I. Foreword .................................................................................................1
   Daniel Garrie
II. No State is an Island in Cyberspace .................4
    Jessica “Zhanna” Malekos Smith
III. Measuring Autonomous Weapon Systems
     against International Humanitarian Law
     Rules ..................................................................................................66
     Dr. Thompson Chengeta
IV. Congressional Cybersecurity Oversight: Who’s
    Who and How It Works ...............................................................147
     Lawrence J. Trautman
FOREWORD
By Daniel Garrie*

Today our country is faced with the stark and harsh reality that cyber warfare is playing an instrumental role in the domestic and foreign policies of both the United States, and international community at large. One cannot go a week without seeing the front page of the news featuring a cyber incident – a crime, attack, act of terror, or other state sponsored activity. From criminals stealing nearly $100 million from the Bank of Bangladesh,1 to the Ukrainian power grid being knocked out, leaving 230,000 citizens in the dark,2 and even to determining elections,3 the impact of cyber warfare is here to stay. The ability of cyber warfare to shape world events can be demonstrated no better than

* Daniel Garrie is an Arbitrator, Forensic Neutral, technical Special Master, at JAMS, available in Los Angeles, New York, and Seattle; Executive Managing Partner of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups, with locations in the United States, India, and Brazil; Partner and Co-Head of Cyber Security at Zeichner, Ellman & Krause; Editor-in-Chief of the Journal of Law and Cyber Warfare; and adjunct Professor of Law at Cardozo School of Law. The author would like to thank Masha Simonova and Benjamin Dynkin as contributors.

1 That Insane, $81M Bangladesh Bank Heist? Here’s What We Know, Kim Zetter, WIRED (May 17, 2016), https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.
the very recent cyber-attack on the Democratic National Convention.

Imagine for a moment that instead of headlines like “Russian government hackers penetrated DNC, stole opposition research on Trump”, 4 “DNC Hack Prompts Allegations of Russian Involvement”, 5 and “Experts: Hard to prove Russians behind DNC hack”, we read a headline “Foreign criminals break into DNC HQ and steal communications and opposition research”. The latter would likely lead to an unprecedented response by the United States Government, leading to a highly publicized hunt for the criminals, which would lock down all means of egress from our nation until the issue was resolved. Pundits on both sides of aisle would debate the issue, and in likelihood congressional summons would be issued.

The truth of the matter is that none of this happened. The story hit the news cycle for 24-48 hours, and over the course of a month nobody paid the issue any attention. That is until we began to see the fallout. When Wikileaks, on July 22, released nearly 20,000 sensitive


emails, the fate of a Presidential election may have been determined. To date, these actors have apparently absconded with zero repercussions, while impacting the election of the leader of the free world, a notion that should seem ludicrous to anyone if it played out in the physical world.

The Journal of Law and Cyber Warfare is not a partisan publication. I write this forward as the Editor-in-Chief to highlight the power of an act of cyber war, and the DNC example is only the tip of the spear.

The articles in this issue present a range of views and perspectives, both U.S. centric and global, and seek to move the issues surrounding cyber warfare and its implications out of the shadows and into the spotlight.

---

7 Search the DNC email database, WIKILEAKS, https://wikileaks.org/dnc-emails/.
NO STATE IS AN ISLAND IN CYBERSPACE
By Jessica “Zhanna” Malekos Smith

ABSTRACT

Economic espionage against one state is an affront to the economic stability of all; for no state is an island in cyberspace. But does a state’s difficulty in attributing a hostile cyber act to its true provenance challenge the enforcement of international law in cyberspace? For if a cyber actor can remain anonymous, or impervious to sanctions, do international accords prohibiting the cyber-enabled theft of intellectual property hold any measurable deterrent effect? Given the distinct cultural norms embedded in distinguishing between permissible and impermissible intelligence collection, a dispute resolution framework that accounts for both cultural disparities and the complexities of attribution, is needed. This Article therefore provides a legal theory – a Cyber Espionage Predominant Purpose Test – for equitably resolving international disputes concerning cyber espionage operations that involve mixed elements of national security espionage and commercial espionage.

*With special thanks to Prof. Matthew Bishop, Prof. Anupam Chander, Prof. David Horton, Thomas E. Smith, Colleen Swanson, and the diligent staff of the Journal of Law and Cyber Warfare for their generosity of time and support.
INTRODUCTION

“No man is an island,
Entire of itself,
Every man is a piece of the continent,
A part of the main.
If a clod be washed away by the sea,
Europe is the less.
...
Any man’s death diminishes me,
Because I am involved in mankind,
And therefore never send to know for whom the bell tolls;
It tolls for thee.”

– John Donne, No Man Is an Island

In the new frontier of cyberspace, no state is an island. As John A. Serabian Jr. noted during a Joint Economic Committee on Cyber Threats and the U.S. Economy, “cyber threats can come from almost anywhere. They can originate from any location, affect systems anywhere in the world, disguise origins and travel routes, and do it all instantaneously.” Adding to the litany of asymmetrical threats is the attribution challenge.

10 See Cyber Threats to National Security, Summary of Symposium One: Countering Challenges to the Global Supply Chain (2010), http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf (stating that “[c]yber threats are asymmetric because attacks may be perpetrated by the few upon the many, with little cost and resources. . .”
Attribution is “the association of data (called a characteristic) with an entity (person, process, file, or other data).”\textsuperscript{11}

The attributive analysis process, as described by University of Nebraska Law Professor Jack M. Beard, involves “[d]etermining the origin of information used in a hostile cyber action, identifying its geographic contours, and attributing the transmission of that information to specific persons and then to a responsible state . . . .”\textsuperscript{12} The reader is cautioned, however, from construing attribution as a matter that can be neatly parsed into categories of “solved” or “unsolved” incidents.\textsuperscript{13}

More accurately, as Professor Thomas Rid and Ben Buchanan of King’s College London War Studies posit, “[a]ctual attribution of cyber events is already more nuanced, more common, and more political than the literature has acknowledged so far.”\textsuperscript{14} While it is tempting to decry a state’s difficulty in properly attributing a hostile cyber act, one can also imagine instances wherein false attribution can strategically mislead an adversary, to gain an informational advantage on the target’s tactics, techniques and procedures. Indeed, just as there is a degree

\textsuperscript{14} See id. at 6.
of risk, as well as a benefit derived from taking antibiotics, attribution frameworks also offer mixed potential outputs.\(^{15}\) Put another way, adding a poetic flourish from John Perry Barlow’s 1996, *A Declaration of the Independence of Cyberspace*: “We cannot separate the air that chokes from the air upon which wings beat.”\(^{16}\)

But given the rich complexities of attributive analysis, can international law be effectively enforced in this domain? For if an actor believes they can remain anonymous, or impervious to sanctions, do international laws prohibiting commercial espionage have any measureable deterrent effect?\(^{17}\) Deterrence, as defined by U.S. Air Force Major Erik M. Mudrinich, is “the ability to persuade others not to attack you because doing so would result in retaliation.”\(^{18}\)

Without a robust deterrence mechanism, does the attribution challenge undermine international accords that prohibit certain state behaviors in cyberspace? For example, under the Obama-Xi Cyber Pact of 2015, President Barack Obama and China’s President Xi Jinping, agreed that neither government would “conduct or

\(^{15}\) See Bishop et. al., *supra* note 4 (explaining that the use of an attribution framework “simplifies some actions and relationships; it also makes more difficult the protection of privacy under some circumstances.”)


knowingly support the cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage.” While accords to normalize cyber state relations are commendable, attribution can also erode enforcement mechanisms here, for “[d]oing attribution well is at the core of virtually all forms of coercion and deterrence, international and domestic. Doing it poorly undermines a state’s credibility, its effectiveness, and ultimately its liberty and security.”

Further, although states collect economic intelligence – a subset of national security espionage – it is commercially motivated espionage by states such as China that is disfavored. But can the law meaningfully distinguish between cyber espionage aimed at gathering economic intelligence for national security purposes, and economic espionage? According to former U.S. Treasury Secretary, Henry M. Paulson, Jr. (2006-2009), “the distinction between cyberespionage and cybertheft from a company for commercial use can become fuzzy.”

---

20 See Rid & Buchanan, supra note 6 at 4 (emphasis added).
The Article proceeds as follows: **PART I** focuses on understanding attribution and how its core modalities challenge the enforcement of international law in cyberspace and support state espionage operations. Next, it considers the attribution needs of states that have fallen victim to hostile cyber acts.23

**PART II** highlights the historical as well as theoretical distinctions, between national security espionage and economic espionage.

**PART III** examines two cases of economic espionage committed by China against the U.S. The first case, Operation Aurora, involves a series of debilitating attacks designed to steal intellectual property information from Google and 34 other companies.24 The second chronicles a three-year breach of U.S. Defense contractor QinetiQ, and their industrial data on military robotic systems and drones.25 It then assesses the import of the Group of 20 (G-20) Summit Cyber Agreement in 2015.

23 See Beard, supra note 5 at 76-77 (“In the case of hostile, state-sponsored actions, the difficulty in identifying the genuine origin of damaging information is only the first step in the arduous process of attributing the transmission of such information to a responsible state.”)


Lastly, PART IV proposes a Cyber Espionage Predominant Purpose Test (CEPP); a legal test designed to enable the International Court of Justice (ICJ) to equitably resolve international disputes concerning espionage operations that involve elements of national security driven intelligence collection activities and commercially motivated espionage.

I. UNDERSTANDING ATTRIBUTION

“There is nothing like first-hand evidence.”
– Sherlock Holmes, A Study in Scarlet.

At its base level, attribution is “the association of data (called a characteristic) with an entity (person, process, file, or other data).” Within the context of cyber security, a term that refers to the practices of protecting data and information communications systems, attribution carries an adversarial connotation. The underlying goal of attribution, as articulated by Matthew Bishop, Carrie Gates,

(last visited March 3, 2016).


27 See Bishop *et. al.*, *supra* note 4; this basic concept of attribution can be analogized with the process of donating a pint of blood to a blood bank, in which information about your ABO blood group (characteristic) is associated with your donation (entity).

28 See *A Glossary of Common Cybersecurity Terminology, National Initiative for Cybersecurity Careers and Studies*, https://niccs.us-cert.gov/glossary#letter_c (defining cybersecurity as “[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.”)
and Jeffrey Hunker, centers on “determining the identity or location of an attacker or an attacker’s intermediary.”

This objective, however, can be thwarted, for “[e]ven if some malicious acts in cyberspace can be traced to specific physical connections, the ultimate origin of the harmful information may remain a mystery because of the nature of the information.”

Furthermore, attribution implicates data assurance. Here, assurance is defined as a “level of certainty associated with showing that the characteristic associated with an entity has a particular value, or one of a particular set of values.” As such, attribution and assurance are part and parcel.

A. The Goal of Attributive Analysis in Cyber Security

Just as “[t]he goal of attribution is to show the characteristic associated with an entity has a particular value, or one of a particular set of values,” a crime scene analyst is driven by the same principle in meticulously preserving, cataloging, and analyzing each item of evidence discovered. Attributing hostile cyber acts and investigating a physical crime scene hold much in common, for “[a]tribution is the art of answering a question as old as

30 See Beard, supra note 5 at 76.
31 See Bishop et. al., supra note 4.
32 See id.
crime and punishment: *who did it?*”

Indeed, the attributive analysis process can be likened to the investigators efforts to examine trace evidence to ascertain information about potential suspect(s). As Henry M. Holden describes in *To Be a Crime Scene Investigator*, “[t]he ultimate purpose of a crime scene search is to collect evidence that links a suspect to the crime or victim.”

Generally, finding data to link a suspect to a cyber crime is a complex endeavor, for cyber malefactors often work anonymously to exploit system vulnerabilities and design payload systems to achieve their desired objectives. While hostile cyber acts manifest in a variety

---

33 See Rid and Buchanan, *supra* note 6 at 4.
35 See George Schiro, *Collection and Preservation of Blood Evidence from Crime Scenes*, CRIME SCENE INVESTIGATORS NETWORK, http://www.crime-scene-investigator.net/blood.html (explaining that “[p]roperly collected and preserved blood evidence can establish a strong link between an individual and a criminal act. Blood evidence or the lack of blood evidence can also be used to bolster or contradict a witness statement or any statements that the suspect may make. Blood evidence can also point the investigator in the direction he or she needs to go to solve the case.”)
37 See Mudrinich, *supra* note 9 at 168 (“A “payload” is software code designed within the worm to deliver a specified effect – from deleting critical files, to taking control of a system or installing a backdoor into the network.”)
38 See Hollis, *supra* note 10 at 384 (noting that attackers “must have both access to the vulnerability and a payload to produce the desired result . . . . Attackers must also have access to that system and a program allowing them to exfiltrate information or to alter, disrupt,
of forms, Professor Duncan Hollis of Temple Law School identifies the five most common as:

(1) targeting the “global supply chain for computer and network hardware and software;”
(2) leveraging remote access capabilities;
(3) a denial-of-access, wherein “data requests flood an Internet server, overwhelming its ability to respond or process requests;”
(4) leveraging proximity to the wireless network “to monitor signals, connect to the same network as their targets, or convince unsuspecting targets to make the connection for them;”
(5) Insiders (e.g. the social engineering threat, wherein “insiders offer up access unwittingly.”

Apart from the technological challenges that flow from attributing the source of these attack forms, the process is also fraught with administrative challenges like limited financial capital and available labor resources. For Morgan Marquis-Boire, a former employee of Google’s

usurp, or destroy the system itself.”)

See id. at 384-85.
See id. at 384.
See id.
See id. at 385.
See id.
See Hollis, supra note 10 at 385.
See Rid & Buchanan, supra note 6 at 10. (“In a world of many incidents and not enough investigators, the amount of damage cause or threatened frequently determines the resources that are invested into attributing the malicious event itself. If an intrusion did not cause any obvious damage, a company or even a government agency may decide to ignore it, or perhaps to improve its defenses generally but not launch an expensive investigation into the origins . . . .”).
security division, it is particularly vexing when a large outlay of resources yields “little more than vague accusations that the guilty parties (might be) working for a particular foreign government or cyber gang.”  

B. Building an Attribution Infrastructure

Attribution infrastructures help manage the characteristics associated with an entity and consist of four components:

[1] a set of entities (actors) having an interest in attribution with respect to a transaction;
[2] a set of data to be attributed;
[3] the level of assurance with which values of attributes can be determined, and with which they can be associated with an entity; and
[4] a policy negotiation engine that actors use to negotiate an acceptable set of attributes and levels of assurance . . .

---

48 See id. (emphasis added).
These components reflect a particular socio-technological interest, based on the dynamic needs of an actor. In turn, this infrastructure provides an organizational benefit to investigators in unpacking the architecture of an attack.\(^{49}\) Another way to conceptualize this, as promulgated by Rid and Buchanan, is to apportion attribution needs based on the three levels of military planning: “The \textbf{tactical} goal is understanding the incident primarily in its technical aspects, the \textit{how}. The \textbf{operational} goal is understanding the attack’s high-level architecture and the attacker’s profile — the \textit{what}. The \textbf{strategic} goal is understanding who is responsible for the attack, assessing the attack’s rationale, significance, appropriate response — the \textit{who} and \textit{why}.\(^{50}\) The next section outlines the different modalities of attribution.

1. Pick-Your-Flavor Attribution

Despite attribution’s import on state behavior, the word ‘attribution’ is only afforded one sentence in the Obama Administration’s 2009 \textit{Cyber Policy Review Report}.\(^{51}\) And although the Department of Defense’s 2015

\(^{49}\) See Rid and Buchanan, \textit{supra} note 6 at 10.
\(^{50}\) See id. (emphasis added).
\(^{51}\) See \textit{U.S. White House Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure} (2009), available at https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (“Architecture: Addresses the performance, cost, and security characteristics of existing information and communications systems and infrastructures as well as strategic planning for the optimal system characteristics that will be needed in the future. This element includes standards, identity management, authentication and \textbf{attribution}, software assurance, research and development,
Cyber Strategy Report does address the attribution challenge in greater detail than the 2009 Cyber Policy Review Report, the former provides only a fleeting glimpse into two classes of attribution, public and private.\textsuperscript{52} This is remarkable considering that attribution is not a ‘plain vanilla’ construct, but comes in a variety of ‘flavors’ or – design requirements – such as: (1) “perfect non-attribution,” (2) “perfect attribution,” (3) “perfect selective attribution” (4) “entity non-attribution, (5) “false attribution,” (6) “imprecise attribution, and (7) “unconcern.”\textsuperscript{53} These relationships are modeled on the seven attribution modalities identified by Bishop, Gates and Hunker.\textsuperscript{54} The following model (Figure 1) underscores the principle that attribution is neither inherently good, nor bad, but its utility is based on the dynamic needs of a state.\textsuperscript{55}

\textbf{Figure 1}

procurement, and supply chain risk management.”) (emphasis added).
\textsuperscript{52} See The U.S. Department of Defense Cyber Strategy, supra note 14 at 20 (“Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack. Public and private attribution can play a significant role in dissuading cyber actors from conducting attacks in the first place. The Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution. This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time.”)
\textsuperscript{53} See Bishop et. al., supra note 4.
\textsuperscript{54} See id.
\textsuperscript{55} See id. (explaining that “[t]he target of attribution may differ depending on the need of the stakeholder. In some cases it might be necessary to attribute a message to a particular individual, while in other cases, only to a specific computer, IP address, or organization.”)
<table>
<thead>
<tr>
<th><strong>PERFECT NON-ATTRIBUTION</strong></th>
<th>“[I]n which attribution is not possible;”&lt;sup&gt;56&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PERFECT ATTRIBUTION</strong></td>
<td>“[I]n which the attributes of both the sender and recipient are known to both parties.”&lt;sup&gt;57&lt;/sup&gt;</td>
</tr>
<tr>
<td><strong>PERFECT SELECTIVE ATTRIBUTION</strong></td>
<td>“[I]n which one entity wants certain attribute-value pairs known to some entities but not others;”&lt;sup&gt;58&lt;/sup&gt;</td>
</tr>
<tr>
<td><strong>ENTITY NON-ATTRIBUTION</strong></td>
<td>“[I]n which an entity wants attribute-value pairs known but not that they are bound to that entity;”&lt;sup&gt;59&lt;/sup&gt;</td>
</tr>
<tr>
<td><strong>FALSE ATTRIBUTION</strong></td>
<td>“[I]n which the recipient can determine attributes of the message but the data, while consistent, is inaccurate;”&lt;sup&gt;60&lt;/sup&gt;</td>
</tr>
<tr>
<td><strong>IMPRECISE ATTRIBUTION</strong></td>
<td>“[I]n which the recipient can eventually attribute data accurately and to the precision needed, but to do so takes too long (so the knowledge is useless or redundant) or costs more than the value of knowing the attribution.”&lt;sup&gt;61&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

---

<sup>56</sup> See id.

<sup>57</sup> See id.

<sup>58</sup> See id.

<sup>59</sup> See Bishop et. al., supra note 4.

<sup>60</sup> See id.

<sup>61</sup> See id.
These modalities capture an actor’s distinct set of preferences and concerns, which may exist in conflict with one another. For instance, while the perpetrator of a hostile cyber act (e.g. a denial of service attack against State X’s central financial bank) may desire perfect non-attribution, victim State Y would desire perfect attribution. From State Y’s perspective, attributing a malicious cyber act to an actor allows it to better position itself to implement proscriptions against the aggressor and/or respond offensively. To that end, Professor Hollis reasons that “by attributing a cyberattack to a particular individual (or military) proscriptions endeavor to remedy past harms and deter future attacks.”

