's definition used to define target computers, or the computers that are targeted in order to obtain information or take further, harmful actions. The CFAA refers to such a target as a "protected computer," which it defines as "computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions."[125] Essentially, the definition is so expansive that in order to qualify as a "protected computer," "it is enough that the computer is connected to the Internet."[126] Additionally, the USA PATRIOT Act amendments further expanded the definition to include all computers inside or outside of the United States, "so long as they affect 'interstate or foreign commerce or communication of the United States.'"[127]

A broad overview of the CFAA can be established by summarizing the seven general subsections of 18 U.S.C. § 1030 (a) and sections (b)-(g) of the statute. Section 1030 (a)(1) outlaws accessing a computer to commit espionage against the United States.[128] Section 1030 (a)(2) "outlaws computer trespassing (e.g., hackers) resulting in exposure to certain governmental, credit, financial, or computer-housed information."[129] To violate section (a)(2), one must "(1) [i]ntentionally access a computer, (2) without or in excess of authorization, (3) [to] obtain information (4) from financial records of financial institution or consumer reporting agency, OR the U.S. government, OR a protected computer."[130] Section 1030 (a)(3) outlaws computer trespassing (hacking by

[124] Orin S. Kerr, *supra* note 5, at 1561.
[125] DOYLE, *supra* note 122, at 47.
[126] *Id*. at 1.
[127] JARRETT ET AL., *supra* note 119, at 5.
[128] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (a)(1) (2008); DOYLE, *supra* note 122, at 1; JARRETT ET AL., *supra* note 119, at 12.
[129] *See* 18 U.S.C. § 1030(a)(2); DOYLE, *supra* note 122, at 2; JARRETT ET AL., *supra* note 119, at 16-17.
[130] JARRETT ET AL., *supra* note 119, at 16.

outside users) into a government computer, even if no information is obtained.[131]

Section 1030 (a)(4) outlaws committing fraud, an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce.[132] To demonstrate a violation under section (a)(4), one must "(1) [k]nowingly access a protected computer without or in excess of authorization, (2) with intent to defraud, (3) [where the] access furthered the intended fraud, and (4) obtained anything of value, including use if value exceeded $5000."[133] Section 1030 (a)(5) outlaws damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (*e.g.*, using a worm, computer virus, Trojan horse, time bomb, a denial of service attack, or other forms of cyber attack, cyber crime, or cyber terrorism).[134] Section (a)(5) has three subsections. To implicate section (a)(5)(A), one must "(1) [k]nowingly cause transmission of a program, information, code, or command, and (2) intentionally cause damage to protected computer without authorization."[135] To implicate sections (a)(5)(B) and (a)(5)(C), one must "[i]ntentionally access a protected computer without authorization" and "recklessly cause damage," or cause damage or loss, respectively.[136] Damage can include physical damage to a computer system or the dismantling of a communication system that prohibits emergency responders from functioning.[137]

Section 1030 (a)(6) outlaws trafficking in passwords for a government computer, or when the trafficking affects interstate or

---

[131] *See* 18 U.S.C. 1030(a)(3); DOYLE, *supra* note 122, at 2-3; JARRETT ET AL., *supra* note 119, at 23.
[132] *See* 18 U.S.C. § 1030(a)(4); DOYLE, *supra* note 122, at 46-48; JARRETT ET AL., *supra* note 119, at 26.
[133] JARRETT ET AL., *supra* note 119, at 26.
[134] *See* 18 U.S.C. § 1030(a)(5); DOYLE, *supra* note 122, at 29-32; JARRETT ET AL., *supra* note 119, at 35-48.
[135] JARRETT ET AL., *supra* note 119, at 35.
[136] *Id.*
[137] *See* DOYLE, *supra* note 122, at 29-32; JARRETT ET AL., *supra* note 119, at 36.

foreign commerce.[138] Section (a)(7) outlaws threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce.[139] Section 1030 (b) makes it a crime to attempt or conspire to commit any of these offenses.[140] Section1030 (c) catalogs the penalties for committing them that range from imprisonment for not more than a year for simple cyberspace trespassing to a maximum of life imprisonment when death results from intentional computer damage.[141]