While it is tempting to decry a victim state’s inability or difficulty in expediently attributing a cyber act (e.g. an imprecise attribution situation), one can imagine instances wherein false attribution strategically misleads an adversary, to gain an informational advantage about a target’s tactics, techniques, and procedures. For instance, with the 2015 cyber attack on the Ukranian power grid, while the attack appears to have originated from Russia, it is still unknown who precisely is at fault, given that

62 See id.
63 See Hollis, supra note 10 at 377 (“Categorizing a cyberattack as cybercrime, cyberwar, or ever cyberterrorism, requires knowing which type of actor was responsible. A cyberattack by a criminal organization, for example, falls under the mantle of cybercrime.”)
64 See id. (internal citation omitted here).
Internet Protocol (IP) addresses can be spoofed. Apart from IP spoofing, cyber malefactors can also obscure their true identities through the ‘timeless magic’ of political subterfuge. This type of concealment, as described in the DoD 2015 *Cyber Strategy Report*, states that because “[s]tate and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation.”

Additionally, drawing on the notorious 2014 cyber hack of *Sony Pictures Entertainment* by an alleged North Korean faction, Morgan Marquis-Boire opined “[t]here’s a good reason that the U.S. government would not reveal much about why it explicitly blamed North Korea” for the attacks. Marquis-Boire acknowledged that a cyber actor might purposefully employ less sophisticated attack methods to not “tip their hand regarding the full extent of their capabilities,” and effectively leverage false attribution tactics. In summary, the normative value placed on attribution is based on the actors’ individual preferences and aversions based on the surrounding political circumstances.

---

67 See *id*.
68 See *id*.
2. Finding the Pieces to Solve the Puzzle

Just as each physical crime scene is processed according to an investigative protocol, digital crimes are subject to a rigorous forensic examination process: “At a very basic level, computer forensics is the analysis of information contained within and created with computer systems, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved.”

According to New York Computer Forensics, a company that specializes in digital forensics and information security, computer forensics deals with three main categories of data:

[1] **Active Data** is the information that we can actually see. This includes data files, programs, and files used by the operating system. This is the easiest type of data to obtain.

[2] **Archival Data** is data that has been backed up and stored. This could mean backup tapes, CDs, floppies, or entire hard drives.

[3] **Latent Data** is the information that one typically needs specialized tools to access. An example of latent data would be information that has been deleted or partially overwritten.”

---

69 See id.


71 See id.
Attributing a hostile cyber act can require analyzing data in one or all of these three areas. Although there is no single method to attribute the identity of a cyber actor, a combination of approaches can be employed to traceback an Internet Protocol (IP) address. The traceback method “was originally designed to determine the originating IP address for spoofed packets in a denial-of-service attack[.]” Other methods include digital fingerprinting and machine learning which serves to “automate the matching of coders with their creations.”

C. The Legal Calculus for Self-Defense

In terms of the impact of attribution on foreign relations, some military theorists have come to regard it as “a key legal, tactical, and technical requirement, and must be performed before a nation executes self-defense activities.” For questions relating to uses of force, “attribution is an essential consideration to the overall legal

---

72 See id.
73 See Hacker High School, Security Awareness for Teens, Complete: Table of Contents and Glossary, INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (defining an IP address as “[a]n identifier for a computer in the internet or on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 61.160.10.240 could be an IP address.”)
74 See Bishop et al., supra note 4.
75 See Greenemeier, supra note 39 (explaining that digital fingerprints “identify a particular program’s formatting styles, how it allocates memory, the ways it attempts to avoid detection and other attributes.”)
76 See id.
77 See Mudrinich, supra note 11 at 172.
calculus in analyzing the scope and magnitude of a hostile cyber act.”  

Article 2(4) expressly prohibits states from employing a “threat or use of force” against another member state: “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”  In military parlance, a “use of force” is regarded as an armed attack. The United Nations (“UN”) Charter does not, however, expressly define what constitutes a “use of force.” As a result, the exact parameters for interpreting a “use of force” in cyberspace has sparked heated discussions across the international legal community. Even the term “cyber attack,” as the Tallinn Manual notes, requires precision of language if it is being invoked to trigger Article 2(4).

---

78 See id.
81 See Catherine Lotrionte, Symposium: International Law and the Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolution fueled by Social Media: State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights, 26 EMORY INT’L L. REV. 825, 828 (“[I]nternational law on the use of force, its content, application, and effectiveness in dealing with the cyber threats has been the object of much debate. . . . If consensus on the rules related to the use of force in cyberspace is not achieved, the result will be a self-help system within the cyber domain with potential spillover into the kinetic sphere.”)
The *Tallinn Manual* defines a cyber attack as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”\(^8^2\) Although this definition is akin to a military definition of a kinetic attack, it is less clear how a denial-of-service attack, or other intentional disruption of network activity, should be categorized.\(^8^3\) For instance, how should operations that target the informational integrity of military personnel databases and financial institutions be regarded under this framework?\(^8^4\) Should these acts be categorized as an “armed attack,” or does it implicate a lower threat threshold standard, such as a cyber intrusion. Cyber intrusions, as defined by Professor Gary Solis, an expert on the law of war at Georgetown University, are precursors to a cyber attack.\(^8^5\)


\(^8^3\) *See Robin Gei, The Conduct of Hostilities in and via Cyberspace*, 104 ASIL 371, 372 (201).


\(^8^5\) *See Lecture on The Law of War by Dr. Gary D. Solis at the UC Davis School of Law*, (Nov. 14, 2013), *recording available at* http://mediasite.ucdavis.edu/mediasite/Play/ba6d0c01f639420e9ed39faa6be743761d.
Apart from the UN Charter, other theorists have advocated for a new conflict resolution framework, because “[t]he attribution problem makes cyberspace so different from other mediums or domains that is requires an entirely new international law approach.”86 With regard to how the Obama Administration views hostile acts in cyberspace, the 2011 *White House International Strategy Report for Cyberspace* states:

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.87

For the purposes of this essay, however, which primarily focuses on cyber economic espionage, the term ‘attack’ shall hereafter refer to U.S. National Initiative for Cybersecurity Careers and Studies (NICCS) definition of an attack as an “attempt to gain unauthorized access to


system services, resources, or information, or an attempt to compromise system integrity.”

1. The Inherent Right of Self-Defense

An important limitation on Article 2(4)’s restrictions on the use of force, however, is the right to self-defense, as enumerated in Article 51. Article 51 reads in part that “[n]othing 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.” This provision applies to the right of individual self-defense and collective self-defense. Further, the 2015 Department of Defense Law of War Manual recognizes that under customary international law, all states have the right to defend themselves in response to imminent attacks.

Central to a state’s right to a use of force, however, is that “the state must possess the ability to adequately attribute responsibility for such attack to another state or

89 See U.N. Charter Article 51.
90 See id.
91 See id.
92 See Department of Defense Law of War Manual, June 2015, p. 47 (“Under customary international law, States had, and continue to have, the right to take measures in response to imminent attacks. Under customary international law, States had, and continue to have, the right to take measures in response to imminent attacks.”)
group of actors. A victim state cannot lawfully launch a response \textbf{without knowing the identity of the attacker.}''\textsuperscript{93}

2. Cyber Crime & Espionage—A Different “Use of Force” Parameter?

Apart from \textit{The Tallinn Manual’s} treatment of cyber attacks, how are “unfriendly acts by states,” (\textit{e.g.} acts of espionage and economic coercion), treated under the UN Charter?\textsuperscript{94} In February 2016, President Obama authored an op-ed piece in the \textit{Wall Street Journal}, wherein he described cyberthreats as “among the most urgent dangers to America’s \textbf{economic} and \textbf{national security.}”\textsuperscript{95} Despite the prevalence of cyber threats to states’ economic security, however, Professor Lotrionte notes that, “the international laws that control state uses of force . . . do not regulate crime or espionage.”\textsuperscript{96} The international community does not regard acts of “non-military techniques of coercion,” such as espionage, economic coercion, and psychological warfare tactics, as illegal uses of force \textit{per se}, “but instead as violations of the principle of nonintervention.”\textsuperscript{97}

\textsuperscript{93} See Mudrinich, \textit{supra} note 11 at 193 (emphasis added ).

\textsuperscript{94} See Beard \textit{supra} note 5 at 117 (explaining that “the consensus that emerged in framing the U.N. Charter, despite the objections of a small number of states, was that Article 2(4) should not be extended to include some important and damaging actions states may employ against each other, including acts involving destructive economic coercion.”)


\textsuperscript{96} See Lotrionte, \textit{supra} note 72 at 839.

\textsuperscript{97} See Beard, \textit{supra} note 5 at 118 (internal citation omitted).
The principle of nonintervention is reflected in the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States, section 3, paragraph 1:

No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.  

Here, if cyber economic espionage is indeed a threat against a state’s “political, economic and cultural elements,” then it stands to reason that it violates the principle of non-intervention.

---

D. The Enforcement Paradox to Law and Order in Cyberspace

Under Article 51 of the U.N. Charter, all states have an inherent right to defend themselves “if an armed attack occurs against a Member of the United Nations[.]”99 Yet from a legal standpoint, a state’s inability to attribute an attack, even with reasonable certainty, poses significant challenges to successfully invoking the right to self-defense. Attribution therefore carries “profound implications for the practicality of using law to respond to cyber threats. It becomes difficult to know which set of proscriptions—crime, war, or terrorism—applies. Dangerous consequences may result if hackers and victims apply different regimes.”100 This enforcement paradox, as summarized by Professor Hollis, exists in cyberspace as “[g]overnments look to discourage unwanted cyberthreats by identifying and holding publicly accountable violators among those regulated. But those who want to remain unidentified online can almost always do so.”101

As a result, should international law be completely jettisoned in cyberspace? According to former U.S. Secretary of State, Madeleine K. Albright (1997-2001), a self-described “optimist who worries a lot,”102 the answer would likely be a resounding no. In Secretary Albright’s book, The Mighty and The Almighty: Reflections on

100 See Hollis, supra, note 4 at 378.
101 See id. at 391.
America, God, and World Affairs, she reasons that while countries often do take action outside of the charter’s guidelines, [d]espite such violations, the standards in the charter remain relevant, just as laws against murder remain relevant even though murders are still committed.”103 Similarly, for Assistant Attorney General for National Security John Carlin, theft is theft, regardless of the domain, and the U.S. “will hold state-sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws.”104

To other idealistic theorists like John Perry Barlow, however, a state’s purported need to attribute hostile cyber acts in order to implement proscriptions against the offender, is an inane notion. In Barlow’s 1996 A Declaration of the Independence of Cyberspace, he reasons:

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there in no matter here. Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion.105

104 See id.
Barlow theorizes that the only rule of law applicable in cyberspace is the Golden Rule. The Golden Rule, as promulgated in the Book of Matthew, Chapter 7 verse 12, reads: “So whatever you wish that others would do to you, do also unto them, for this is the Law and the Prophets.” It is Barlow’s ideal that the denizens of cyberspace apply the Golden Rule in their digital interactions.

In theory, a ‘cyber Golden Rule’ is certainly a laudable goal to aspire to. In practice, however, one need only look to recent headlines about hostile cyber acts such as the Estonian cyber attack in 2007, the deployment of the Stuxnet worm, and attack on a portion of the Ukrainian power grid in 2015, to apprehend the sagacity

---

106 See id. (“The only law that all our constituent cultures would generally recognize is the Golden Rule.”)
107 See Matthew 7:12.
108 See Barlow, supra note 98.
109 See Beard, supra note 5 (explaining that “[w]hile many observers alleged that the hostile cyber actions taken against Estonia in 2007 were directed or sponsored by the Russian government, the origin of these actions, their geographic nexus, and the identity of the responsible parties remain unknown.”)
110 See Mudrinich, supra note 11 (explaining that “[t]he advent of worms like Stuxnet has demonstrated that actors within the global digital environment possess the capability to “weaponized” software code. . . . Nations, their militaries, and their economies are vulnerable to ever sophisticated cyber threats.”).
111 See Shane Harris, CIA Eyes Russian Hackers in ‘Blackout’ Attack, THE DAILY BEAST, (Jan. 6, 2016), http://www.thedailybeast.com/articles/2016/01/06/exclusive-cia-eyes-russian-hackers-in-blackout-attack.html (last visited Jan. 23, 2016) (explaining that on December 23, 2015, “a large area of the country had been left without electricity due to “interference” in its systems. Approximately 700,000 homes were without power for several hours. If the blackout is positively attributed to the work of hackers, it will be
of Yogi Berra’s remark “in theory, there is no difference between theory and practice. But in practice, there is.”

1. Imputed State Responsibility

The attribution challenge is not entirely without its own unique solutions, designed to mitigate the harmful effects of hostile cyber acts. For instance, the laws of state responsibility, as promulgated under the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, have been cited as a potential remedy to the attribution challenge. Specifically, Article 2 of the Draft Articles lists the elements of an internationally wrongful act of a State as:

There is an internationally wrongful act of a State when conduct consisting of an action or omission:

(a) is attributable to the State under international law; and
(b) constitutes a breach of an international obligation of the State.

the first documented case of a cyber attack on an electrical power facility that led to a loss of electricity. While hackers are suspected of having caused a blackout at least once in the past, there has never been a publicly confirmed case with technical data to back it up.”


See Mudrinich, supra note 11 at 193 (noting that “[i]mputed attribution can be used against states that harbor or allow attacks from with their borders.”)

To theorists like U.S. Air Force Major Erik M. Mudrinich, the concept of imputed state responsibility in cyberspace is “based on a state’s violation of what is viewed as an established duty to prevent one’s territory from being used as a haven or sanctuary for those launching terrorist or cyber attacks.” Essentially, imputed state responsibility is a standard duty of care owed by all states to one another. A breach of this duty occurs when a state routinely “fails to undertake measures to prevent or legally respond to these attacks.” The doctrine of imputed state responsibility is not, however, a panacea, and may indeed operate better under certain attribution frameworks than others.

Rather than develop a solution to the attribution problem, a common counterargument is that “developing a solution to the attribution problem is just a waste of time and resources—instead, the nation should focus on network


115 See Mudrinich, supra note 11 at 193.


117 See Mudrinich, supra note 11 at 193.
resiliency and redundancy.”118 While network resiliency issues also deserve attention, to completely disregard the impact of attribution on applying the law of armed conflict in cyberspace and customary international law at large, is akin to pigheadedly taking one’s kickball from the schoolyard and going home in protest. Such a defeatist attitude is injurious to both state security and the stability of foreign relations. In sum, the zero-sum mentality of the attribution challenge is not the type of prescient thinking that the twenty-first century needs. The following section discusses the theoretical, as well as historical distinctions, between economic intelligence collection activities and acts of economic espionage.

II. ESPIONAGE - A HISTORICAL OVERVIEW

“There is nothing new under the sun.”
(Ecclesiastes 1:9)

While ‘spying’ may strike some as indecorous state behavior, it is essentially akin to a bodily function that is necessary to sustaining the health of the body politic. To that end, all states perform some form of intelligence collection and analysis against one another.119 Often referred to as the ‘world’s second oldest profession,’ scholars have chronicled the early beginnings of spying and intelligence activities as far back as biblical times.120

118 See id. at 194.
119 See Peter K. Yu, Trade Secret Hacking, Online Data Breaches, and China’s Cyberthreats, CARDozo L. Rev. de Novo 130, 141 (2015) (“all governments conduct surveillance and intelligence activities.”)
120 See Watson, Ronald E., "Spying: A Normative Account of the
Intelligence, according to A. John Radsan, a law professor at William Mitchell College of Law, “can be divided into two basic categories: collection and analysis.”\textsuperscript{121} As noted by Mark Lowenthal in *Intelligence: From Secrets to Policy*, intelligence exists in a variety of forms:

Most people tend to think of intelligence in terms of military information—troop movements, weapons capabilities, and plans for surprise attack, the first reason for having intelligence agencies—but it is not the only one. Many different kinds of intelligence ([1] political, [2] economic, [3] social, [4] environmental, [5] health, and [6]... 

---

\textsuperscript{121} See A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 *Michigan Journal of International Law*, 597, 599 (2007) (noting that “[t]his division corresponds with the two main sections at the Central Intelligence Agency: the Directorate of Operations and the Directorate of Intelligence. A ‘case officer’ in the Directorate of Operations collects the intelligence and an “analyst” from the Directorate of Intelligence synthesizes intelligence that has been collected.”)
For the purposes of this essay, I collectively refer to these six bases, as traditional espionage. According to Dr. Catherine Lotrionte of Georgetown University Law Center, “espionage is one aspect of a nation’s intelligence work, encompassing the government’s efforts to acquire classified or otherwise protected information in order to deal with threats from actual or potential adversaries.”

A. Espionage and the Law of War

But during times of war, is state-sponsored espionage lawful under international law? The U.S. Army Judge Advocate General’s Corps General Legal Center and School maintains that espionage is implicitly recognized as lawful under international law. In the 2009 *U.S. Army

---

124 See US Army JAG Corps 2009 *Law of War Documentary Supplement*, (quoting Executive Order 12333, United States Intelligence Activities (Dec. 4, 1981) (“The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law. Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President. (d) Special emphasis should be given to detecting and countering: (1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests.”))
JAG Corps Law of War Documentary Supplement it states that Articles 24 and 29 of the Hague Regulation “tacitly recognize the well-established right of belligerents to employ spies and other secret agents for obtaining information of the enemy. Resort to that practice involves no offense against inter-national law. Spies are punished, not as violators of the laws of war, but to render that method of obtaining information as dangerous, difficult, and ineffective as possible.”

But is peacetime espionage lawful under international law? For Roger Scott, an international relations theorist, “[e]spionage is not prohibited by international law as a fundamentally wrongful activity.” While peacetime espionage is a contentious area in academia, attorney Robert D. Williams opines that “espionage is a practice that states have long engaged in and acknowledged as a matter of practical reality.”

125 See Yale Law School, The Avalon Project, Laws of War: Laws and Customs of War on Land (Hague IV); October 18, 1907, http://avalon.law.yale.edu/20th_century/hague04.asp#art24 (“Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible.”) (last visited Feb. 4, 2016).
1. The Lieber Code of 1863

With regard to espionage performed during times of war, the Lieber Code of 1863 recognized spies as a condition of war and accordingly set forth strict punishments (often in the form of death)\(^\text{129}\) for captured spies.\(^\text{130}\) During the American Civil War, President Abraham Lincoln appointed political theorist, Francis Lieber, to draft a new code of war.\(^\text{131}\) Following its formal adoption by the U.S. Army in 1863, the Lieber Code became a foundational core for other foreign treaties and military codes.\(^\text{132}\) But how is espionage viewed under the Lieber Code? Pursuant to Article 88, a spy is defined as “a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy.”\(^\text{133}\)

2. Peacetime Espionage

In Professor Radsan’s opinion, the following quotation by Richard A. Falk,\(^\text{134}\) a former U.N. Human

\(^{129}\) See LIEBER CODE ART. 88 (“The spy is punishable with death by hanging by the neck, whether or not he succeed in obtaining the information or in conveying it to the enemy.”)

\(^{130}\) See Todd, supra note 76, at 94 (reasoning that spying does not violate the fundamental laws of war, because it “was first recognized in the Lieber Code in 1883.”)


\(^{132}\) See id.

\(^{133}\) See LIEBER CODE ART. 88.

\(^{134}\) See Richard Falk, THE NATION,
Rights Special Rapporteur, best encapsulates the treatment of peacetime espionage under international law: “[t]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture.”\(^{135}\)

With respect to the Hague Conventions, specifically Hague Convention IV of 1907, Article 29 reads:

A person can only be considered a spy when, acting clandestinely or on false pretenses, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party.

Thus, soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies. Similarly, the following are not considered spies: Soldiers and civilians, carrying out their mission openly, entrusted with the delivery of despatches intended either for their own army or for the enemy's army. To this class belong likewise persons sent in balloons for the purpose of carrying despatches and, generally, of maintaining communications between the

different parts of an army or a territory.\textsuperscript{136}

In terms of global efforts made to regulate spying, like automated forms of surveillance, the Wassenar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies,\textsuperscript{137} is the main international agreement.\textsuperscript{138} As noted by Foreign Policy journalist James Bamford, the Wassenar Arrangement “allows for regulating spying of conventional weapons and dual-use goods and technologies. But it is nonbinding on its 41 signatories, including the United States, and Israel has never formally agreed to its terms.”\textsuperscript{139} While there is a robust debate over whether peacetime espionage is lawful under international law, the predominant practice of states


\textsuperscript{137} See The Wassenaar Arrangement, About Us, http://www.wassenaar.org/about-us/ (last visited Feb. 7, 2016) (“The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.”)

\textsuperscript{138} See James Bamford, The Espionage Economy, FOREIGN POLICY (Jan. 22, 2016).

\textsuperscript{139} See id.
has been to implicitly accept this behavior and conduct intelligence collection activities.\(^{140}\)

B. \textit{Differences between Economic Intelligence and Economic Espionage}

Economic intelligence, according to Dr. Lotrionte, comprises “national gross domestic product and inflation rate figures, as well as more privileged information, kept secret by many states and therefore the target of foreign intelligence services, such as budgetary allocations for defense, and national research and development expenditures.”\(^{141}\) In turn, this type of intelligence helps enable policymakers in chartering national security and homeland security matters, including but not limited to “whether to raise the interest rates, what position to take in trade negotiations, in assessing the economic capability of a potential military adversary, or following the developments affecting the flow of vital strategic resources.”\(^{142}\)

Economic espionage is different from economic intelligence, however, because the former entails “providing such information to the collecting state’s own private entities to gain economic advantages.”\(^{143}\)

Further, the U.S. Economic Espionage Act (EEA), enacted on October 11, 1996, adds clarity here by defining what acts constitute economic espionage: “(1) whoever


\(^{141}\) See Lotrionte, \textit{supra} note 116, at 463-64 (internal citation omitted here).

\(^{142}\) See \textit{id.} at 464.

\(^{143}\) See \textit{id.}. 


knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent.”  

Not only does the EEA regulate misconduct in the U.S., but as Congressional Research Services legislative attorney Jennifer K. Elsea points out, the statute also applies to “the activities of foreign nationals overseas, at least when they take an active part in seeking out information.” Elsea explains that the EEA’s language regulates “the receipt and unauthorized dissemination of national defense information, which has been interpreted broadly to cover closely held government materials related to U.S. military operations, facilities, and personnel.”

With regard to industrial espionage, the Federal Bureau of Investigation (FBI) classifies this as the theft of trade secrets. Pursuant to Title 18 U.S.C. § 1832, theft of trade secrets is “(1) whoever knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to (2) knowingly benefit anyone other than the owner.” Pursuant to § 1831, the penalty violation can


146 See id.


include a fine of no more than $5,000,000 or a prison sentence no more than 15 years, or both.\textsuperscript{149} At the organizational level, the punishment is a fine “not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.”\textsuperscript{150}

\textit{C. An American Perspective}

Cyber economic espionage is deleterious to a state because it “target[s] companies’ business strategies and plans, intellectual property, and expensive research and development projects, eroding their competitive advantage in the international market place and placing the acquirer an unfair leap ahead on technological developments.”\textsuperscript{151} A generally good rule of thumb for discerning economic espionage is to examine whether the intelligence at issue is being used to impart a commercial competitive advantage to benefit the home state’s industries or companies.

According to FireEye, a U.S. network security company, “67\% of victims learn they are breached from a third party.”\textsuperscript{152} While such statistics are helpful in internalizing the high prevalence rate of online data breaches, an exact figure on cyber espionage incidents, as

\footnotesize{\textsuperscript{149} See 18 U.S.C. § 1831.  
\textsuperscript{150} See id.  
\textsuperscript{151} See Lotrionte, supra note 116, at 452.  
InfoSec Institute conceded, is incalculable.\textsuperscript{153} The Institute’s reasoning is that “[p]rivate companies and governments often do not report losses because in many cases, they aren’t able to detect the attacks. When the cyber espionage campaigns are discovered, information on them may be kept secret for fear of brand and/or reputation damage, company devaluation and loss of public confidence.”\textsuperscript{154}

In 2012, former National Security Agency (NSA) Director, General Keith Alexander, described economic espionage as the “greatest transfer of wealth in history,” and explained to the American Enterprise Institute that “investigations by the FBI and other agencies find that for every company that detects a cyberattack there are 100 others that are unknowingly being hacked.”\textsuperscript{155} In terms of states that have been identified as having conducted economic espionage against the U.S., the list includes “China, South Korea, Japan, France, Russia, Israel, and Germany” – to name a few.\textsuperscript{156} In 2013 the U.S. National Intelligence Estimate announced “France, alongside Russia and Israel, to be in a distant but respectable second place behind China in using cyberespionage for economic gain.”\textsuperscript{157} In comparison, the U.S. does not conduct commercially motivated cyber espionage.\textsuperscript{158}

\textsuperscript{154} See id.
\textsuperscript{155} See id.
\textsuperscript{156} See Lotrionte, supra, note 116, at 468.
The FBI estimates that this threat “costs the American economy hundreds of billions of dollars per year and puts our national security at risk.” Although this threat is not new to modern times, as more industries digitize their sensitive commercial information and/or migrate to employing smart technology in their enterprise, the attack surface area also increases. In terms of financial loss, U.S. News reported in 2013 that the “price tag for intellectual property theft from U.S. companies is at least $250 billion a year. That's far more than what businesses pay in federal corporate income taxes.”

D. Definitional Distinctions and Principles

As previously stated, the U.S. does not practice economic espionage. An important caveat, however, as

---

158 See Lotrionte, supra, note 116, at 465 (“U.S. intelligence agencies do not collect the trade secrets of foreign corporations and provide those secrets to U.S. Companies.”)
160 See generally id. (“While it is not a new threat, it is a growing one, and the theft attempts by our foreign competitors and adversaries are becoming more brazen and more varied in their approach. The FBI estimates that hundreds of billions of U.S. dollars are lost to foreign competitors every year. These foreign competitors deliberately target economic intelligence in advanced technologies and flourishing U.S. industries.”)
identified by American journalist, Ronald Kessler in *Inside the CIA* is that “[t]he CIA has always tried to obtain the negotiating positions of other countries before arm talks or trade talks begin. Like the problem of weapons proliferation, economic matters have been given higher priority by the CIA since the end of the Cold War.”\(^{162}\) Kessler points out that the boundary lines between state secrets and trade secrets can become nebulous, for “[w]hile the CIA cannot be in the position of handing over commercial secrets to selected American companies, it can pass the information along to the Commerce Department so that it can issue broad guidance to all companies. For example, the Commerce Department might issue an advisory on the direction of the Japanese computer industry.”\(^{163}\)

As such, is this a contradiction in principles, or simply a form of economic intelligence? For Kessler, state action in enhancing trade talks and the negotiation process would likely fall under the scope of permissible economic intelligence collection. The following section, however, will examine the scope of impermissible economic espionage by China against the U.S.

III. ECONOMIC SECURITY RELATIONS BETWEEN THE U.S. AND CHINA

In terms of China’s projected defense spending plans for 2016, *Lawfare* reporter John Lee postulates that the Chinese Communist Party (CCP) seems determined and able to increase defense spending by double-digit rates


\(^{163}\) *See id.*
irrespective of national economic performance.\textsuperscript{164} Ian Bremmer offered a similar forecast in \textit{TIME}, in describing the top five geopolitical risks of 2016: “The recognition in 2016 that China is both the most important and the most uncertain driver of a series of global outcomes will increasingly unnerve other international players who aren’

As noted by Williams University Law Professor Zoe Argento, “[t]he Chinese government, and to a lesser degree, the Russian government, encourage and in some cases, directly participate in the appropriation of other countries’ technologies and business information.”\textsuperscript{166} Apart from China’s stance on economic espionage, the Russian government avers that “intelligence collection serves the goal of developing Russian science and technology for economic purposes.”\textsuperscript{167}

\textit{A. Advanced Persistent Threat I}

According to the FBI’s Counterintelligence: Economic Espionage Homepage, there are three main


\textsuperscript{167} \textit{See id. at} 194 (internal citation omitted here).
avenues in which foreign entities can wage economic espionage against the U.S.:

1. Aggressively target present and former foreign nationals working for U.S. companies and research institutions;
2. Recruit and perform technical operations to include bribery, discreet theft, dumpster diving (in search of discarded trade secrets) and wiretapping; and,
3. Establish seemingly innocent business relationships between foreign companies and U.S. industries to gather economic intelligence including proprietary information.¹⁶⁸

The Mandiant Report on *Exposing One of China’s Cyber Espionage Units* is a helpful guide to understanding the harmful ramifications of some of these methods in practice. Advanced Persistent Threat One (APT1), is “believed to be the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).”¹⁶⁹ According to Mandiant, Unit

---

¹⁶⁹ See Mandiant, APT 1 Exposing One of China’s Cyber Espionage Units, MANDIANT,
61398 has a long-standing history of stealing the following categories of information from foreign companies:

- product development and use, including information on test results, system designs, product manuals, parts lists, and simulation technologies; manufacturing procedures, such as descriptions of proprietary processes, standards, and waste management processes; business plans, such as information on contract negotiation positions and product pricing, legal events, mergers, joint ventures, and acquisitions; policy positions and analysis, such as white papers, and agendas and minutes from meetings involving high-ranking personnel; emails of high-ranking employees; and user credentials and network architecture information.\textsuperscript{170}

In terms of Unit 61398’s \textit{modus operandi}, Mandiant reports that once Unit 61398 infiltrates a network, “they repeatedly monitor and steal proprietary data and communications from the victim for months or even years. . . [and] [t]he longest time period APT1 maintained access to a victim’s network was at least 1,764 days.”\textsuperscript{171}

\textbf{B. Case Studies on Chinese Economic Espionage}

But the story of APT1 does not end here. In 2014 the U.S. Justice Department publicly issued the indictments of five members of Unit 61398 for committing acts of

\textsuperscript{170} See id.
\textsuperscript{171} See id.
economic espionage and computer hacking.\textsuperscript{172} In May 2014 the FBI announced that from “2006-2014, defendants Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People’s Liberation Army, were allegedly involved a hacking conspiracy that targeted Westinghouse Electric Co.; U.S. subsidiaries of SolarWorld AG; United States Steel Corp.; Allegheny Technologies Inc.; the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union; and Alcoa, Inc.”\textsuperscript{173} Prior to the 2014 indictments, however, another incident of economic espionage, committed by China against the U.S., known as Operation Aurora, garnered international attention.\textsuperscript{174}

1. Operation Aurora

From 2009 to 2010, Google and 34 other companies fell victim to an intricate Chinese economic espionage operation.\textsuperscript{175} In 2010, Google publicly acknowledged that a sophisticated adversary, with connections to China, had attacked them.\textsuperscript{176} According to \textit{Help Net Security}, this theft

\begin{footnotesize}
\begin{enumerate}
\item See id.
\item See Schwartz, \textit{supra} note 17.
\item See id.
\end{enumerate}
\end{footnotesize}
of intellectual property was enabled when “a flaw in the Internet Explorer browser was exploited to insert malware which drop[ped] a backdoor program in the targeted systems and networks.”\textsuperscript{177} \textit{InfoSec Institute} also reported that apart from harming Google, Operation Aurora targeted “dozens of organizations operating in various sectors, including Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical.”\textsuperscript{178}

While Operation Aurora featured the large-scale theft of intellectual property, the attack on Google’s Gmail account system may also have been waged with the intent to gather intelligence against Chinese dissidents.\textsuperscript{179} Overall, this operation served as a wake up call to American businesses and policy makers about the “espionage-by-malware” threat.\textsuperscript{180}

\textsuperscript{177} See Zeljka Zorz, Operation Aurora Malware Investigated, (February 10, 2010), https://www.helpnetsecurity.com/2010/02/10/operation-aurora-malware-investigated/

\textsuperscript{178} See id.

\textsuperscript{179} See id. (“Indeed, taking into consideration the thriving global underground economy that sprung up around malware and data theft, and the considerable money-hungry hacking subculture existing in China, it is likely that the ultimate goal was money. In Google’s case, it’s possible that the compromise of Gmail accounts belonging to Chinese dissidents served to throw the investigators off the scent of the real culprits.”)

2. The Three-Year Breach of U.S. Defense Contractor QinetiQ

In terms of recent allegations of economic espionage by China, the Headlines & Global News reported on January 18, 2016, the U.S.-China Economic and Security Review Commission began “looking into the possibility that China hacked into a defense contractor for the Pentagon in order to steal secret robot plans” between 2007 and 2009. Initial investigation efforts of this attack on military software systems have thus far been tracked back to Unit 61398.

The attack was perpetrated against QinetiQ North America, a military gadget manufacturer, whose “parent firm is the storied company that inspired Q’s lab in the James Bond thrillers.” Bloomberg Business dubbed this three-year breach of QinetiQ records as a ‘major embarrassment’ that “jeopardized the company’s sensitive technology involving drones, satellites, the U.S. Army’s combat helicopter fleet, and military robotics, both already-deployed systems and those still in development[].” But why did China engage in cyber economic espionage here?

182 See id.
183 See id.
The underlying motivation for the Chinese attack, as posited by former CIA director Michael Hayden, was to reap the benefits of billions of dollars of research on advanced U.S. warfare technology without incurring the actual costs.\textsuperscript{185}

Other theorists have similarly noted that in the case of China, “stealing intellectual property and proprietary information is much more cost-effective than investing in lengthy R&D programs.”\textsuperscript{186} In November 2012 the U.S.-China Economic Security Review Commission’s Annual Report revealed to Congress that “China apparently uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on U.S. strategies and plans, enable future military operations, shorten research and development (R&D) timelines for military

\textsuperscript{185} See id. (“The spying on QinetiQ and other defense contractors appears aimed at helping China leapfrog the U.S.’s technologically-advanced military, foregoing years of research and development that would have cost billions of dollars, according to Michael Hayden, former director of the CIA.”)

technologies, and identify vulnerabilities in U.S. systems and develop countermeasures.”

Another example of China engaging in intellectual property theft involves Chinese businessman, Su Bin, who stole sensitive military aircraft data on the F-35, F-22, and C-17 from two American defense contractors. As reported by Aaron Boyd in the Federal Times, from “October 2008 to March 2014, Su worked with two hackers, instructing them on which companies to target and what information he was looking for. Su would then translate the information into Chinese and forward it to his customers along with detailed reports.” As a result, such actions aimed at pilfering defense-industrial information are of significant concern to the U.S. military and the security of its operations.

189 See id.
190 See id. (explaining that “China’s cyber espionage against the U.S. government and defense industrial bases poses a major threat to U.S. military operations, the security and well-being of U.S. military
C. Measuring the Pulse of the Obama-Xi Cyber Pact of 2015

In a 2013 interview with Epoch Times, Indiana University Maurer School of Law professor David P. Fiddler commented “there was a chance the United States could have slowed the rate of global economic espionage, “but Snowden destroyed that.” In the aftermath of the Snowden leaks, Professor Fiddler expressed his skepticism of the role of diplomacy in remedying the issue of economic espionage: “Right now the idea of trying to have a sort of diplomatic initiative on economic espionage is dead in the water[.]” As a result, an impartial conflict resolution could be of great value here in bridging the cultural and ideological gaps between ‘state secrets’ and protected proprietary information like trade secrets. Following the Snowden leaks, President Obama and Chinese President Xi pledged that their countries would not conduct or knowingly support commercial cyber espionage against one another. A major critique of the Obama-Xi personnel, the effectiveness of equipment, and readiness.”

192 See Peter K. Yu, Trade Secret Hacking, Online Data Breaches, and China’s Cyberthreats, CARDOZO L. REV. DE NOVO 130, 146-47 (2015) (until the international community, or at least China and the United States, can agree on new international minimum standards, it is unlikely that the dispute between China and the United States can be easily resolved.”)
Cyber pact, however, as vocalized by the *Wall Street Journal*, was that it essentially represented “a digital arms deal that is full of promises but no enforcement.”

Jack Goldsmith, a professor at Harvard Law School, was also highly skeptical of this cyber pact, describing it as being “full of loopholes.”

Furthermore, without an enforcement mechanism that takes the attribution challenge into consideration, this flaw is an unsightly blemish on the face of this agreement.

The Obama-Xi Cyber Pact did, however, have an impact on the G20 Summit in Antalya Turkey. At the summit, the U.S. championed a “set of voluntary, non-binding peacetime norms of state behavior” aimed at

---


195 *See Jack Goldsmith, China and Cybertheft: Did Action Follow Words?*, LAWFARE, (March 18, 2016), https://lawfareblog.com/china-and-cybertheft-did-action-follow-words (explaining that “I was skeptical of the “deal” for many reasons. First, it was full of loopholes – what does “knowingly support” mean?; how to ascertain China’s “intent” to aid local firms when it might have so many other reasons for commercial theft?, etc. The unclear agreement left much room for opportunistic action. Second, I couldn’t fathom why China would back down from commercial theft practices worth (allegedly) hundreds of billions of dollars in the face of threatened (but never consummated) U.S. sanctions that at best would impose only a tiny cost compared to China’s gains. Third, and relatedly, there was no other public evidence that the U.S. made the type of seriously threatening actions, or concessions in its own behavior, that might have induced China to give up its commercial theft practices.”)
mitigating the potential for conflict in this domain.\textsuperscript{196} One norm,\textsuperscript{197} reported by \textit{Washington Post} correspondent Ellen Nakashima, was that no state conduct or support the theft of intellectual property in cyberspace.\textsuperscript{198} The G20 leaders reached the consensus that “no country should conduct or support [cyber]-enabled theft of intellectual property, including trade secrets or other confidential business information with the intent of providing competitive advantages to companies or commercial sectors.”\textsuperscript{199} The world leaders in attendance also affirmed that the bounds of international law fully apply in regulating state conduct in cyberspace.\textsuperscript{200}

According to Christopher Painter, the U.S. State Department Coordinator for Cyber Issues, this consensus is “an important building block in our effort to promote international security in cyberspace.”\textsuperscript{201}

\begin{flushleft}
\textsuperscript{197} See Anna-Maria Osula and Henry Roigas (Eds.), NATO CCD COE Publications, Tallinn 2016, \textit{International Cyber Norms: Legal, Policy & Industry Perspectives}, 12 (defining a norm as “‘a standard of appropriate behavior for actors with a given identity.’ This broad definition implies that norms can substantially differ in scope and legal ‘bindingness,’ as well as featuring legal, political, technological, ethical, or social characteristics.”) (internal citation to Martha Finnemore and Kathryn Sikkink, ‘International Norm Dynamics and Political Change,’ \textit{International Organization} 52 (1998): 887-917.)
\textsuperscript{198} See Nakashima, \textit{supra} note 174.
\textsuperscript{199} See \textit{id}.
\textsuperscript{200} See Painter, \textit{supra} note 182.
\textsuperscript{201} See \textit{id}.
\end{flushleft}
Painter’s optimism that this consensus marks a promising start for harmonizing cyber state relations, these promulgated norms of self-restraint need an edifice that accounts for the unique set of complexities that attribution brings to bear, and the difficulties in distinguishing between acts of economic intelligence and commercial espionage.