Finally, there are the interesting parts of the CFAA that cause a problem for military cyber activities. Section 1030 (d) preserves the investigative authority of the Secret Service.[142] Section 1030 (f) disclaims any application to otherwise permissible law enforcement activities or intelligence activities, thus establishing an exemption for law enforcement or intelligence activities that would otherwise violate the CFAA.[143] Section 1030 (g) creates a civil cause of action for victims of these crimes.[144] "[A]ny person who suffers loss or damage by reason of a violation of" the CFAA may use section (g) to bring a civil cause of action against the actor who violated the CFAA, where person is defined as "any individual, firm, corporation, educational institution, governmental entity, or legal or other entity."[145] Additionally, there is a broad definition for the types of losses covered under section (g). And because the CFAA covers all "protected computers," which, as mentioned above, is broadly defined, the jurisdiction for such claims is wide.

---

[138] *See* 18 U.S.C. § 1030(a)(6); DOYLE, *supra* note 122, at 68-70; JARRETT ET AL., *supra* note 119, at 49.
[139] *See* 18 U.S.C. § 1030(a)(7); DOYLE, *supra* note 122, at 2; JARRETT ET AL., *supra* note 119, at 52.
[140] *See* 18 U.S.C. § 1030(b); DOYLE, *supra* note 122, at 2; JARRETT ET AL., *supra* note 119, at 55.
[141] *See* 18 U.S.C. § 1030(c); DOYLE, *supra* note 122, at 2.
[142] *See* 18 U.S.C. § 1030(d)(1); DOYLE, *supra* note 122, at 2.
[143] *See* 18 U.S.C. § 1030(f); DOYLE, *supra* note 122, at 2. *See also* Letter from John O. Brennan, Dir., Cent. Intelligence Agency, to Senator Ron Wyden, Cent. Intelligence Agency (Feb. 3, 2014), http://www.wyden.senate.gov/download/?id= 0a7dcd9a-d768-473c-937c-cb47ec3ac966&download=1 (explaining that 18 U.S.C. § 1030(f) allows the Central Intelligence Agency the ability to conduct any lawful investigation necessary).
[144] *See* 18 U.S.C. § 1030(g); DOYLE, *supra* note 122, at 2.
[145] DOYLE, *supra* note 122, at 24.

III. DO MILITARY ACTIONS IN CYBERSPACE VIOLATE THE CFAA?

A. U.S. Military Cyber Activities

Joint Publication 3-12(R): Cyberspace Operations (JP 3-12) is the military's doctrine for synchronizing the military's operations in cyberspace. The Joint Staff, J3 Operations division maintains this doctrine and promulgates it throughout the military and all of the services to provide guidance on military cyberspace operations. JP 3-12 states that military "[c]ommanders conduct cyberspace operations (CO) to retain freedom of maneuver in cyberspace, accomplish the joint force commander's objectives, deny freedom of action to adversaries, and enable other operational activities."[146] JP 3-12 names three categories of cyberspace operations that the military carries out: (1) offensive cyberspace operations (OCO), (2) defensive cyberspace operations (DCO) and DOD information network operations.[147]

OCO are CO intended to project power by the application of force in and through cyberspace. DCO are CO intended to defend DOD or other friendly cyberspace. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation.[148]

JP 3-12 enumerates several threats that it intends to counter with this combination of CO. First, there is the Nation State threat, where "[o]ther nations may employ cyberspace to either attack or conduct espionage against the U.S."[149] The second threat, the Transnational Actor threat, involves "actors [that] use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist actions within cyberspace."[150] The third

---

[146] JP 3-12, *supra* note 2, at vi.
[147] *Id*. at vii.
[148] *Id*.
[149] *Id.* at I-6.
[150] *Id*. at I-7.

threat, Criminal Organization, uses cyberspace to "steal information for their own use or, in turn, to sell to raise capital."[151] Additionally, criminal organizations may also "be used as surrogates by nation states or transnational actors to conduct attacks or espionage through [cyber operations]."[152] The fourth threat, Individual Actors or Small Groups can gain "access into systems to discover vulnerabilities, sometimes sharing the information with the owners; however, they also may have malicious intent."[153] Because Individual Actors and Small Groups are often driven by strong political points of view, cyberspace provides an easy way to spread their message. "These actors can be exploited by others, such as criminal organizations or nation states, in order to execute concealed operations against targets in order to preserve their identity or create plausible deniability."[154]

JP 3-12(R) does not reveal much about the OCO used by the military to engage these threats; however, it does mention, "OCO are CO intended to project power by the application of force in and through cyberspace."[155] Additionally, OCO require authorization "like [traditional military] offensive operations in the physical domains, via an execute order" and must be conducted in accordance with current policies.[156] "DCO are CO intended to defend DOD or other friendly cyberspace."[157] DCO are both passive and active CO designed to "preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[158] DCO Response Actions "must be authorized in accordance with the standing rules of engagement and any applicable supplemental rules of engagement and may rise to the level of use of force."[159] JP 3-12(R) encourages cyber activities to "be

[151] *Id*.
[152] JP 3-12, *supra* note 2, at I-7.
[153] *Id*.
[154] *Id*.
[155] *Id*. at II-2.
[156] *Id*.
[157] *Id*.
[158] JP 3-12, *supra* note 2, at II-2.
[159] *Id*. at II-3.

in compliance with U.S. domestic law, international law, and applicable rules of engagement."[160]

JP 3-12(R) also explains the type of capabilities that the military might exploit in cyberspace. Cyberspace defense is one such capability, which includes activities such as "protect[ing], detect[ing], characterize[ing], counter[ing], and mitigat[ing]" actions taking place in cyberspace.[161] Cyberspace intelligence, surveillance, and reconnaissance (ISR) is an action "conducted to gather intelligence that may be required to support future operations, including OCO or DCO."[162]

Cyberspace attacks are "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."[163] Cyberspace attacks that fall under the category of "denial" are designed to "degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time."[164] Within such attacks, to "degrade" access means to "deny access to, or operation of, a target to a level represented as a percentage of capacity."[165] To "disrupt" means to "completely but temporarily deny access to, or operation of, a target for a period of time."[166] And to "destroy" means to "permanently, completely, and irreparably deny access to, or operation of, a target."[167] Manipulation attacks aim to "control or change the adversary's information, information systems, and/or networks in a manner that supports the [military's] objectives."[168]

Based on DOD's policy regarding cyber operations and CYBERCOM's mission, DOD's current CO may conflict with its need for DOD actions to comply with domestic and international

---

[160] *Id.*
[161] *Id.* at II-4.
[162] *Id.* at II-5.
[163] *Id.*
[164] JP 3-12, *supra* note 2, at II-5.
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*

legal frameworks governing cyberspace. While DOD may be justified in responding to a cyber attack against the United States., some of the DOD operations described likely violate the CFAA. Thus, if the CFAA applies to DOD and members of the armed forces, U.S. military personnel may find themselves personally liable for the cyber activities they conduct, despite carrying out those activities in accordance with their orders.

B. Interpreting the CFAA: Is the Military Acting in Violation of the Law?

When examining the CFAA, one thing is evident: 18 U.S.C. §1030 (f) creates an exception that states "[t]his section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."[169] As the military increases its role in cyberspace and potentially takes actions that may violate the CFAA, determining whether this exception applies to DOD is critical. After all, the United States does not hold members of the armed forces personally liable for violating other laws, such as when members of the armed forces are handed weapons and told to kill enemy combatants.[170] Thus, CYBERCOM's success in meeting its objectives may turn on whether members of the armed services are violating the CFAA and whether members of the armed services may be held civilly liable for the actions undertaken by the DOD.[171]

This analysis will begin by examining judicial precedent on the applicability of federal laws to government agents and whether members of the military may be held personally liable for acting in accordance with their orders. The analysis will continue by applying

---

[169] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(f) (2008).

[170] DYCUS ET AL., *supra* note 4, at 404.

[171] Where military personnel are operating under the authority of intelligence agencies, they are covered by the exception. *See* 18 U.S.C. § 1030(f). This occurs when military personnel are stationed—or their permanent duty station is— at one of the intelligence agencies. However, as CYBERCOM has its own mission and authorities, whether DOD's actions violate the CFAA is a key concern. CYBERCOM must also act in accordance with domestic law and international law governing conduct at war. *See* Exec. Order No. 12,333, 46 F.R. 59941 (1981).

canons of statutory interpretation to the text of the CFAA. The analysis will then use various methods of statutory interpretation, to include plain meaning and new textualism, pragmatism, and legislative intent, in determining whether the Supreme Court would find that the military's cyber activities violate the CFAA. The analysis ultimately concludes that the military is likely violating the CFAA and suggests a way forward to resolve this potential problem and avoid holding soldiers, sailors, airmen, and marines personally liable for merely following orders.