IV. BUILDING & REBUILDING INTERNATIONAL NORMS IN CYBERSPACE

While economic espionage may not constitute armed force under Article 2(4), scholars like Professor Lotrionte reason that “a highly coercive act into the economic and political freedoms of a state, may constitute a wrongful act of intervention in violation of the customary norm.”202 Indeed, there is a strong presumption against states either directly or indirectly violating the territorial integrity or political independence of other states via coercion. 203 This principle of non-intervention is implicit in Article 2(4), which provides that states “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 the Purposes of the United Nations.” 204

An act of economic espionage against one state, however, can rise to the level of coercion, thereby undermining the non-intervention principle, as well as economic sovereignty of all states. Indeed, cyber crimes

202 See Lotrionte, supra, note 116, at 496.
203 See id. at 497.
204 See U.N. Charter, Article 2(4).
that enable intellectual property theft and other acts of economic espionage result in billions of dollars in harm to the global economy each year.\textsuperscript{205} As such, a dispute settlement mechanism that accounts for the ambiguities of attribution, and distinguishes between acts of state-sponsored espionage is needed.

It merits noting that under Article 2, paragraph 3 of the UN Charter, all states have an obligation to settle “their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.”\textsuperscript{206} As a result, all states maintain an obligation to peacefully resolve their international disputes. By drawing upon the pre-existing international dispute settlement architecture under Article 33, the aim of this paper is to call on states to reflect upon this obligation, in an effort to promote a global dialogue on normalizing state relations in cyberspace. Article 33 reads in part:

\begin{quote}
The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.\textsuperscript{207}
\end{quote}


\textsuperscript{206} See U.N. Charter, Article 2(3).

\textsuperscript{207} See U.N. Charter Article 33(1).
Based on Article 33’s judicial settlement framework, I offer the Cyber Espionage Predominant Purpose Test (CEPP) as a legal test for the International Court of Justice (ICJ) to apply in resolving disputes in this area.

A. The Predominant Purpose Test

Under the common law\textsuperscript{208} tradition of U.S. contract law, if a transaction involves a sale for both goods and services, the approach taken by courts is to “determine which aspect is dominant and apply the law governing that aspect to the whole contract.”\textsuperscript{209} This process, known as the Predominant Purpose Test, allows courts to consider the underlying nature of the mixed transaction and decide which legal regimes to apply.

More specifically, as described by University of California Davis Law Professor David Horton, this test “helps courts decide whether the UCC or the common law

\textsuperscript{208} See The Common Law and Civil Law Traditions, The Robbins Collection, University of California, Berkeley School of Law, https://www.law.berkeley.edu/library/robbins/pdf/CommonLawCivilLawTraditions.pdf (explaining that “Most nations today follow one of two major legal traditions: common law or civil law. The common law tradition emerged in England during the Middle Ages and was applied within British colonies across continents. The civil law tradition developed in continental Europe at the same time and was applied in the colonies of European imperial powers such as Spain and Portugal. Civil law was also adopted in the nineteenth and twentieth centuries by countries formerly possessing distinctive legal traditions, such as Russia and Japan, that sought to reform their legal systems in order to gain economic and political power comparable to that of Western European nation-states.”) (last visited May 2016).

governs a particular transaction that involves both goods and services. (For instance, the sale of a household appliance that needs to be installed can be seen as involving both tangible and moveable property and significant labor).”

Here, if the contract is found to be primarily for the good (e.g. the household appliance), then Article 2 of the Uniform Commercial Code would apply. On the other hand, if the contract is primarily for the installation service, then the common law of contracts governs. Having outlined the basic structure of the Predominant Purpose Test, I apply its basic premise in the CEPP Test.

**B. The Cyber Espionage Predominant Purpose Test**

The central purpose of the CEPP Test is to resolve international disputes concerning cyber espionage operations that involve mixed elements of national security espionage and commercial espionage. As previously described, the test would be administered by the ICJ under Article 33. Given the distinct cultural norms represented in distinguishing between permissible and impermissible intelligence collection, the CEPP Test considers the cultural disparities in ‘state secrets’ versus ‘for-profit’ espionage. Under the definitional norm framework put forth by Anna-Maria Osula and Henry Roigas in *International Cyber*.

---

210 See David. O Horton, University of California Davis School of Law Professor of Contracts, via e-mail conversation (Feb. 12, 2016). “The test depends on the following factors: (1) the language of the contract (whether it refers to goods or services more often), (2) the nature of the supplier (is it a company that primarily sells goods or provides services?), and (3) the intrinsic worth of the goods versus the price of the services.”
**Norms: Legal, Policy & Industry Perspectives**, the CEPP Test would embody an international norm that “carr[ies] a legally binding obligation (i.e. treatises and other sources of international law).”

In terms of the legal analysis, the CEPP Test evaluates the following three factors:

1. The **intrinsic nature** of the economic information in dispute;
2. The **means of acquisition and predominant application** by the collecting entity (e.g. is it more akin to misappropriation of a trade secret to provide a competitive advantage to home-state companies or industries, or more driven by national security considerations as a form of classic espionage?);
3. And the **overall intent** of the collecting entity.

The Obama Administration avers that a “major difference [exists] between spying for national security

---

211 See Osula and Roigas, *supra* note 184, at 12 (the publication differentiates “between two principal types of norms that regulate state activities in cyberspace. These are: (1) International norms that carry a legally binding obligation (i.e. treatises and other sources of international law); and (2) International norms that act as points of reference for expected behavior but are not subject to legal enforcement mechanisms (e.g. legally non-binding voluntary norms of behavior) and are usually expressed in diplomatic agreements.”)
purposes, something the U.S. does daily, and the commercial, for-profit espionage carried out by China’s military.”

For Drake University Law Professor Peter Yu, however, this distinction “is not as clear as one would expect. Not only do most countries—democratic or otherwise—fail to recognize it, this line is also not always drawn in situations involving U.S. intelligence and surveillance efforts.” Professor Yu highlights that for countries like China, the U.S.’ definitional distinction imparts little clarity here, given the “overlap between security and economic concerns” among Chinese policymakers and the continued domination of state-owned enterprises in the local business environment.”

The CEPP Test functions to equitably reconcile these differences by balancing the nature of the disputed economic intelligence at issue, assessing the means of acquisition and predominant application by the entity, and the overall intent of the collecting entity. As a counterbalance to the attribution challenge, the CEPP Test would utilize a lower evidentiary standard from the civil law scheme—a preponderance of the evidence—to allow the aggrieved state the opportunity to seek legal recourse from the ICJ. Based on the issues at bar, the ICJ ultimately determines which standard of proof applies. However,

212 See Yu, supra note 107, at 132-33 (2015).
213 See id. at 133.
214 See id. at 134.
215 See Bryan A. Garner, A Handbook of Basic Law Terms, Black’s Law Dictionary, (West Group, 1999), p. 166 (defining a preponderance of the evidence as “[t]he greater weight of the evidence; the burden of proof in a civil trial, in which the jury is instructed to find for the party that, on the whole, has the stronger evidence, however slight the edge may be.”)
216 See Rules of Evidence Before the International Court of Justice,
as promulgated by the ICJ in the Nicaragua case: “A comparatively lower standard is demanded of the parties when the Court determines that a fact has to be proved in a convincing manner.”

The benefit of applying a lower standard of proof here, versus a heightened “beyond a reasonable doubt” standard typically applied in criminal proceedings, is that it provides a stronger cost deterrent. Faced with the looming specter of litigation and its associated costs, states that routinely engage in cyber economic espionage would therefore face a greater disincentive here. Indeed, as postulated by Christopher Painter, the U.S. State Department Coordinator for Cyber Issues, when “all states have an incentive to enjoy the benefits of cyberspace and

LAWTEACHER, http://www.lawteacher.net/free-law-essays/international-law/rules-of-evidence-before-the-international-court-of-justice-international-law-essay.php (explaining that “The standard of preponderance of evidence and that of reasonable conclusion have not found explicit mention in decisions by the Court, but for proving facts of relatively lesser importance, the Court appears to be willing to accept these standards, which fall between proof beyond reasonable doubt and proving facts in a convincing manner. [51] It is quite apparent that it is up to the Court to decide when it wants to apply what standard, and such decision is based on the facts and merits of the case at hand.”) (last visited May 2016).

217 See id. (describing that “The Nicaragua Case appears to be one in which such a standard has been applied. The only reference any the standard of proof in the Statute of the Court is in Article 53, which declares that if a party fails to appear in Court or defend its case, the Court, after satisfying itself that it has jurisdiction and the claim is “well founded in fact and law”, shall rule in favour of the other party. The Court, in the case, elaborated on the provisions of Article 53(2), [46] saying that ‘satisfy itself’ means that the Court must attain a “degree of certainty”, as in any other case, that the facts are based on convincing evidence. [47] Therefore, a standard lower than absolute proof beyond a reasonable doubt is provided for.”)
little incentive to disrupt it, cyberspace can continue to be an engine for economic and social growth around the globe.”218

1. Reconciling Differences

Admittedly, international norms do not blossom into fully-grown gardens overnight. Moreover, a bright line rule that prohibits gathering intelligence on all state-industrial entities would not be viable in China, because it “overlook[s] the historical fact that trade secrets originated in China as a form of state secret.”219 The Obama-Xi Cyber Agreement of 2015 is of great interest here, for as noted in the Washington Post, “Beijing until that point had made no distinction between commercial cybertheft to profit a nation’s industries and espionage for traditional political and military purposes.”220

The CEPP Test addresses Professor Yu’s concern of cultural differences by instead embracing these disparities as inputs and producing a more balanced, holistic output.221 Thus, rather than argue for one country’s particular definition here, the CEPP Test solicits input from both parties in reaching a settlement. CEPP strikes this balancing by having the ICJ assesses the nature of the information at issue, its acquisition, predominant

218 See Painter, supra note 181.
219 See Yu, supra note 107, at 145.
220 See Nakashima, supra note 174.
221 See Yu, supra note 107, at 146 (“[I]t is important to be more specific about the type of secret involved. Does the debate concern state secrets, political secrets, military secrets, personal secrets, scientific or technological secrets, or business, industrial, or trade secrets?”)
application and intent of the collecting entity, to proffer a balanced ruling. In summary, the CEPP test recognizes the ambiguity in espionage operations, as well as the competing cross-cultural economic espionage norms.

V. CONCLUSION

In summary, to verify compliance, a certain level of attribution, coupled with proper assurance, is necessary. Given the complexities of attributing a hostile cyber act to its true source(s), however, this informational uncertainty can create an enforcement paradox to upholding international law in cyberspace. And although international norms do not emerge suddenly in full force, the CEPP Test offers a legal theory—a proverbial seed—which if properly cultivated, can serve as a mechanism for resolving international disputes regarding espionage operations. As a counter balance to the attribution challenge, the CEPP Test would utilize a preponderance of the evidence standard. The benefit of borrowing the lower evidentiary standard of a civil proceeding, as opposed to the criminal standard of beyond a reasonable doubt, is that it would better enable the aggrieved state the opportunity to seek legal recourse from the ICJ, as well as place an increased cost/risk on states that routinely engage in commercial espionage.

Ultimately, because no state is an island in cyberspace, a model that is both adaptable to the attribution challenge and recognizes cross-cultural economic espionage norms, can help promote the economic security of all.
MEASURING AUTONOMOUS WEAPON SYSTEMS AGAINST INTERNATIONAL HUMANITARIAN LAW RULES
Dr. Thompson Chengeta*

ABSTRACT

In this paper, I argue that Autonomous Weapon Systems (AWS) will not be able to comply with important rules of international humanitarian law (IHL) such as distinction, proportionality, and military necessity. Currently, it is impossible to develop a lethal robot that can comply with IHL rules because IHL terms such as “civilians”, “combatants”, “direct participation in hostilities” etc. have no precise definitions that can be decoded into a machine. Further, in many instances, the nature of today’s armed conflicts demands human judgement which machines do not possess. Even in cases where AWS may comply with some rules of IHL, I argue that AWS still violate the right to dignity which demands that the decision to use force against another human must be taken by a fellow human. To this end, I note that the issue is not about comparing whether robots can perform better than humans, but whether they should be allowed to act as combatants in the first place.

*Dr. Chengeta holds an LL.D from the University of Pretoria, an LL.M. from Harvard Law School, an LL.M. from the University of Pretoria, and an LL.B. from MSU.
I. INTRODUCTION

The development of unmanned systems that are remotely controlled and those with increased autonomy in their critical functions has been a concern to the international community for more than a decade. The idea to develop autonomous weapon systems with increased autonomy in their critical functions (AWS) – machines that once activated are able to make the decision to kill humans without further human intervention – has sparked heated debates across the globe. The old adage, “technology is a double-edged sword”\(^1\) has never, in the history of weapon development, been more pertinent than it is with AWS. On one hand, AWS clearly promises a potential to save lives – to make a change to the unacceptable current state of affairs in armed conflict and elsewhere – where force is used. At the same time, AWS poses potential threats to the right to life, dignity and other important rights.\(^2\) With the

\(^1\) “We have to realize that science is a double-edged sword. One edge of the sword can cut against poverty, illness, disease and give us more democracies, and democracies never war with other democracies, but the other side of the sword could give us nuclear proliferation, bio-germs and even forces of darkness.” Michio Kaku Quotes, BrainyQuote, available at http://www.brainyquote.com/quotes/keywords/sword.html (accessed 2 August 2015).

technology still in the preliminary stages of development and yet to be deployed, it is as difficult to ascertain whether AWS are legal or illegal weapons as it is to brand their deployment ethical or unethical, moral or immoral when they become available. It is these uncertainties that have left scholars, organizations, states and the international community divided on how to respond to AWS. Although their development is at an advanced stage, it is important to note that AWS do not yet exist.

Across the globe, the debate on AWS has focused more on the ramifications of AWS on International Humanitarian Law (IHL) than on other branches of international law. This is so because the general expectation is that AWS will be deployed in the context of armed conflict; thus International Humanitarian Law being the applicable regime. To this end, scholars have grappled with the question of whether AWS are capable of complying with important and customary IHL rules of military necessity, distinction, proportionality and precaution. This is an important question because to many people it may be that the acceptability or otherwise of this technology depends on AWS’ capability to comply with the aforementioned rules – at least in the context of armed conflict. It should be remembered, however, that the IHL rules discussed below were meant to be applied by human combatants, not by autonomous robots.

In the context of armed conflict, there are at least three camps of thought on whether AWS are capable of complying with IHL rules of humanity, necessity, distinction, proportionality and precaution. Firstly, there are commentators who opine that there is not enough

material and knowledge on the technology to formulate a correct position on AWS’ capability to comply with the aforementioned rules.\textsuperscript{3} Such scholars contend that any form of action by the international community would be premised on a fallacious basis.\textsuperscript{4} To that end, they consider the proposal for an outright ban to present a “risk of failing to develop forms of automation that might make the use of force more precise and less harmful to civilians caught near it”.\textsuperscript{5} In the face of the proposed ban, some commentators thus note the argument that the US and other states involved in the development of AWS “should not unnecessarily constrain themselves in advance to a set of normative commitments given the vast uncertainties about the technology and future security environment”.\textsuperscript{6} It seems such scholars want to adopt a wait and see approach – i.e. wait at least until the technology is available. The major problem with such an approach is that once the technology, especially in terms of weapons, is available, it may be too late to formulate correct and effective regulation.\textsuperscript{7} Worse still, it may be in fact an elegant way of buying time for the technology to be developed.

Secondly, there are scholars who argue that there is sufficient evidence to believe that AWS may do a better job as far as complying with the above IHL rules is concerned. Such arguments are centered on facts such as AWS’ inability to act out of panic, anger, frustration etc., and that

\textsuperscript{4} Id.
\textsuperscript{5} Id., at 1.
\textsuperscript{6} Id., at 18.
they do not seek revenge. Unless specifically programed to do so, AWS will not intentionally commit war crimes. The major argument in this regard is that AWS will not only enhance the quality of life of soldiers, but it will also address the plight of civilians – not to be victimized whenever and wherever there is an armed conflict.

Thirdly, and in response to the above argument, there are commentators who argue that because a machine can never have human intelligence, a situational awareness to capture and understand a bigger picture – qualities which are extremely important on the battlefield – they will never be able to comply with the above mentioned rules of international humanitarian law. For example, a machine cannot tell that a fighter is about to surrender, making his or her death unnecessary.

The summary of arguments that I make in this paper constitutes that when ascertaining whether or not AWS are capable of complying with international humanitarian law rules, such a question should not be generalized because the levels of autonomy of AWS differ. In this paper, I focus on those Autonomous Weapon Systems that are not under

---

8 See Id., at 10; See also Gary Marchant et al., International Governance of Autonomous Military Robots, 12 COLUM. SCI. & TECH. L. REV. 272 (2011).
10 See Ronald Arkin, Lethal Autonomous Systems and the Plight of the Non-Combatant, AISB QUARTERLY, No. 137 (July 2013).
11 See Sharkey, supra note 2.
“Meaningful Human Control”\textsuperscript{13} after their activation.

Regarding autonomous systems that are not under “Meaningful Human Control”, if they are deployed in areas where there are civilians, protected persons and objects, such AWS may be incapable of complying with rules of IHL such as the rule of distinction and proportionality.\textsuperscript{14} This is mainly because of technological limitations, the unpredictability of the battle field and the ever changing circumstances and status of fighters or combatants.\textsuperscript{15}

Even if deployed in environments that are only occupied by combatants or fighters, AWS that are not under meaningful control of a human once activated may still violate some important rules of IHL such as those relating to the protection of those placed hors de combat by wounds or sickness or those that wish to surrender.\textsuperscript{16}

In response to Ron Arkin’s argument that robots can perform better than humans as far as complying with


\textsuperscript{14} On IHL rules see generally JEAN-MARIE HENCKAERTS ET AL., \textit{CUSTOMARY INTERNATIONAL HUMANITARIAN LAW} (2005).


international humanitarian law rules is concerned, I argue that even if one were to assume for a moment that robots are better, that is not the end of the matter. Giving robots the power of life and death, even over legitimate targets may be incompatible with international human rights norms that continue to apply even in times of armed conflict.\footnote{See Gerd Oberleitner, Human Rights in Armed Conflict 1 (2015).}

Furthermore, there are other roboticists like Noel Sharkey who argue that it may be technically impossible to create robots that can comply with rules of armed conflict, worse still, to be better than humans.\footnote{Ronald Arkin, Governing Lethal Behaviour: Embedding Ethics in A Hybrid Deliberative/Reactive Robot Architecture, TECHNICAL REPORT GIT-GVU-07-11, at 61 (2011); See also Ronald Arkin, Governing Lethal Behaviour in Autonomous Robots International Committee of the Red Cross Press 127 (2009); Marchant, supra note 8, at 280.} As for the International Humanitarian Law rule of precaution, I note and agree to some extent that AWS may well comply with the rule of precaution; for example, where they can wait to be shot at first in cases where they are not sure whether or not one is participating in hostilities.\footnote{On robots acting in a conservative way, see A/HRC/23/47, supra note 2, at 280; P.W. Singer, Wired For War: The Robotics Revolution and Conflict in the 21st Century 398 (2009).} However, the rule of precaution, just like the customary rules of proportionality and distinction, needs human judgment to be effectively complied with.\footnote{On the importance of human judgement, see RED CROSS, supra note 15, at 21, 26, 32, 72; Autonomy in Weapon Systems, Directive 3000.09, U.S. DEP’T OF DEF. (Nov. 21, 2012); Asaro supra note 2, at 94; Geneva Academy, supra note 15.} Where humans are not involved once the system is activated, chances are high that these rules will be violated.
In conclusion, my position is that AWS that have high levels of autonomy to the extent of being unpredictable or those that are not under “Meaningful Human Control” once they are activated may not be able to comply with important customary international law rules of International Humanitarian Law.

A. The Importance of Complying with the Rules of IHL

Before assessing AWS against some of the important IHL rules, it is necessary to explain the importance of complying with such rules. There are several reasons why the issue of whether AWS are capable of complying with international humanitarian rules must be taken seriously. Firstly, compliance with International Humanitarian Law serves to promote and protect all persons that are protected in terms of the law during an armed conflict like civilians, those who are hors de combat, medical personnel and employees of humanitarian organizations. Where AWS are unable to comply with the rules of IHL that are discussed below, it means the protection that is offered to these groups of people is severely diminished. Protection of those who are not taking part in hostilities is the core of international humanitarian law.

21 See Dieter Fleck, International humanitarian law after September 11: Challenges and the need to respond in YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 63 (Heike Krieger et al. eds., 2003).

Secondly, compliance with rules of International Humanitarian Law is important especially in today’s armed conflict that involves non-state actors such as rebel groups. In most cases where non-state actors are involved, there is a lack of guidance and incentive as far as complying with IHL rules is concerned. In fact, “clandestine methods and means may be the predominant rule”. In such circumstances, states must ensure that the means and methods of warfare they use comply with the rules of International Humanitarian Law as a way to show and make known the standards that the non-state actor ought to abide by. In this sense, compliance with the law “furthers acceptance of such rules and offers incentives to encourage the expectation of reciprocity” especially from the aforementioned non-state actors.

Along the same lines, compliance with rules of International Humanitarian Law contributes to discouraging belligerents involving themselves in reprisals – a situation where combatants or fighters willfully violate the law on the basis that the other part of the conflict is not abiding by the same laws. Of course, this is not to say that compliance with the law on the part of non-state actors or other parties to a conflict is dependent on reciprocity of good behavior, but it is a compelling argument that acceptable conduct of states in as far as conduct of

---

24 See Fleck supra note 21, at 66.
25 See Id., at 65.
26 See Dieter Fleck, THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 228 (2013).
27 See Henckaerts supra note 14, at 498. It is explained that compliance with IHL is not dependent on reciprocity.
hostilities is concerned not only gives them the standing to reprimand erring non-state actors but set a good example.

Thirdly, compliance with rules of International Humanitarian Law is of importance as far as peace is concerned. In general, complying with the law is the core of the rule of law which is what knits and binds the world community together. In the context of armed conflict, Dieter Fleck has noted that compliance with the rules of International Humanitarian Law “is part of good governance even in times of crisis”.28 Thus during armed conflict, the means and methods of warfare that a state chooses to use must comply with the law because this is important “for the reestablishment and maintenance of peace”.29

Fourthly, and related to the reestablishment and maintenance of peace argument, complying with rules of International Humanitarian Law serves to maintain military discipline.30 Military discipline referred to herein is where combatants concentrate and focus only on legitimate targets thereby serving time and resources in incapacitating the enemy.31 The earlier the enemy is incapacitated the quicker the peace is regained. Peace is the ideal environment within which human rights are better protected.32 For that reason, peace should be the norm and wars must be just a temporary short lapse.33 Arguably, military discipline and compliance with the law shortens wars.34

28 See Fleck supra note 21, at 65.
29 Id.
30 Id., at 64.
31 Id., at 63.
32 See A/68/382 supra note 2.
34 See Fleck supra note 21, at 64.
Finally, and in view of the above, it is emphasized that when considering the question as to whether AWS are capable of complying with rules of International Humanitarian Law, commentators must understand the important issues that are implicated. This is an issue that involves matters of life and death, security and peace. Thus, in the development of weapons or designing methods of warfare, states must always seek to comply with the rules of International Humanitarian Law, even at an “expense of short term disadvantages”.\(^{35}\) There should generally be a culture to comply with the above mentioned rules and when states develop weapons, they must understand that they should “not only act in the interest of their own state, but they should also consider themselves as guardians of the people in the area of conflict”.\(^{36}\) It is important that when seeking to use certain weapons and “in choosing the means and methods of their operations, they must consider public opinion in all the countries affected” by weapons they use.\(^{37}\)

A cutting edge example in regard to choice of weapons and compliance with rules of International Humanitarian Law is the use of drones by the US in countries like Pakistan, Yemen and Afghanistan.\(^{38}\) Alleged failure to comply with international law – in particular, distinguishing between terrorists and civilians – has produced a backlash with other scholars claiming that drones are a vending machine for more terrorists against

\(^{35}\) Id.
\(^{36}\) Id.
\(^{37}\) Id.
MEASURING AUTONOMOUS WEAPONS . . . [2016]

the US. Such claims are supported by an anti-American sentiment in some of the territories that are affected by drones.

For the above stronger reasons, compliance with the law, the choice of the means and methods of warfare is of paramount importance as far as guaranteeing the protection of those who are not participating in hostilities and the maintenance of peace, in general, is concerned. In as much as the first port of call is to consider whether a particular weapon is in line with the law, it is also important that the state considers the ramifications of using such a particular weapon, especially in the wake of fighting against global terrorism. As observed by the former UN Secretary General Kofi Annan, when it comes to choosing means and methods of warfare against terrorism and other forms of today’s armed conflict; “there is no trade-off between effective action against terrorism and protection of human rights”, rather, “human rights, along with democracy and social justice, are one of the best prophylactics against terrorism”.

uneral

40 See Ross, supra note 39.

Having articulated some of the important considerations that are at stake, I now turn to consider some of the important rules of International humanitarian law and how they relate to AWS.

B. *IHL Rule of Distinction and AWS*

The International Humanitarian Law rule of distinction is meant to protect those who are not taking part in hostilities, in particular, civilians. It is also meant to protect fighters or combatants who have been placed *hors de combat* by sickness or wounds.\(^{42}\) The rule of distinction was first provided for in the St. Petersburg Declaration which categorically stated that the aim of war is to weaken the enemy by attacking only its armed forces.\(^{43}\) The rule was further endorsed in the Hague Regulations which proscribed attacking “towns, villages, dwellings or buildings which are undefined” therefore being “shots in the dark” with the possibility of killing civilians and combatants indiscriminately.\(^{44}\)

Today, the rule of distinction is codified in laws applicable both to international and non-international armed conflict.\(^{45}\) For international armed conflicts, Additional Protocol I to the Geneva Conventions has a

\(^{42}\) See HENCKAERTS, *supra* note 14, at Rule 47.


\(^{44}\) See Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land art. 25, Oct. 18, 1907.

\(^{45}\) HENCKAERTS, *supra* note 14, at 5.
number of provisions on the rule of distinction:

In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.46

The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.47

Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.48

Similar provisions are also found in laws pertaining to the governance of non-international armed conflicts.49 For that reason, it does not matter whether AWS will be used in non-international or international armed conflicts; the rule of distinction equally applies. During the negotiations of Additional Protocols I and II to the Geneva

46 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977.
47 Id., at Art. 51 (2).
48 Id., at Article 52(2).
49 See e.g. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) art. 13(2), (June 8, 1977) (“The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.”).
Conventions of 1949 as applicable to international and non-international armed conflicts respectively, the rule of distinction was considered a fundamental basic rule to which no reservation was permitted.\(^{50}\)

The rule of distinction is part of customary international humanitarian law and is a *jus cogens* rule.\(^{51}\) Rule 1 of the International Committee of the Red Cross study on customary international humanitarian law provides that it is a matter of customary international law as supported by state practice that “parties to a conflict must at all times distinguish between civilians and combatants”.\(^{52}\)

The term “combatant” in this sense refers to both combatant as denoting the legal status of a member of a state’s armed forces and fighters in general or those participating in hostilities.\(^{53}\)

In contemporary armed conflicts where sophisticated weapons are used, the rule of distinction is the

---

\(^{50}\) See *e.g.* Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Volume VII, Statements of the UK and Mexico (1974-77).

\(^{51}\) HENCKAERTS, supra note 14, at 3; See Corte Constitucional [C.C.] [Constitutional Court], April 25, 2007, Sentencia C-291/07, Gaceta de la Corte Constitucional [G.C.C.] (p. 70) (Colom.) (“the essential principles of international humanitarian law have acquired jus cogens status, based on the fact that the international community as a whole has recognized their peremptory and imperative nature . . . Among the essential principles of international humanitarian law with jus cogens status [is] the principle of distinction.”); See also Practice Relating to Rule 1 on the Principle of Distinction between Civilians and Combatants, INT’L COMM. RED CROSS, available at https://www.icrc.org/customary-ihl/eng/docs/v2_ccha_chapter1_rule1.


\(^{53}\) HENCKAERTS, *supra* note 14, at 3.
cornerstone and central to the protection of civilians.\textsuperscript{54} Some commentators have thus referred to it as a “pillar of international humanitarian law” and a “means to an end” – i.e. protection of those not taking part in hostilities.\textsuperscript{55} Thus, a belligerent deploying Autonomous Weapon Systems is bound by customary international law “to distinguish between military and civilian objects”.\textsuperscript{56}

In terms of Article 52(2) of Additional Protocol I to the Geneva Conventions, military objectives refer only to objects that have an “effective contribution to military action” and whose neutralization gives a belligerent a definite and real military advantage that must be offered “in the circumstances ruling at the time”\textsuperscript{57}. There are a number of scholars who agree that the above definition is part of customary international law.\textsuperscript{58} Therefore, in order to target legitimate targets, an Autonomous Weapon System must be able to understand and effectively implement the definition of a military objective.\textsuperscript{59} The autonomous system needs to

\textsuperscript{54} Anicee Van Engeland, Civilian or Combatant?: A Challenge for the 21st Century 16 (2011); Nils Melzer, Targeted Killing in International Law 300 (2008); Dan Saxon, International Humanitarian Law and the Changing Technology of War 107 (2013).

\textsuperscript{55} Fleck, supra note 21, at 6.


\textsuperscript{58} Henckaerts supra note 14, 329-32.

\textsuperscript{59} See Agnieszka Jachec-Neale, The Concept of Military
be taught to be able to make a difference between military advantage that is “tangible” therefore necessitating an attack and military advantage that is “in abstract or general” which may not justify an attack and likely to violate the rule of distinction. Thus, in terms of the rule of distinction, an autonomous system’s decision to target and kill must give “direct and tangible military advantage”. It is important, therefore, to understand who is a civilian in armed conflict and also other protected persons.

The weapons that a belligerent chooses to use in armed conflict have a direct impact on whether or not the rule of distinction will be complied with. Thus in international weapons law, the rule of distinction has also been emphasized. It is for that reason that the purpose of certain weapon treaties is identified as “to put an end to the suffering and casualties caused by anti-personnel mines that kill or maim hundreds of people every week, mostly innocent and defenceless civilians and especially children”. Some treaties on conventional weapons also have in detail the rule of distinction:

It is prohibited in all circumstances to direct weapons to which this Article applies, either in offence, defence or by way of reprisals, against the civilian population as such or against individual civilians.

---

**Objective in International Law and Targeting Practice 170 (2014).**


62 *See also* Int’l Comm. Red Cross, *supra* note 51.


64 Protocol II to the Convention on Prohibitions or Restrictions on the
The indiscriminate use of weapons to which this Article applies is prohibited. Indiscriminate use is any placement of such weapons:

a) which is not on, or directed at, a military objective; or
b) which employs a method or means of delivery which cannot be directed at a specific military objective; or
c) 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.65

These similar rules can also be found in Article 2(1) of Protocol III to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects.66

The rule of distinction is also incorporated in international criminal law where failure to abide by it leads to prosecutable war crimes, for example, crimes against humanity or grave breaches of the Geneva Conventions of 1949.67 The proscription of military conduct that fails to distinguish between civilians and combatants is found in
many military manuals and national criminal legislation of many states.\(^68\) Domestic and international courts have also considered the rule of distinction as a cardinal and intransgressible rule of international humanitarian law.\(^69\)

1. Complications of Contemporary Armed Conflicts and Rule of Distinction

When the rule of distinction was initially formulated, it was done in view of conventional warfare and armed conflicts where it was easy to distinguish between combatants and civilians.\(^70\) In most cases, wars were even fought outside villages or towns and combatants carried their arms openly and wore distinctive marks.\(^71\)

However, in contemporary armed conflicts, especially those involving terrorists, there is “decivilianisation of civilians”, civilians providing human shields to fighters, either willingly or unwillingly, thereby complicating the implementation of the rule of distinction.\(^72\) Armed conflicts are brought to villages, towns and other dwellings of civilians.\(^73\) Many fighters neither carry arms openly nor do they wear distinctive

\(^{68}\) See Henckaerts, supra note 14, at 4.

\(^{69}\) See Nuclear Weapons Case, 434; See also Military Court sitting in Ramallah, Military Prosecutor V. Omar Mahmud Kassem et al. (Apr. 13, 1969), at ¶ 271.


\(^{71}\) See Heather Dinniss, Cyber Warfare and The Laws Of War 148 (2012).


\(^{73}\) See Tim Bunnell et al., Cleavage, Connection and Conflict in Rural, Urban and Contemporary Asia 90 (2012).
marks or uniforms. The role of civilians in some of the conflicts has become more and more confusing.

On account of the foregoing, many commentators and even the fighters themselves have acknowledged the difficulties encountered on the battlefield as far as applying the rule of distinction is concerned. This contributes to some of the high numbers of incidental harm that is suffered by civilians in contemporary armed conflicts. Combatants and fighters have been called upon to be more careful and to apply due diligence and care when designating targets and targeting them. This is because the mentioned complications do not mean that the rule of distinction loses its importance; in fact, it becomes more important than ever. Arkin argues that the current status quo on the battlefield is unacceptable and proposes that AWS may, in fact, perform better in as far as complying with the rule of distinction on this complicated battle field. The question arises, therefore, whether the advent of Autonomous Weapon Systems to operate on this complicated battle field is the solution or whether it will actually exacerbate the situation.

As noted above, the rule of distinction “was not drafted to rule on war, but rather to protect victims of war, in particular, civilians”. But who is the civilian, given

75 See Id.
76 Id.
77 See DANIELLE BESWICK & PAUL JACKSON, CONFLICT, SECURITY AND DEVELOPMENT: AN INTRODUCTION 36 (2014).
78 See Id.
79 See Arkin supra note 10, at 9.
80 ENGELAND supra note 54, at 245; See also Robin Geiss & Michael
some of the difficulties referred to above? Civilians, as a matter of law, are only entitled to protection when they do not directly participate in hostilities. 81

2. Definition of Civilian, Rule of Distinction in IAC and NIAC

All persons who are not part of the armed forces belonging to a state or who are not members of an armed group participating in an armed conflict are considered to be civilians. 82 Membership to a state’s armed forces or armed group is where an individual’s function is to fight for that armed force or group. 83 In the context of international armed conflict, “all organized armed forces, groups or units under a command responsible to a state party to the


81 See Bouchet-Saulnier, supra note 70, at 61.
82 See Rule 5. Definition of Civilians, INT’L COMM. RED CROSS, available at https://www.icrc.org/customary-ihl/eng/docs/v1_chapter1_rule5; See also Henckaerts, supra note 14, at17; Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, INT’L COMM. RED CROSS, available at https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf. The Interpretive Guidance is not legally binding. It is however, persuasive since it was influenced expert discussions and represents the views of the ICRC, “a neutral and independent humanitarian organization that has been mandated by States to promote IHL and work for a better understanding of the law.”
conflict” are not civilians while in NIACs it is only the “organized armed groups who constitute the armed forces of a non-state party to the conflict”.  

As already indicated earlier, ascertaining who falls within the definition of a civilian is difficult in some of the armed conflicts that are witnessed currently. In some cases, the conduct of civilians, especially in non-international armed conflict, needs careful assessment as to whether they have lost their protection or they are still within the confines of protected persons.

It is not uncommon that civilians support a particular group or state in an armed conflict. This is sometimes in a direct, “spontaneous, sporadic or unorganized way”. Questions arise as to whether such civilians can be considered to be members of a particular armed group or they are still civilians entitled to protection. In these circumstances, careful and considered human judgment as to who qualifies as a civilian is essential to determine which conduct by a civilian result in them losing protection.

In a bid to make some clarifications as to when a civilian loses protection for participating in hostilities and

---

84 Dieter Fleck supra note 26, at 248; Clapham & Gaeta supra note 16, at 309; See also INT’L COMM. RED CROSS, supra note 83.

85 See Bouchet-Saulnier, supra note 70, at 61.

86 See INT’L COMM. RED CROSS, supra note 81.

87 See Id.

88 See Id. The issue of continuous combatant function is discussed below.

also to make clear legitimate targets for the purposes of abiding by the rule of distinction, the ICRC compiled a guideline on direct participation in hostilities.

3. Direct Participation in Hostilities

The rule of distinction demands that civilians be distinguished from legitimate targets. Civilians are not legitimate targets and attacks may not be directed against them unless and until “such time they are directly taking part in hostilities”.

Civilian protection can thus be lost when a civilian directly takes part in hostilities. The rule of distinction does not protect such persons as they become lawful targets. The fundamental question is: When is a person deemed to be directly participating in hostilities and will AWS be able to apply this complex standard?

It is only where a person intends his or her actions to substantially cause harm to one of the belligerents that he or she is considered to be directly participating in hostilities. While an individual who belongs to a state’s or

---

90 Supra note 46, at Art. 51(3); See also TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 118 (Michael N. Schmitt ed., 2013); UC JHA INTERNATIONAL HUMANITARIAN LAW: THE LAWS OF WAR 29 (2011).
93 CLAUDE PILLOUD ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS: OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 619 (1987); Melzer, supra 82, at 1016; CLAIRE
an organized group’s armed forces is legitimate targets for the duration of his or her membership— that is as long as they do not surrender or “placed hors de combat by wounds or sickness”— a civilian is only a legitimate target “for such time as he or she directly participates in hostilities.”

The concept of “direct participation in hostilities” is complicated, that is why commentators do not necessarily agree on how it should be interpreted. On the one hand, there are scholars who note that there are several things that civilians may do on the battlefield— actions that may not be anticipated but have a harming effect to one belligerent, therefore, justifying the argument that direct participation should be interpreted expansively.

The above is an acknowledgment that the nature of contemporary armed conflicts constantly needs human


94 Fleck, supra note 26, at 248; Clapham & Gaeta, supra note 16, at 309; See also Int’l Comm. Red Cross, supra note 82.

95 Supra note 46, at Art. 51(3); Hampson, supra note 60, at 47.


97 Id.

98 Fausto Pocar et al., War Crimes and the Conduct of Hostilities: Challenges to Adjudication and Investigation 135 (2013); Roland Otto, Targeted Killings and International Law: With Special Regard to Human Rights and International Humanitarian Law 532 (2011); See Emily Crawford, Identifying the Enemy: Civilian Participation in Armed Conflict 70 (2015) (arguing however, against such an expansive interpretation).
judgment and discretion, both for the protection of civilians and not unfairly militating against the rights of combatants. Autonomous Weapon Systems may not have such human discretion and the ability to make human judgments – the quality judgment that is so fundamental if the rule of distinction is to be complied with in contemporary conflicts. On the other hand, while combatants and belligerents may benefit from the broad interpretation of what constitutes direct participation, it may threaten the protection of civilians.\textsuperscript{99}

Ascertaining whether a civilian is directly participating in an armed conflict is on a case by case basis – it is a subjective test.\textsuperscript{100} When applying a subjective test, combatants and fighters must always remember that a civilian must be clearly involved in an armed conflict or military operation in order to be a legitimate target. It can be argued that subjective tests in most cases require human judgment.\textsuperscript{101}

The international Committee of the Red Cross defines a person as taking a direct part in hostilities if the person is engaging in acts that “aim to support one party to the conflict by directly causing harm to another party”.\textsuperscript{102} That harm may cause death, injury or destruction to the


\textsuperscript{100} Derek Jinks et al., Applying International Humanitarian Law in Judicial and Quasi-Judicial Bodies: International and Domestic Aspect 79 (2014); See also Michael Schmitt et al., Yearbook of International Humanitarian Law 166 (2011).