Nardone v. United States is an excellent place to begin the analysis assessing the applicability of the CFAA to DOD cyber activities.[172] *Nardone* explains that when the legislature fails to create an exception for the activities of the government or government agents, activities undertaken by such agents that violate the statute are impermissible.[173] In *Nardone*, the Supreme Court was analyzing the Federal Communications Act of 1934.[174] The statute provides that

> no person who, as an employee, has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employees, save in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority; and "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[175]

The Court found that because the statute read "no person" and did not create any exceptions for agents of or for the federal government, the statute prohibited wiretapping by all persons, including federal agents of the government, even when doing so for investigative purposes.[176] The evidence federal agents obtained to

---

[172] Nardone v. United States, 302 U.S. 379, 379 (1937).
[173] *Id*. at 383.
[174] *Id*. at 380-81.
[175] *Id.*
[176] *Id.* at 384-85.

prosecute Nardone and his conspirators for alcohol smuggling during Prohibition was inadmissible because the agents had knowingly violated the Federal Communications Act of 1934 to obtain it.[177] Two years later, the Court further held that a summary of the general content, not only the exact wording of the messages, was also inadmissible as it was also illegally obtained.[178] The content was the "fruit of the poisonous tree;" thus, what the government had wrongfully obtained was inadmissible regardless of whether it was the exact words or a summary of the content.[179]

The Court, in the first *Nardone* case, held that if Congress desired to permit the government or government agents to act contrary to the statute, Congress was more than capable of writing such an exception into the act.[180] However, the Court found that "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty." Thus, the Court relied on the plain words of the statute and Congress's intent to protect personal liberty.[181] The Court found that where Congress had created no exception, the government could not act contrary to the statute.[182]

The *Nardone* cases set a strong precedent for general applicability statutes: where Congress creates no exception for the government or government agents, activities conducted by the government or its agents that violate the statute are impermissible. Thus, the words of the statute bind the conduct of the federal government, or the agents thereof, the same way they bind any other person.

Moreover, in *Little v. Barreme*, a Supreme Court case from 1804, the Court found that members of the military may be held personally liable for damages caused to any person injured by their

---

[177] *Id*. at 389.
[178] Nardone v. United States, 308 U.S. 338, 340-41 (1939).
[179] *Id*.
[180] Nardone v. United States, 302 U.S. 379, 381-83 (1937).
[181] *Id*. at 384-85.
[182] *Id*.

actions, even if the actions were in accordance with their orders.[183] In *Little*, a ship captain was found liable for civil damages when he seized a ship coming from a French port on direct orders from the President, the Commander in Chief, because such actions exceeded the statutory authority granted for seizing ships.[184] The statutory authority permitted the seizing of ships going to a French port; when the orders were given, however, the executive expanded them to include ships going to and coming from a French port.[185] Chief Justice Marshall explained that it seemed logical to hold the issuing authority responsible for the liabilities arising from the actions of military officers following their instructions, as it is the duty of military personnel to obey orders.[186] However, the Chief Justice further explained that the fact that a military member was merely following orders did not change the nature of the actions or legalize an act that exceeded the statutory authority granted by the legislature.[187] Thus, the Court found the captain to be personally liable for the damages.[188]

Little stands for the proposition that military personnel may be held liable for damages caused by their actions when such actions violate statutory law, even if the actions are taken in accordance with military orders. Although *Nardone* is from the 1930's and *Little* from the 1800's, both still stand as applicable law. Taken together, there is a strong precedent for holding members of the armed forces personally liable for their actions, even when acting in accordance with orders, when those actions violate valid statutory law.

In *Legislation and Statutory Interpretation*, authors William N. Eskridge, Philip P. Frickey, and Elizabeth Garret explain that there is a "super strong presumption of correctness" when the Court interprets statutes and creates precedent for interpreting statutes.[189]

---

[183] Little v. Barreme, 6 U.S. 170, 179 (1804).
[184] *Id*. at 177-78.
[185] *Id*.
[186] *Id*. at 179.
[187] *Id*.
[188] *Id*.
[189] WILLIAM N. ESKRIDGE ET AL., LEGISLATION AND STATUTORY INTERPRETATION 284 (2nd ed. 2006).