\textsuperscript{101} On importance of human judgement, see Int’l Comm. Red Cross, supra note 20, at 21,26,32,72; U.S. Dep’t of Def. supra note 20; Asaro supra note 2; Geneva Academy supra note 15.

\textsuperscript{102} See Int’l Comm. Red Cross, supra note 83.
property belonging to another belligerent.\textsuperscript{103} There are various examples of acts that would amount to direct participation in hostilities and they include some of the following:

Capturing, wounding or killing military personnel; damaging military objects; or restricting or disturbing military deployment, logistics and communication, for example through sabotage, erecting road blocks or interrupting the power supply of radar stations, interfering electronically with military computer networks and transmitting tactical targeting intelligence for a specific attack.\textsuperscript{104}

Furthermore, when assessing whether the actions of a person constitute direct participation in hostilities, combatants and fighters must always remember that there should be a direct link between someone’s actions and the armed conflict. Such actions must be specifically designed to aid one belligerent to the disadvantage of the other. For that reason, it does not mean that every violent act in armed conflict establishes direct participation especially in cases where a civilian or an individual acts in personal self-defence.\textsuperscript{105} Thus, if a person, not for the purposes of supporting any party to the conflict fires shots against some fighters abusing his family, purely in self-defence of his family, that person is not directly participating in hostilities.\textsuperscript{106} The question which one will have to answer is whether Autonomous Weapon Systems will have the intelligence to understand such situations.

In order to understand and implement the concept of direct participation in hostilities as an element of the rule of distinction, Autonomous Weapon Systems will have to

\begin{itemize}
\item \textsuperscript{103} See Id.
\item \textsuperscript{104} See Id.
\item \textsuperscript{105} See Id.
\item \textsuperscript{106} See Id.
\end{itemize}
possess the human-like capacity to give the qualitative judgement on which civilians are directly participating in hostilities and, therefore, targetable. Understanding the concept of direct participation in hostilities is important for the purposes of the rule of distinction because indirect participation in hostilities does not make a civilian a legitimate target.\textsuperscript{107}

In many cases, indirect participation in hostilities can potentially aid a belligerent’s war effort but such participation does not lead to loss of protection on the part of the civilian.\textsuperscript{108} Examples of indirect participation in hostilities would include someone involved in the production, sale, and transfer of weapons, provision of finances, administration, political support and other infrastructure.\textsuperscript{109} AWS, especially those that have no “Meaningful Human Control” after activation, will need artificial intelligence equivalent to that of humans in order to be able to distinguish between direct and indirect participation in hostilities which is a qualitative distinction.\textsuperscript{110}

More so, I have referred to the temporal limitation as to when a civilian may be targeted for direct participation in hostilities. As already mentioned, a civilian is only a legitimate target at “such time as” he or she is involved in hostilities. An intense debate has resulted on account of this rule with two main arguments emerging. On the one hand, it is argued that this temporal limitation is unfair to fighters and combatants as it allows some unscrupulous civilians to be “farmers by day and fighters

\textsuperscript{107} See BOUCHET-SAULNIER, supra note 70, at 60.
\textsuperscript{108} See INT’L COMM. RED CROSS, supra note 83.
\textsuperscript{109} See Id.
\textsuperscript{110} See INT’L COMM. RED CROSS supra note 89, at 7.
by night” – escaping unfairly from legitimate use of force. On the other hand, other commentators have argued that this can be solved by the doctrine of continuous combatant function to be discussed below.

The requirement to attack civilians only for “such time as” they are participating in hostilities presents challenges especially in the fight against terrorism. This is so because in some cases terrorists qualify as civilians and because of the secrecy of their operations, it is difficult if not impossible to pin-point at which time one may say that they are directly participating in armed conflict.

In the drone warfare against terrorism, targeting has not only been on the basis of direct participation in hostilities but also on the basis of membership or suspicion of membership to a terrorist organization. There are many scholars who criticize targeting of individuals on the basis that they are members or suspected members of a particular terrorist organization or network as it is contrary to the rule of distinction. It is not unforeseeable that AWS may be used in the fight against terrorism and that the same kind of designating targets that is currently used in drone targeting may be used when Autonomous Weapon

---

111 RÖMER supra note 96, at 62.
113 See generally ANNA GOPPEL KILLING TERRORISTS: A MORAL AND LEGAL ANALYSIS (2013); ADIL DUYAN DEFENCE AGAINST TERRORISM: DIFFERENT DIMENSIONS AND TRENDS OF AN EMERGING THREAT (2012).
114 See MELZER supra note 54, at 411; AVERY PLAΪW, TARGETING TERRORISTS: A LICENSE TO KILL? 1 (2013); OTTO supra note 98, at 482.
Systems are finally deployed. For that reason, the objections that have been noted in as far as drone use and designation of targets is concerned must be repeated and cautioned against in the case of Autonomous Weapon Systems. Such selection of targets includes signature strikes and targeting on the basis of mere suspicion.  

4. Continuous Combatant Function

The concept of Continuous Combatant Function (CCF) is sometimes invoked when a person is targeted at a time when they were not involved in a military operation. CCF is an important concept that needs to be understood if the rule of distinction is to be complied with. Under this concept, an individual is targeted because of his or her continued function of fighting for one of the belligerents. The CCF concept is a recent International Humanitarian Law formulation meant to be a

---


118 “The doctrine of continuous combat function posits that a civilian who is repeatedly involved in hostilities through persistent acts of direct participation maybe targeted even at the time he/she is not actively engaged. However, scholars also disagree on what constitutes CCF.” Thompson Chengeta, Are US Drone Targeted Killings Within the Confines of the Law?, Unpublished LL.M Thesis, at 41 (2011), available at http://repository.up.ac.za/bitstream/handle/2263/18610/Chengeta_Are(2012).pdf?sequence=1(last visited 13 July 2015).

119 See INT’L COMM. RED CROSS, supra note 83.
solution to some of the challenges that are raised by the
doctrine of direct participation in hostilities like the
“revolving door dilemma”.\textsuperscript{120} This is when a protected
person regularly changes from civilian to combatant and
back to civilian again.\textsuperscript{121} Proponents of the CCF argue that
such a civilian may be viewed as assuming a continuous
combatant function.\textsuperscript{122} This means that a civilian who
regularly engages in hostilities is targetable even at a time
he or she is not directly involved in hostilities.\textsuperscript{123}

There is, however, a number of scholars who
disapprove of the CCF concept because it weakens the
protection of civilians and is inconsistent with the specific
treaty language that targeting must only be “for such time”
that a civilian is engaged directly in hostilities.\textsuperscript{124} Further,
they point out that the CCF concept has not been accepted
by many states as there is an insistence that civilians must
not be referred to as “combatants” and may only be
targeted when directly participating in hostilities.\textsuperscript{125} Thus,
some scholars have specifically condemned the use of
unmanned systems to targeted individuals on the basis of
CCF.\textsuperscript{126} The main reason is that there is no clarity as to
whether targeted individuals were, in fact, members of a
particular armed group or whether the terrorist group is an

\begin{itemize}
\item \textsuperscript{120} \textit{Melzer supra} note 54, at 347; Römer \textit{supra} note 96, at 62; \textit{Francesco Francioni \& Natalino Ronzitti, War By Contract: Human Rights, Humanitarian Law, and Private Contractors} 213 (2011).
\item \textsuperscript{121} \textit{Melzer supra} note 54, at 347; Melzer \textit{supra} note 82, at 1.
\item \textsuperscript{122} \textit{See Solis supra} note 117, at 205.
\item \textsuperscript{123} \textit{Id.}
\item \textsuperscript{124} \textit{See supra} note 64, at Art. 13(3).
\item \textsuperscript{125} Clapham \& Gaeta \textit{supra} note 16, at 321.
\item \textsuperscript{126} Sikander Shah, \textit{International Law and Drone Strikes in Pakistan: The Legal and Socio-Political Aspects} 183-85 (2014).
\end{itemize}
armed group in the first place.\textsuperscript{127}

A belligerent who chooses to target an individual on the basis of CCF doctrine carries an onerous burden to prove that the individual targeted was indeed assuming that role – a burden which the US has been reluctant to discharge as far as its targeting of suspected terrorists is concerned.\textsuperscript{128} The targeting of persons on the basis of suspicion that they are members of terrorist groups is condemned in the strongest terms and such condemnation extends to all use of unmanned systems – AWS included.

To this end, in order to comply with the rule of distinction, autonomous systems should not, in the first place, be programmed to target individuals on the basis of suspicion alone. Such occurrence is likely since one of the ways by which AWS will identify their targets is through the facial recognition that is coded into the computer of the system before it is deployed.\textsuperscript{129} Before someone’s facial features or identity is put into a robot, the rule of distinction would require at least that there should be a traceable record of that particular person’s involvement in hostilities.\textsuperscript{130}

Further, it is emphasized that in order for Autonomous Weapon Systems to comply fully with the rule of distinction, they should not be programmed to target all “associated forces and supporters of terrorist groups” as has been the case with drone targeted killings.\textsuperscript{131} It goes

\textsuperscript{127} Id.

\textsuperscript{128} Mary Ellen O’Connell, \textit{Unlawful Killing With Combat Drones A Case Study Of Pakistan}, \textsc{Notre Dame Law School Legal Studies Research Paper No. 09-43}, at 2 (July 2010).

\textsuperscript{129} See Geneva Academy \textit{supra} note 15.

\textsuperscript{130} This is in accordance with the rule on distinction.

\textsuperscript{131} Duffy \textit{supra} note 112, at 413.
without saying that targeting individuals on the basis of an "abstract affiliation" is inconsistent with the rule of distinction.\textsuperscript{132} Having discussed the status and requirements of the rule of distinction, I now turn to consider whether AWS are capable of complying with the standard above.

5. Autonomous Weapon Systems’ Capability to Comply with Distinction

In view of the challenges faced on the battlefield when it comes to distinguishing those directly taking part in hostilities and those who are not, the question is whether or not AWS will be able to comply with the rule of distinction.\textsuperscript{133} Of course, one of the fundamental and underlying considerations in this whole discussion is whether in the first place AWS should be allowed to make this legal calculation and judgment which has been the preserve of human combatants. To ask whether AWS can comply with the rule of distinction is like to “approach the courts with dirty hands”, it is like to question whether child soldiers are capable of complying with International Humanitarian Law – the case falls where it stands. As observed by Heyns, there are two questions to this matter: \textit{Can they do it and should they do it?} In my opinion, the question \textit{should they do it} takes precedence because robots cannot be actors in international law.

\begin{itemize}
\item \textsuperscript{132} Crawford supra note 98, at 123.
\item \textsuperscript{133} Clapham & Gaeta supra note 16, at 331, noting the difficulties in the practical application of the rule of distinction in contemporary armed conflicts; See also Schmitt supra note 92, at 699; Bill Boothby, \textit{And For Such Time As: The Time Dimension to Direct Participation in Hostilities}, 42 N.Y.U. J. INT’L L. & POL. 758 (2010).
\end{itemize}
a. How AWS select their targets

In order to fully discuss the above question on whether AWS can be able to comply with the rule of distinction, it is important to start by understanding some ways by which AWS will select their targets. Correct identification of legitimate targets is the crux of the rule of distinction which in armed conflict demands belligerents to distinguish between combatants and civilians whilst in human rights law lethal force must only be directed against lawful targets.\(^{134}\)

As noted above, the rule of distinction is applicable both to natural persons and objects\(^{135}\) with the intention of minimizing harm to civilians and their property.\(^{136}\) Just like humans, AWS are expected to distinguish civilians from combatants. To discriminate between civilian and military objects and personnel, AWS are expected to use devices like “cameras, infrared sensors, sonars, lasers, temperature sensors, and radars” etc.\(^{137}\) AWS will have some form of artificial intelligence, equipping them with definite “human like capabilities such as a pattern recognition, text parsing and planning/problem solving”.\(^{138}\)

There is a concern, however, as to whether the rule

\(^{134}\) *Supra* note 46, at Art. 48


of distinction as discussed above can be sufficiently translated into a computer code when currently International Humanitarian Law does not provide an adequate definition of a civilian that could allow AWS to correctly and lawfully select their targets.\(^{139}\) This is exacerbated by the complications and unpredictability nature of contemporary conflicts as highlighted above.\(^{140}\)

Notwithstanding the above concern, to make the sensory and visual discrimination in their targeting, AWS may rely on two aspects of identification. Firstly, the appearance of the target – this includes aspects such as facial recognition where the target is human – and other distinctive signs such as military uniforms.\(^{141}\) In relation to appearance-based targeting, AWS are “programmed to recognize who the enemy is and what objects belong to the enemy”.\(^{142}\) In order to recognize this distinction in a consistent manner, AWS are expected to have advanced image recognition technology incorporated in them.\(^{143}\)

As far as selection of targets on the basis of facial recognition is concerned, targeting by AWS may be more

\(^{139}\) Supra note 46, at Art. 50(1) (defining a civilian in the negative sense as someone who is not a combatant whilst the Geneva Conventions more fully require the use of common sense in ascertaining who is a civilian); See also Sharkey supra note 137, at 788-89.

\(^{140}\) See CAROLINE HARVEY ET AL., CONTEMPORARY CHALLENGES TO THE LAWS OF WAR: ESSAYS IN HONOUR OF PROFESSOR PETER ROWE 86 (2014).

\(^{141}\) See Peter Finn, A future for drones: automated killing, WASHINGTON POST (Sept. 19, 2011); see also Noel Sharkey & Lucy Suchman, Wishful Mnemonics and Autonomous Killing Machines, 136 PROCEEDINGS OF THE AISB 14-22 (May 2013).

\(^{142}\) Jeffrey Thurnher, No One at the Controls: Legal Implications of Autonomous Targeting 67 JOINT FORCE Q. 80 (2012).

\(^{143}\) KRISHAN, supra note 138, at 2.
However, such criteria will be limited to targeted killings of known individuals as opposed to the general members of an armed force or group.

As regards to other appearance or forms such as military uniforms, military instalments and other distinctive marks, it remains to be seen whether it is possible technologically, for AWS and their sensors to distinguish military uniforms of its own soldiers – given that most uniforms worldwide are camouflage – and own military installations from those of the enemy. In essence, it may be very easy for the enemy to deceive AWS by, for example, carrying marks that are considered friendly. One can imagine what an Autonomous Weapon System would do in a situation where it is deployed alongside human soldiers who then happen to be captured or become hors de combat in the hands of the enemy. Will AWS be able to distinguish its own soldiers from enemy soldiers who are all dressed in camouflage? Will the presence of their own soldiers amongst the enemy stop AWS from engaging the enemy soldiers? How about installations and armored vehicles belonging to peace keeping missions?

More importantly, the rule of distinction demands that civilian objects should be distinguished from military objects. It is not new that sometimes civilian objects may

---

144 See Armin Krishan, Autonomous Weapons Systems and the Future of War, E-INTERNATIONAL RELATIONS (May 27, 2013), http://www.e-ir.info/2013/05/27/autonomous-weapons-systems-and-the-future-of-war/ (noting that “an autonomous micro-drone could be sent to search for a particular individual using biometrical identification methods (e.g. facial recognition or DNA analysis) and kill this individual with high precision and with no collateral damage.”) (last visited Apr. 13, 2015).

145 See Id.

146 BASAK CALI, INTERNATIONAL LAW FOR INTERNATIONAL RELATIONS 246 (2010).
have dual use, used by both civilians and soldiers or may be abused to a certain extent by fighters.\textsuperscript{147} This is where a human soldier is required to make a value judgment, proportional calculations in order to comply with the rule of distinction.\textsuperscript{148} If AWS without “Meaningful Human Control” are going to be programmed to attack, the question is whether in some of these circumstances they will be able to make these value judgments to comply with the rule of distinction.

The second criterion for selection of targets is based on the patterns of behavior or conduct of the targeted individual.\textsuperscript{149} This type of selection of targets is more relevant in current armed conflicts especially non-international armed conflicts (NIAC), where in most cases fighters do not have uniforms.\textsuperscript{150} In that regard, targeting—even by human soldiers—has been on the basis of one’s conduct, which is direct participation in hostilities as discussed above.\textsuperscript{151}

Ascertaining that a civilian is directly participating in hostilities is difficult. Like in the case of human combatants, it is expected that AWS will have difficulties ascertaining legitimate targets on the basis of conduct.\textsuperscript{152} Carrying of arms alone does not make one a legitimate target.\textsuperscript{153} There are many ways by which AWS may

\textsuperscript{147} HENDERSON, supra note 91, at 59.
\textsuperscript{148} On assessing the degree of usage for a civilian object to be targetable, see Bouchet-Saulnier, supra note 70, at 270.
\textsuperscript{149} Thurnher supra note 142.
\textsuperscript{150} SANDESH SIVAKUMARAN, THE LAW OF NON-INTERNATIONAL ARMED CONFLICT 417 (2012).
\textsuperscript{151} 151 Supra note 46, at Art. 51(3).
\textsuperscript{152} SINGER, supra note 19, at 402.
\textsuperscript{153} TOMIS KAPITAN, PHILOSOPHICAL PERSPECTIVES ON THE ISRAELI-PALESTINIAN CONFLICT 150 (1997).
misconstrue a person’s conduct either to the detriment of the person or to their own detriment.\(^{154}\)

To be fair, if AWS were to be deployed in certain environments for example where there are only combatants or fighters, they may be able to comply with the rule of distinction to some extent since in those circumstances the battlefield is less complicated.\(^{155}\) An example is where a soldier in a desert would activate an Autonomous Weapon System to search for a particular individual or enemy. Now that they are no civilians or other protected persons in the desert hence no need for proportional calculations and other value judgments, it is likely that the system may not violate the rule of distinction.

It should be remembered nevertheless, that the rule of distinction does not only seek to protect civilians but also fighters who surrender or who become *hors de combat* by virtue of wounds or sickness.\(^{156}\) In the above example, a situation may arise that after activation of the Autonomous Weapon System to hunt for a specific person; the person may seek to surrender or may become *hors de combat* by virtue of sickness or wounds. The fundamental question becomes whether AWS have the technological advancement to take note of this and refrain from targeting. Failure to do so or attacking a surrendering fighter or one who is no longer participating in hostilities by virtue of wounds or sickness would be a violation of the rule of

\(^{154}\) Of course in the case of AWS the detriment is to the one who deploys them.


Furthermore, in many situations, it can be argued that AWS may be incapable of complying with the rule of distinction. This is so because of four major reasons: technological limitations of AWS, lack of precise definitions in international humanitarian law, the nature of today’s armed conflict that demands in many instances human judgement and technical fault or possible malfunctioning of AWS.

b. Technological limitations of AWS to comply with rule of distinction

One of the major reasons noted as to why AWS will be unable to comply with the rule of distinction is that there are technological limitations of AWS which makes it impossible for them to be designed in a way that can comply with the rule of distinction. We do not have the necessary or adequate technology to design AWS with sufficient artificial intelligence that would allow them to

---

157 See Id.


159 INT’L COMM. RED CROSS supra note 89, at 7.


162 A/HRC/23/47, supra note 2, at ¶ 90.

163 INT’L COMM. RED CROSS, at 7.
discriminate targets in accordance with the law.\textsuperscript{164}

Scholars have articulated various situations within which AWS may fail to sufficiently discriminate in terms of the law. One of such examples is where AWS may fail to distinguish civilians from combatants due to failure to ascertain identity.\textsuperscript{165} This may be due to what roboticist Noel Sharkey notes as limitations of existing sensors to make proper identification.\textsuperscript{166}

In his presentation during the 2014 CCW Meeting on AWS, Sharkey noted that programming of the simplest of software that is needed to make AWS IHL compliant will take several decades.\textsuperscript{167} Another example is where AWS may fail to interpret conduct of an individual, as to whether one is directly participating in hostilities or not as noted above. In this regard, Noel Sharkey has referred to possible situations where an autonomous system may mistakenly gun down a child who is running around with a toy gun towards it.\textsuperscript{168} In those cases, Sharkey argues that human judgment is vital as a human combatant would understand such a situation while a robot cannot.\textsuperscript{169}

More so, as already noted above, it is doubted

\begin{footnotesize}
\begin{enumerate}
\item Id.
\item Sharkey \textit{supra} note 2.
\item N Sharkey, \textit{supra} note 2, at 88-89.
\item \textit{See} Noel Sharkey, Presentation, Toy soldiers to killer robots: Prof Noel Sharkey at TEDxSheffield 2013, \textit{available at} https://www.youtube.com/watch?v=kjRV9FzdQNk&hd=1 (last visited Apr. 13, 2015).
\item Id.
\end{enumerate}
\end{footnotesize}
whether AWS will have sensors that are advanced enough to note that someone is about to surrender or is in pain due to wounds and therefore eligible for protection since the person is now hors de combat.\textsuperscript{170} Of course, there are current roboticists who claim that there are robots which are able to sense whether one is in pain or faking it.\textsuperscript{171} Whether such software will be installed in AWS remains to be seen.

However, as far as a possible scenario of a fighter or combatant surrendering is concerned, there are two hurdles that may be impossible to overcome. Firstly, on the battlefield, to ascertain whether one is surrendering or is about to surrender requires the ability – at least to some degree – to be able to read human intention.\textsuperscript{172} It is unlikely that AWS may be able to read human intention.\textsuperscript{173} Secondly, the current form of AWS like the X47B and the Taranis are in the form of drones the only difference being that no one is at the controls. Since most of these AWS will be flying hundreds if not thousands of feet high, it is practically impossible to surrender to them.\textsuperscript{174}

\begin{footnotes}
\item[170] HENSEL supra note 16, at 222.
\item[172] INT’L COMM. RED CROSS, at 12.
\item[174] See Advancing the Debate on Killer Robots: 12 Key Arguments for a Pre-Emptive Ban on Fully Autonomous Weapons, HUMAN RIGHTS WATCH (May 13, 2014), available at https://www.hrw.org/news/2014/05/13/advancing-debate-killer-robots; see also What are the problematic issues related to the development of autonomous weapons?,
\end{footnotes}
opportunity to surrender is ultimately taken away – a situation almost equivalent to giving an “order that there shall be no survivors” which is prohibited under the laws of international humanitarian law.\textsuperscript{175}

Although this is related to technological limitation, the following argument is more of a programing and design limitation on AWS. The definition of AWS is that once they are activated, they require no further human intervention.\textsuperscript{176} If such AWS are deployed, it is highly likely that they may violate the rule of distinction at a certain stage. A legitimate target, I argue, can turn into an illegitimate target during the course of an attack for several reasons some of them I have already addressed above.\textsuperscript{177} For that reason, if there is no one at the controls, when the status of the target changes to that which is protected by the laws of war, then the system will, from that stage henceforth, violate the rule of distinction.

c. The challenge of definitional imprecision of IHL terms

As already noted, defining a civilian who is directly participating in hostilities, who can be designated as a continuous combatant function, who is a combatant or what is meant by a military objective is a daunting task. There remains a definitional deficiency or uncertainty of these

\textsuperscript{175} JONATHAN CROWE \& KYLIE WESTON-SCHEUBER, PRINCIPLES OF INTERNATIONAL HUMANITARIAN LAW 67 (2013); HENCKAERTS, supra note 14, at 163.
\textsuperscript{176} A/HRC/23/47, supra note 2, at ¶ 38.
\textsuperscript{177} For example if an individual becomes \textit{hors de combat} by virtue of wounds or sickness.
International Humanitarian Law terms despite the International Committee of the Red Cross’s continued effort to give clarity to some of these terms.

The question at this stage becomes how to translate imprecise terms that are subject to case by case application into a computer. If anything, the basic rule of computers is precision, no wonder one of the basic lessons to a computer science learner is what have become to be known as “Garbage In, Garbage Out” (GIGO). This means that “if invalid data is entered in a computer program, the resulting output will also be invalid”. To the same end, if weapon systems are going to be programmed and coded with imprecise definitions, what we are going to get are imprecise outcomes – much to the violation of the rule of distinction. The question may be: How then are these definitions being used as they currently stand? The answer is simple: - humans on the battle field continue in every circumstance to use discretion, human judgment and deliberation which is most suited if not needed to make most of these definitions workable.

To this end, Asaro augmenting Sharkey points out that the complexity and absence of clarity in terms that are used in International Humanitarian Law in particular as to who qualifies as a combatant or civilian makes it impossible for the definitions to be sufficiently translated

---

179 See Id.
180 On the importance of human judgement, see INT’L COMM. RED CROSS, at 21,26,32,72; U.S. DEP’T DEF., supra note 20; Asaro supra note 2, at 696; Geneva Academy, supra note 15.
into computers. The end result is that AWS that will be programmed on the basis of the current definitions and subsequently unleashed without “Meaningful Human Control” pose a high risk of not being able to comply with the rule of distinction.

d. The nature of contemporary armed conflicts and impracticability of AWS

As I have already highlighted above, the nature of contemporary conflicts, where there is civilianization of armed conflicts, requires that a human being, with all the situational awareness and discernment, be present at the point when force is deployed to ascertain the correctness of targets. This point has been noted by Human Rights Watch which notes that most cases of today’s armed conflict have taken the form of asymmetric warfare.

More often than not, it is difficult to distinguish who is directly participating in hostilities, therefore making human judgement enigmatically important in interpreting emotions and intentions for accurate identification of legitimate targets. Thus, the arguments that have been made by certain scholars that AWS should not be outlawed because there are certain circumstances where in a closed environment and removed from civilians AWS can be used legally, fails to appreciate the nature of contemporary

181 Asaro supra note 2, at 11.
182 See Sharkey supra note 137; N Sharkey supra note 2.
183 Id.
184 WILLIAM BANKS, NEW BATTLEFIELDS/OLD LAWS: CRITICAL DEBATES ON ASYMMETRIC WARFARE (2013).
185 HUMAN RIGHTS WATCH, supra note 158, at 31.
conflicts.

Furthermore, not only does the above argument is similar to the one that was being made in favor of nuclear weapons that they can be used in certain environments in accordance with the law, but also fails to appreciate the nature of contemporary armed conflicts wherein these AWS are likely to be used. It would be an error to fail to recognize that one of the major factors that have influenced the production of unmanned systems such as drones is the idea of using them against terrorist without risking one’s personnel.186 Terrorists’ *modus operandi* is to blend in with civilians and fight from within the civilian population.187 Therefore, to argue that states will spend billions of dollars to develop a state of the art weapon only to wait to use it in a highly improbable situation where they find a terrorist tottering alone in a lone desert is too theoretical and academic.

The ICRC has interpreted Article 36 of Additional Protocol 1 on the review of new weapons to the effect that when considering the lawfulness of new weapons, it is its probable and normal use of the weapon that should be taken into consideration.188 It is within reason that most of the Autonomous Weapon Systems like the X47B will be used in the war on terror just like their predecessor – armed drones.189 The environment in which these high-tech

186 *See generally* MEDEA BENJAMIN, DRONE WARFARE: KILLING BY REMOTE CONTROL (2013).
187 *See generally* MATTHEW EVANGELISTA, LAW, ETHICS, AND THE WAR ON TERROR (2013).
189 *See BENJAMIN supra* note 186.
weapons are likely to be used makes it difficult if not impossible to comply with the rule of distinction.

e. Technical fault or malfunctioning of AWS and the rule of distinction.

Another fundamental issue that may threaten the rule of distinction is that these systems may malfunction and, as a result, violate this important rule. There are definitely several reasons why the said malfunction is possible. There have been situations where some of these unmanned autonomous systems malfunctioned; turning against the persons deploying them and in some cases actually killing individuals by mistake.\(^\text{190}\)

Of course, the immediate response to the above argument is that humans make mistakes too. However, here I refer to the argument that is propounded by Heyns: where a belligerent chooses to use high-tech weapons, the standard should be raised higher.\(^\text{191}\) If there is a possibility that these weapon systems may malfunction, then they should remain under human control – a human combatant or fighter who supervises them so that he or she may override, terminate or abort missions the moment it becomes clear that the system is malfunctioning.\(^\text{192}\)


\(^{191}\) Discussion by Thompson Chengeta and Professor Christof Heyns.

\(^{192}\) Sharkey *supra* note 2.
f. The argument that AWS can comply with distinction better than humans.

It would be an injustice to conclude this section without referring to some of the arguments that have been made that AWS are capable of complying with the rule of distinction and other rules to be discussed below – better than humans can.\textsuperscript{193}

Arkin is amongst the leading scholars postulating that it is possible not only to create AWS capable of complying with the rules of distinction and others but even so – better than humans.\textsuperscript{194} He argues that it is possible to integrate “a moral faculty” into AWS through components such as “a transformer/suppressor of system-generated lethal action” (ethical governor) whose purpose is to ensure better compliance with the law.\textsuperscript{195}

According to Arkin, there are about four elements that can be coded into AWS to comply with the law namely; “(1) post facto suppression of unethical behavior, (2) behavioral design that incorporates ethical constraints from the onset, (3) the use of affective functions as an adaptive component in the event of unethical action, and (4) a mechanism in support of identifying and advising operators regarding the ultimate responsibility for the deployment of such a system”.\textsuperscript{196}

\textsuperscript{193} Arkin \textit{supra} note 18; See also Arkin, \textit{Governing Lethal Behavior}, \textit{supra} note 18, at 127.
\textsuperscript{194} Arkin \textit{supra} note 18; See also Arkin, \textit{Governing Lethal Behavior}, \textit{supra} note 18, at 127.
\textsuperscript{195} Arkin \textit{supra} note 18; See also Arkin, \textit{Governing Lethal Behavior}, \textit{supra} note 18, at 127.
\textsuperscript{196} Arkin \textit{Governing Lethal Behavior}, \textit{supra} note 18, at 1.
A reading of Arkin’s article may give an idea that it is possible to create an ethical robot. Nevertheless, during a debate on AWS between him and Robert Sparrow, Arkin conceded that a robot can never be termed ethical, especially from a philosophical point of view. Such a concession may not, however, mean that a robot cannot act ethically.

Citing scholars like May and others who attribute war atrocities to human emotions such as “the passion for inflicting harm, the cruel thirst for vengeance, an unpacific and relentless spirit, the fever of revolt, the lust for power, and suchlike things.” Arkin argues that because AWS are devoid of human emotions, they can do a better job in complying with international humanitarian law rules such as the rule of distinction. He insists that the current state of affairs on the battlefield is unacceptable therefore making it imperative to develop AWS.

To this end, Schmitt argues that from the beginning it should be understood that AWS are not unlawful weapons per se, as their autonomy does not mean that they cannot comply with important rules like distinction and weapons law rules on the prohibition of those that cause unnecessary or superfluous injury. For that reason, he argues that recommendations to ban Autonomous Weapon

199 Arkin, Governing Lethal Behavior, supra note 18, at 2.
200 See Georgia Tech Center for Ethics & Technology supra note 197.
Systems are “insupportable as a matter of law, policy, and operational good sense”.\textsuperscript{202}

When I addressed the argument that there is the possibility of AWS malfunctioning, I noted my concurrence with Heyns that if a state is to use these high-tech weapons, the standard must be higher.\textsuperscript{203} However, in support of Arkin’s proposals, Patrick Lin postulates that “scientists and engineers need not first solve the daunting task of creating a truly ‘ethical’ robot, at least in the foreseeable future; rather, it seems that they only need to program a robot to act in compliance” with IHL which is “a low standard to satisfy”.\textsuperscript{204} To that end, Lin argues that the question should not be whether robots should be infallible but whether they can perform better than humans as far as compliance with the law is concerned.\textsuperscript{205} Comparing humans to machines, Martin Cook states that “human beings fall short of [the already low] standard with depressing regularity”.\textsuperscript{206}

g. On whether the possibility of robots performing better than humans is the crux of the matter

\textit{State a moral case to a ploughman and a professor. The former will decide it as well, and often better than the latter because he has not been led astray by artificial rules.}\textsuperscript{207}

\textsuperscript{202} Id., at 3.
\textsuperscript{203} Supra note 91.
\textsuperscript{204} Patrick Lin et al., \textit{Robots in War: Issues of Risk and Ethics} in \textit{Ethics and Robotics} 50 (Capurro & Nagenborg eds., 2009).
\textsuperscript{205} Id.
\textsuperscript{207} Arkin, \textit{Governing Lethal Behavior}, supra note 18 (quoting Thomas
As to whether AWS can be better than humans in when it comes to complying with the rules of International Humanitarian Law such as distinction, Marchant et al and relying on Arkin’s 2011 paper\textsuperscript{208}, refer to a number of reasons why they can be better.\textsuperscript{209} According to these scholars, since AWS are created without emotions, they do not act out of anger, frustration, revenge fear or hysteria which in the battle field always influences human combatants to “press toward fearful measures”.\textsuperscript{210}

More so, because AWS are non-human without the need of self-preservation, they can act conservatively, for example, using lethal force only when they are fired upon.\textsuperscript{211} Furthermore, it is considered that AWS’ robotic sensors give them better “battlefield observations” compared to humans and their advanced processors allow them to analyze information from different sources faster and more accurate than humans, who, in today’s technological warfare have thus become the weakest link as far as information processing is concerned.\textsuperscript{212} Over and above, Marchant hints on the potential capability of AWS to “independently and objectively” monitor the “ethical behavior on the battlefield by all parties and reporting infractions that might be observed”.\textsuperscript{213}

If the above arguments pro-AWS hold water, Jonathan Herbach argues that there would be an obligation

\begin{flushleft}
\textsuperscript{208} Arkin, \textit{Governing Lethal Behavior}, \textit{supra} note 18, at 6.
\textsuperscript{209} Marchant, \textit{supra} note 8, at 280.
\textsuperscript{210} MICHAEL WALZER, \textit{JUST AND UNJUST WARS} 251 (1977).
\textsuperscript{211} Marchant, \textit{supra} note 8, at 280.
\textsuperscript{212} \textit{Id}.
\textsuperscript{213} \textit{Id}.
\end{flushleft}
to use them\textsuperscript{214} since even the ICRC considers that “any weapon that makes it possible to carry out more precise attacks, and helps avoid or minimize incidental loss of civilian life, injury to civilians, or damage to civilian objects, should be given preference over weapons that do not”\textsuperscript{215}.

However, as much as it is true that AWS will not act in self-preservation, waiting to be fired upon first thereby targeting only those who are immediately participating in hostilities, this argument again fails to take into account the realities of the form of the technology and the context within which it will be used. To start with, with AWS that may be used to hunt and kill perceived terrorists, it is highly unlikely that terrorists will see it and shoot at it. For that reason, it would be useless that billions of dollars will be spent on the development of a weapon whose offensive is only triggered upon it being shot at first. Above all things, if the enemy combatant will know that the robot only attacks after being attacked, why on earth would one risk their life by attacking it? Where one would choose to attack it, surely it will not be to “bruise” it but to totally disenable it. Are states willing to have billions of dollars put to waste through this way? It is unlikely.

Regarding the argument that AWS will be able to process information faster thereby making decisions quicker as far as targeting is concerned, it is agreeable that


this may be advantageous when it comes to precision. Nevertheless, precision in targeting does not necessarily mean that those targeted are lawful targets. This goes back to the argument I noted above: it all depends on the correctness of the information the AWS is processing faster than humans – garbage in garbage out.\textsuperscript{216} If the sensors of an AWS are unable to correctly identify targets, then the information so gathered is erroneous and will lead to the violation of the rule of distinction and other rules.

More importantly, as I have noted when I addressed the rule of humanity above, the rules of International Humanitarian Law work in unison – they complement each other. The ultimate goal of these rules is not only to save lives of protected persons;\textsuperscript{217} it is also to protect the right to dignity of both protected persons and fighters.\textsuperscript{218} That is where the rule of humanity comes into play. Thus, even if in certain situations AWS may be able to comply with the rule of distinction thereby satisfying the \textit{can they do it} question, it still needs to be considered whether they \textit{should do it} which falls under the rule of humanity articulated above.\textsuperscript{219}

To summarize the arguments, I have made on the rule of distinction and whether AWS without “Meaningful Human Control” can comply with this rule, I note that the rule of distinction is the corner stone for the protection of civilians and other protected persons. This rule has

\begin{flushleft}
\textsuperscript{216} \textit{See GIGO supra} note 178.
\textsuperscript{217} \textsc{Curtis Doebbler}, \textsc{Introduction to International Humanitarian Law} 39 (2005).
\textsuperscript{218} \textsc{Gerd Oberleitner}, \textsc{Human Rights in Armed Conflict} 102 (2015).
\textsuperscript{219} Professor Christof Heyns in his forthcoming paper discusses the legal question can AWS do it and if they can do it the moral question should they do it.
\end{flushleft}
acquired the status of *jus cogens* and should be respected. Understanding the definition of a civilian, direct participation in hostilities and other terms is fundamental for the purposes of implementing the rule. The existing definitions are not clear cut and are delicate; they are subject to change depending on the conduct of the individual in a particular circumstance. Protection available to persons in terms of this rule is, therefore, fluid, changing depending on particular circumstances. For that reason, it is difficult if not impossible to translate these definitions sufficiently into AWS. Furthermore, the technological limitations of AWS, the uncertainties of the nature of contemporary conflicts, the confusing role played by civilians in these conflicts makes one conclude that AWS without “Meaningful Human Control” will not be able to comply with the rule of distinction.

C. *IHL Rule of Proportionality and AWS*

Another important rule in International Humanitarian Law is the rule of proportionality. While the principle of distinction demands that a belligerent must distinguish between military and civilian objectives, it is common place that a strike on a military object may have an effect on civilian objects.\(^{220}\) In International Humanitarian Law, incidental harm is acceptable but only when it complies with the rule of proportionality.

The rule of proportionality is a rule of customary international law\(^{221}\) prohibiting attacks on military


objectives that have can extreme “incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof” that cannot be justified by any “concrete and direct military advantage anticipated”.

The rule of proportionality is not a stand-alone rule but a critical element of the rule of distinction – in that an attack that causes disproportionate harm to a civilian may in certain circumstances be considered an indiscriminate attack. While the rule of distinction concerns itself with “which things may be attacked”, the rule of proportionality focuses on “how things may be attacked”. It thus prohibits a belligerent from choosing a means or method of warfare that will cause disproportionate harm to the military advantage anticipated.

In relation to weapons, a combatant is obliged to first consider the impact of a particular weapon in a particular context and only choose a weapon that has a higher degree of precision in order to minimize incidental harm. Fighters must choose means and methods of warfare that save the lives of civilians. This is the same consideration when complying with the rule on precaution.

---

222 Supra note 46, at Art. 51(5); See CROWE & WESTON-SCHEUBER supra note 178, at 55; Fleck supra note 21, at 160; CRAWFORD supra note 98, at 174.


224 CROWE & WESTON-SCHEUBER supra note 178, at 55; Fleck supra note 21, at 160; EMILY CRAWFORD & ALISON PERT, INTERNATIONAL HUMANITARIAN LAW 174 (2015).