"Once the Supreme Court has authoritatively construed a federal statute, that precedent is not only entitled to the usual presumption of correctness suggested by the common law doctrine of *stare decisis*, but it is supposed to be given an even stronger *stare decisis* effect."[190] Furthermore, the Court believes that when its interpretation is wrong, Congress, rather than the Court, is responsible for fixing the meaning of the statute.[191]

Given precedent, and the Court's deference in accordance with the principle of *stare decisis*, it is likely that the Court would hold members of the armed services who conduct cyber activities that violate the CFAA personally liable for those activities. It is possible to argue that because the CFAA creates an exception for some government activity (the section 1030 (f) exception for law enforcement and intelligence activities), the *Nardone* general applicability rule does not apply to the CFAA. This, however, fails to incorporate the notion of *expressio unius est exclusio alterius (expressio unius)*. This canon of statutory interpretation translates to and means, "the expression of one thing suggests exclusion of all others."[192] The Court relies on canons of interpretation to help create consistency in interpretation of statutes.[193]

Thus, in following the Court's logic in *Nardone* and employing the *expressio unius* canon, Congress's failure to create an exception for the military while creating an exception for law enforcement and intelligence activities implies that the military cannot make use of the exception. After all, had Congress wanted to include the military in the exception, it easily could have done so when it created an exception for two other forms of government—law enforcement and intelligence activities. The fact that Congress created an exception for certain aspects of the federal government does not imply that all government agencies, departments, or agents may make use of the exception. In fact, it would seem to be the opposite. If Congress legislates certain, limited exceptions rather

[190] *Id*. at 286.
[191] *Id*.
[192] *Id*. at 263.
[193] *Id*. at 260.

than generally excusing government activities, it conveys the intent to limit the exceptions only to what Congress expressly grants.

Furthermore, when examining the text of the CFAA under a new textualist approach, the plain meaning is that Congress did not grant the military an exception for cyber activities that ostensibly violate the CFAA. New textualists believe that the meaning of statutory text should be derived from "the meaning an ordinary speaker of the English language would draw from the statutory text."[194] According to new textualists, "the only thing that actually becomes law is the statutory text, [and] any unwritten intentions of one House of one committee or of one member are not law."[195] Under this theory, "when the text is relatively clear, interpreters should not even consider other evidence of specific legislative intent or general purpose."[196] The plain meaning of the CFAA, from a new textualist perspective, indicates that Congress wanted to create a limited exception for certain government activities. From this perspective, the CFAA makes clear that some elements of the government are exempt from complying with the statute. The military however, is not included in 18 U.S.C. § 1030 (f).

It is possible to argue pragmatically, using a dynamic theory, to find an exception for the military implied in section 1030 (f).[197] After all, the statutory text does not exist in isolation and given the likely good intentions of military cyber activities, it might make sense to imply an exception for military activities when one already exists for similar government actions. However, given the strong precedent and plain meaning of the text, these arguments would likely fail. Because the "rule of law requires a law of rules that are predictable applied to everyone," deciding based on arguments that do not comport to the plain meaning of the text would essentially be deciding against what has become law.[198] The Constitution set up a rigid process for creating law—the process of Bicameralism and

[194] *Id*. at 235-36.
[195] ESKRIDGE ET AL., *supra* note 189, at 235-36.
[196] *Id*.
[197] *Id*. at 245-50.
[198] *Id*. at 237.

Presentment—that was designed to create well-reasoned laws.[199] Through this process, Congress created a limited exception without extending 18 U.S.C. § 1030 (f) to the military. Thus, finding an exception where none exists would go against judicial precedent, plain meaning, and the text of the statute that became law.

While the original intent of the CFAA may have been narrowly tailored for the protection of government computers and prohibiting access to sensitive government information, its continuous evolution through numerous amendments has drastically changed its reach and intent.[200] As previously mentioned, the CFAA reaches almost every computer and every computer user because of the ever-growing cyber security threat.[201] Thus, while law enforcement and intelligence activities have remained in the 18 U.S.C. § 1030 (f) exception, the legislature has failed to extend that exception to the military. As the DOD's role in cyber security continues to grow and expand, a problem arises because of the CFAA's liabilities and the statute's likely applicability to U.S. military personnel. While the United States does not hold members of the military liable for other offenses committed in violation of domestic or international law when acting in accordance with their orders, military personnel may find themselves liable under the CFAA.

IV. THE SOLUTION

A. A Quick Fix

The obvious quick fix is to add the military to the Section 1030 exception or amend the statute adding a new exception for the military. This conclusion seems logical, given the wording of 18 U.S.C. § 1030 (f), which permits lawful investigative, protective, and intelligence cyber activities of law enforcement and intelligence

---

[199] *Id.*

[200] *See, e.g.*, Major Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, 2013 ARMY LAW. 4, 15 (2013) (explaining that the CFAA now includes civil liability for anyone who "intentionally access[es] a protected computer without authorization or exceed[s] authorized access") (quoting the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4) (2008)).

[201] *See* JARRETT ET AL., *supra* note 119, at 4; DYCUS ET AL., *supra* note 4, at 267-375.

agencies. Thus, lawfully authorized, investigative, protective, and intelligence activities, or those similar in nature, carried out by the armed forces to protect and defend the United States seem to qualify for the same exception. This solution, however, is dependent on Congress's determination that the military should be exempted from CFAA liability.

Congress could also choose to define an exception for the military by granting the military a specific exception for certain DOD activities under the CFAA. Because the military is already operating in cyberspace in ways that potentially violate the CFAA, this exception is necessary, even if it is only temporary. This will enable the military to continue operating without violating the statute and potentially creating civil liabilities for U.S. servicemen and women.

B. The Computer Fraud and Abuse Act

More importantly, Congress should revise the CFAA to reflect its original intent more closely, which was to protect government computer systems and sensitive government information. Because of the CFAA's evolution over the last thirty years, its coverage has become immensely broad; some would argue that it has become so over encompassing that a court should hold it void for vagueness.[202] Congress originally enacted the CFAA with limited applicability.[203] Revising the CFAA so that it resembles this original intent is necessary. Such a modification reflects a more reasonable standard without neglecting the problems the CFAA sought to prevent—most notably, possible attacks on USG computer systems and the loss of sensitive government information. Ignoring this step in the solution exposes more than just the members of the armed forces to potential liabilities. Currently, the statute regulates computer activities of which the average computer user is likely unaware.

More drastically, scrapping the CFAA entirely to replace it with a statute reflecting the more limited, original intent would add

---

[202] Kerr, *supra* note 5, at 1562.
[203] *Id.*

clarity to the overly broad statute. Congress could also draft a statute that avoids exposing members of the military to civil liabilities.

C. The Military's Role in Cyber Security

The military's role, and the larger DOD role, in cyberspace needs to be more clearly defined. Domestically, there are a number of actors involved in the cyber security debate ranging from the President, to Congress, to the DHS and beyond. Additionally, the volume of applicable statutory material makes it difficult to determine what rules apply to cyberspace and what actions DOD can take that do not violate other federal laws (a main problem underlying the CFAA debate). Moreover, although cyberspace is becoming a major concern for the USG and U.S. allies, the international policy on cyberspace is unsettled. Therefore, determining what constitutes a cyber attack, determining an appropriate response to cyber incidents, and determining what actions can be taken offensively and defensively in cyberspace are necessary to create a legal framework for governing this 21st-century battlefield.

Based on the indefiniteness of policy in this area, this is no easy task. However, as the world becomes increasingly reliant on technology and cyberspace, including U.S. adversaries, and incidents involving cyberspace continue to occur with increasing frequency, efforts to establish the DOD's role in cyberspace, as well as clarifying the rules of engagement in cyberspace are critical to U.S. national security. And, as this comment demonstrates, it is essential to protecting servicemen and women from civil liabilities for merely following military orders that may violate the law.

V. CONCLUSION

Cyberspace is one of the newest and most challenging battlefields, and it is accompanied by a lack of clear legal standards governing conduct. Because of the unique challenges presented by cyberspace, traditional international law and U.S. domestic law have left a gap in authority for DOD action. As DOD increases its presence in cyberspace, it faces a unique challenge: potential civil

liabilities for members of the armed services when acting in accordance with orders that violate the CFAA. The military merits a speedy exception to this statute similar to that provided for law enforcement and the intelligence community. Furthermore, the CFAA needs a revision to embody its original intent to correct its over encompassing expansion after 30 years and many amendments. Finally, defining the military's role in cyberspace and the rules of engagement for this new battlefield is essential to U.S. national security.