1. Calculating Proportionality

The calculation of whether certain collateral damage is excusable is on a case by case basis and in many circumstances requires a human judgment that allows an all-round assessment of the situation.\(^{226}\) To that end, Heyns notes that “proportionality assessments often involve qualitative rather than quantitative judgments”\(^{227}\) – assessments which at present can only be done by humans. It is for that reason that Sharkey insists that the lack of human judgement in AWS will make it impossible for them to comply with the rule of proportionality.\(^{228}\) Thus, Krishnan perceives situations where AWS may launch an attack based on misconceptions of the context.\(^{229}\)

One scholar thus observes that “proportionality could be like an elephant, difficult to define but easy to recognize”.\(^{230}\) For the same reasons as have been cited concerning other rules, AWS will not be able to comply with the rule of proportionality if humans are out of the loop or not in “meaningful control” of them once they are activated. The rule of proportionality is also linked to the

\(^{226}\) On importance of human judgement see INT’L COMM. RED CROSS supra note 89, at 21,26,32,72; U.S. DEP’T DEF., supra note 20; Asaro supra note 2, at 696; Geneva Academy, supra note 15.


\(^{228}\) Noel Sharkey, Automated Killers and the Computing Profession 40 COMPUTER 122 (2007).

\(^{229}\) Krishnan supra note 138, at 98-99.

\(^{230}\) Hampson supra note 60, at 54.
rule of military necessity.\textsuperscript{231}

\textit{D. IHL Rule of Precaution and AWS}

The IHL rule of precaution is codified in Article 57 of Additional Protocol I (API) to the Geneva Conventions. The rule of precaution is part of customary international law.\textsuperscript{232} It is important to emphasize that this is a rule of customary international law because some states that are involved in the development of AWS, such as the United States and Israel, are not party to API. \textsuperscript{233}

The ICRC’s Customary International Humanitarian Law Database provides that Article 57 of API codified existing customary international law.\textsuperscript{234} This supports the argument that in warfare, the rule of precaution has always existed, even before the codification of International Humanitarian Law. The rule of precaution is closely related to the rule of distinction.\textsuperscript{235} The objective of the rule of precaution is to make sure that protected persons do not lose their protection as a result of error or irresponsible use of force.\textsuperscript{236}

Some commentators observe that unlike in the past, the rule of precaution has become important on account of the nature of today’s armed conflict. David Herbach observes that in “the changing nature of 21st century armed

\begin{itemize}
\item \textsuperscript{231} Crowe \textit{supra} note 175, at 56.
\item \textsuperscript{233} Id.
\item \textsuperscript{234} ICRC, \textit{supra} note 52 (citing rules 16 and 18).
\item \textsuperscript{235} Herbach, \textit{supra} note 232, at 5.
\item \textsuperscript{236} Geneva Convention Relation to the Protection of Victims of International Armed Conflicts (Protocol I), art. 57, June 8, 1978.
\end{itemize}
conflict” it is difficult to target enemies who “are more mobile, more difficult to identify, and often ensconced among the civilian population within populated areas, a situation in which the elements of precaution are of the highest importance.”

The rule of precaution is codified in Article 57 of Additional Protocol I, which provides as follows:

Article 57 — Precautions in attack
1. In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.
2. With respect to attacks, the following precautions shall be taken:
   a) those who plan or decide upon an attack shall:
      i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;
      ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;
      iii) refrain from deciding to launch any 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;
   b) an attack shall be cancelled or suspended if it

237 Herbach, supra note 235, 4.
becomes apparent that the objective is not a military one or is subject to special protection or that the attack 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;
c) effective advance warning shall be given of attacks which may affect the civilian population, unless circumstances do not permit.
3. When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.
4. In the conduct of military operations at sea or in the air, each Party to the conflict shall, in conformity with its rights and duties under the rules of international law applicable in armed conflict, take all reasonable precautions to avoid losses of civilian lives and damage to civilian objects.
5. No provision of this Article may be construed as authorizing any attacks against the civilian population, civilians or civilian objects.

Understood in terms of Article 57, the rule of precaution thus refers to measures and actions “taken in advance of a particular action in order to prevent or avoid harm foreseeable to be caused by that action.”\textsuperscript{238} Herbach suggests that the way the rule of precaution is understood in International Humanitarian Law is the same as in

\textsuperscript{238} \textit{Id.} at 7.
environmental law, in the sense that “the risk of harm or undesired results is the measuring stick rather than the certainty of outcomes.”

Article 57 places an obligation to comply with the rule of precaution on planners of attacks or military operations. However, it seems the wording of Article 57 may raise challenges when it comes to autonomous systems. Questions arise as to whether those who assemble and program Autonomous Weapon Systems are considered planners who are bound by the International Humanitarian Law rule of precaution. There is an extreme danger in “equating operation programming of a military combat robot with attack planning as it might draw civilian technicians into non-civilian roles, or in other words result in civilians taking a direct part in hostilities.”

Furthermore, planning of an attack is subject to re-planning during the course of the attack that may be necessitated by the change of circumstances on the battlefield. In this sense, where autonomous systems are responsible for re-planning, do they become planners of the attack and hence actors in their own right? My position at this stage is that given the intricacies of the rule of precaution and the need for its constant application throughout a military attack, AWS without “Meaningful Human Control” are unlikely to comply with the rule of precaution.

Likewise, the rule of precaution provides that when planning attacks, there should be consideration of the effects of the attack.

\[239\] Id.
\[240\] Id. at 8.
Article 58 — Precautions against the effects of attacks

The Parties to the conflict shall, to the maximum extent feasible:

a) without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;

b) avoid locating military objectives within or near densely populated areas;

c) take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.

The question that arises is whether AWS without “Meaningful Human Control,” once activated, would be able to take precaution as far as the effects of the attack are concerned. The inability to control the effects of an attack may lead such an attack to be indiscriminate, which is contrary not only to the rule of precaution, but also to the rule of distinction. Now that such AWS lack human judgement, it is unlikely that the rule of precaution will be complied with.  

For what it is worth, the rule of precaution demands that when Autonomous Weapon Systems exercise their selection of targets, precaution must be taken in verifying targets and also making sure that there is the minimization of harm to innocent civilians. There are many forms of precautions that a belligerent should take. Many of them resonate from the provisions of the Geneva Conventions

---

241 Id. at 17-19.
and their Additional Protocols. The following are some of the precautionary measures and considerations that a belligerent or combatants must take before initiating an attack:

1. Uncertainties regarding the status of an individual

It is common place in contemporary armed conflicts that the status of a particular individual as to whether they are a civilian or not, and whether they are participating in hostilities or not, may be difficult to ascertain. In those circumstances, the law demands that the following precautions be taken. Firstly, in terms of the rule of distinction, one must be certain of the status of the target and not only suspect such status. Secondly, where there is uncertainty as to whether an individual is a civilian or not, the individual must be presumed to be a civilian. Thirdly, in relation to uncertainties as to whether a particular civilian is directly participating in hostilities, a presumption must be held in favor of the individual that his or her actions do not amount to direct participation in hostilities. Without a doubt, these intricacies require human judgment and individual assessment of each case. It is unlikely that AWS would be able to make these assessments and take presumptions in line with the law.

---

243 Id.
2. Assessment of choices of weapons available to belligerent

In terms of Article 57, the rule of precaution also demands that a belligerent assess the choices of weapons at its disposal. It is the means or weapons that limit collateral damage to the greatest extent possible that the attacking state must choose.\textsuperscript{245} Herbach suggests that this standard is subjective; it depends on the tools or weapons that are in the hands of a state.\textsuperscript{246} Where, for example, a state has advanced technology, the standard of precaution that the state must take before attacking is high.\textsuperscript{247} Most of the unmanned systems like drones and Autonomous Weapon Systems have advanced surveillance capabilities and this should raise the bar for the kind of precaution that the possessor of this technology takes when targeting.\textsuperscript{248}

3. Verification of the basis on which an individual is targeted

In current armed conflicts, where most targeting decisions are made on the basis of information gathered by intelligence, the rule of precaution would require belligerents first and foremost to gather reliable information.\textsuperscript{249} The information that is used as the basis for targeting an individual must be verified independently.\textsuperscript{250}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{245} Geneva, \textit{supra} note236, at 57.; \textit{See also} Herbach \textit{supra} note 235, at 7.
\item \textsuperscript{246}Herbach, \textit{supra} note 235, at 7.
\item \textsuperscript{247}\textit{Id.}
\item \textsuperscript{249} Geneva, \textit{supra} note 236 (citing art. 57(2)(a)(i)).
\item \textsuperscript{250} Geneva, \textit{supra} note 236 (citing art, 57(2)(a)(iii)).
\end{itemize}
\end{footnotesize}
MEASURING AUTONOMOUS WEAPONS . . . [2016]

Failure to thoroughly verify information concerning targets not only violates the rule of precaution, but rules of distinction\(^{251}\) and proportionality\(^{252}\).

4. Assessment of the environment where the target is located

After verifying a target as a military target, a belligerent according to the rule of precaution must assess the location within which the target is situated\(^{253}\). Combatants and fighters must desist from attacking if the target is located where there are too many civilians who may be injured or killed\(^{254}\). That assessment must be done in good faith and with a clear understanding of the law that “presence within the civilian population of individuals who do not come within the definition of civilians does not deprive the population of its civilian character.”\(^{255}\)

5. Warning civilians in the environment of impending attack

Where there are civilians in the vicinity of a verified target, the rule of precaution would require a belligerent to inform or give civilians a warning of an imminent military operation. During the war, such kinds of warnings have been considered by many scholars to be impractical\(^{256}\). This

\(^{251}\) ICRC, *supra* note 52 (citing rule 6).

\(^{252}\) Geneva, *supra* note 236 (citing art. 51(5)(b)).

\(^{253}\) *Id.*

\(^{254}\) *Id.*

\(^{255}\) Geneva, *supra* note 236 (citing art. 50(3)).

brings one to the language that is used in Article 57 of Additional Protocol I. Belligerents are required to take all *feasible* precaution. Herbach has considered what is meant by feasible, and concluded that the term “does not denote a specific obligation of the result but rather one of effort or due diligence in accordance with military objectives.”257 To that end, feasible precautions refer to those that are “practicable or practically possible, taking into account all circumstances including humanitarian and military considerations prevailing at the time that the plans or decisions are made or the actions undertaken.”258

**E. AWS and The Rule of Precaution**

Questions arise whether AWS, especially those without “Meaningful Human Control” would be able to abide by the rule of precaution. To begin, precaution starts right from the moment where a belligerent plans an attack. As already noted, in planning an attack a belligerent must carefully choose the means to be employed in that attack.259 It may be questioned whether a belligerent who chooses to employ AWS without “Meaningful Human Control” once activated can be said to be complying with the rule of precaution. For the reasons I have already referred to when I discussed the rule of humanity and distinction above, a belligerent who chooses to employ AWS without “Meaningful Human Control” once they are activated is throwing precaution out of the window. AWS are unpredictable, especially in unstructured environments;

258 *Id.*
deploying them all the same is taking chances with the lives of protected persons. Where a belligerent chooses to gamble with the lives of protected persons, surely that is contrary to the essence of the rule of precaution.

Of course, the rule of precaution demands that where a belligerent is in possession of weapons that are more precise and minimize civilian harm, such weapons must be used. The first issue is that AWS are not weapons in the strict sense of the word. A belligerent who chooses to use child soldiers ignores the rule of precaution because children do not have a moral responsibility, which is an important element wherever force is used. The same argument can be invoked in the case of bloodless machine combatants.

Arguments have been made that AWS will save lives because unlike humans, they will not act out of malice or the need to self-preserve. Some scholars have also noted the utility of robotic weapons, especially in view of today’s armed conflict where “the time-lag from detection to engagement means that targets may slip away, eluding military action.”260 In this sense, it has been noted that AWS will be more precise.

However, it should be noted that “precision is not a synonym of accuracy. Accuracy in the military context refers to the ability of a weapon to strike a specific location at which it is aimed, while precision involves the ability of target and identification, the timely and accurate strike of said targets, and the determination of whether the desired effects have been accomplished or whether another strike is

260 Herbach, supra note 235, at 5; See also Brendan Gogarty & Meredith Hagger, The Laws of Man Over VehiclesUnmanned: The Legal Response to Robotic Revolution on Sea, Land, and Air, 19 LAW, INFO. & SCI. (2008).
necessary”. To this end, precision is then understood to mean the operational strategies chosen by a belligerent when engaging the enemy, which is meant to minimize risk to one’s own forces while at the same time reducing collateral damage.

Schmitt has argued that military technological innovations are capable of enhancing precision and thereby reducing collateral damage. It is in this sense that Article 9 of the 1956 Draft Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of War demands that “in towns and other places with a large civilian population…the attack shall be conducted with the greatest degree of precision.” Schmitt even suggests that where a belligerent is in possession of weapons that allow precision in attack, it is obligatory to use such weapons. Thus where AWS are deemed to be more precise, failure to use them in order to minimize harm to civilians “would be in contravention of legal obligations under IHL.”

There is no doubt that weapon systems may be more accurate in targeting. However, before one goes on to emphasize the accuracy and efficiency of AWS, such accuracy only matters if and only if they are able to correctly identify their targets in the first place. That is what precision is all about. In this sense, accuracy would mean nothing if the weapon systems are targeting wrong people or illegitimate targets.

---

261 Herbach, supra note 235, at 11-12.
262 Herbach, supra note 235, at 12.
263 Schmitt, supra note 201, at 446.
265 Gill & Fleck, supra 83, at 261.
266 Herbach, supra note 235, at 14.
As I have already indicated, on account of the uncertainties that are met on the battlefield, human judgment is needed for these weapons to comply with the rules of International Humanitarian Law such as distinction and precaution. It is for this reason that Herbach has categorically stated that AWS, as they are currently defined, will not be able to comply with these important rules. Thus, while they may be accurate in most circumstances, AWS may not be precise as understood in International Humanitarian Law.

F. IHL Military Necessity Rule and AWS

The military necessity rule demands that belligerents only use force that is necessary to accomplish a specific and reasonable military objective. If Autonomous Weapon Systems are to operate within the confines of this rule, they must be programmed to understand what is meant by military necessity, to recognize it on the battlefield, and only do that which achieves the military advantage. This rule is related to the rules of proportionality, distinction and humanity.

For Autonomous Weapon Systems to comply with the military necessity rule, the force used will only be deemed to be necessary if it is proportional, targeted on a military objective, and in line with the dictates of humanity. Put differently, “there can be no appeal to military necessity outside [the other] rules.” If there is no

---

267 Herbach, supra note 235, at 17-19.
268 Geneva, supra note 236 (citing art. 51(5)(b)); See also Rome Statute, art. 8, para. 2(b)(iv), Int’l Crim. Ct., July 17, 1998.
269 Geneva, supra note 236 (citing art. 1(2)).
270 F. Thompson, The Principle of Proportionality in the Law of Armed
one at the controls, chances of AWS inflicting harm that is militarily unnecessary is high.

\[\text{G. IHL Rule of Humanity and AWS}\]

Humanity should be understood to refer to the humaneness of humankind,\(^{271}\) where humans motivated by sentiments of goodwill like kindness, mercy, pity and gentleness accord fellow humans treatment that is befitting to a human being in terms of human rights.\(^{272}\)

According to some scholars, the rule of humanity

---


and other basic principles of international humanitarian law have acquired the force of *jus cogens*. In many ways, the rule of humanity is the core and basis of International Humanitarian Law. Rules like distinction, proportionality and military necessity discussed above flow from the rule of humanity. These other rules are said to be geared towards preserving a sense of humanity and actualizing it in armed conflict. Without the rule of humanity, chances of belligerences wanting to view and treat the enemy as non-human are high. The rule of humanity is there to maintain and remind fighters that even in the existence of a war, everyone is still human and worthy of respect and human dignity.

The rule of humanity has been largely responsible for the codification of most of the international

---


humanitarian laws. For example, the Geneva Conventions are said to have come into being after the horrors and suffering of soldiers on land at the battle of Solferino, the tragic events at sea at the battle of Tsushima, and the suffering of prisoners of war in World Wars I and II. Today there are various treaties and legal documents in International Humanitarian Law that contain the rule of humanity.

Furthermore, the International Humanitarian Law rule of humanity is important because it has influenced The Hague law on the governance of weapons. Since time immemorial, determination of whether a weapon is acceptable or not has been influenced by the rule of humanity. Thus, even before its inclusion in the Hague Law, the principle of humanity demanded that belligerents must not use means and methods of warfare that cause the

279 See for example, Article 76 of the Lieber Code (1863); Article 3 Common to the Geneva Conventions; Article 12 of Geneva Convention I; Article 12 of Geneva Convention II; Article 13 of Geneva Convention III; Article 27 of Geneva Convention IV; Article 75 (1) of Additional Protocol I; Article 4(1) of Additional Protocol II; *See also* the 1868 Saint Petersburg Declaration; the First Hague Peace Conference in 1899.
281 Coupland, *supra* note 275, at 971.

The proscription against use of indiscriminate weapons is also motivated by the rule of humanity,\footnote{GEORGE BOGASKI, \textit{AMERICAN PROTESTANTS AND THE DEBATE OVER THE VIETNAM WAR: EVIL WAS LOOSE IN THE WORLD 12 (2014) (See for example Convention on Certain Conventional Weapons in 1980).} \footnote{Geneva, \textit{supra} note 236 (citing art. 3).} \footnote{See Rome Statute, \textit{supra} note 37 at art. 7.} \footnote{WALTER KALIN, \textit{REPORT OF THE UNITED NATIONS SPECIAL RAPPORTEUR ON THE SITUATION OF HUMAN RIGHTS IN KUWAIT UNDER IRAQ OCCUPATION} (1992) (noting paragraph 36).} \footnote{Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1987 I.C.J. (June 27); \textit{See also} Corfu Channel (U.K. v. Albania), Judgement 1949 I.C.J. (Dec. 15); ICRC, \textit{supra} note 52 (citing rules 17).} where various acts such as “violence to life and person, in particular, murder of all kinds, mutilation, cruel treatment and torture; taking of hostages; outrages upon personal dignity, in particular, humiliating and degrading treatment” are proscribed.\footnote{Geneva, \textit{supra} note 236 (citing art. 3).} Any inhumane act, method or means of warfare that is inhumane is prohibited, be it in IAC or NIAC.\footnote{See Rome Statute, \textit{supra} note 37 at art. 7.} Therefore, humanity is the core in governing the means and methods of warfare.\footnote{WALTER KALIN, \textit{REPORT OF THE UNITED NATIONS SPECIAL RAPPORTEUR ON THE SITUATION OF HUMAN RIGHTS IN KUWAIT UNDER IRAQ OCCUPATION} (1992) (noting paragraph 36).} Even courts have recognized the importance of the rule of humanity in this regard.\footnote{Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1987 I.C.J. (June 27); \textit{See also} Corfu Channel (U.K. v. Albania), Judgement 1949 I.C.J. (Dec. 15); ICRC, \textit{supra} note 52 (citing rules 17).}

The rule of humanity does not prohibit the development and use of advanced technology. In fact, where technology can comply with the rules of International Humanitarian Law, it is encouraged.\footnote{See Rome Statute, \textit{supra} note 37 at art. 7.} The question is only whether such advanced technology promotes the rules in question. There are three arguments that can be made in relation to AWS and how they relate to the rule of humanity: that giving AWS the power to decide
who to kill is inhumane and an infraction on the dignity of fighters and civilian casualties alike; that the potential impossibility of a chance to surrender when AWS are used is inhumane; and that in general the use of AWS depersonalizes the use of force to the extent that all resulting deaths are meaningless and therefore inhumane. I now consider these three arguments in turn.

1. Giving AWS the Power Over Life and Death is Inhuman and an Infraction on the Dignity of Fighters and Civilians Alike

Dignity is very important in terms of International Humanitarian Law, and acts that impinge on the dignity and worth of the human being are proscribed.\(^{289}\) The right to dignity in armed conflict encompasses the prohibition against inhuman treatment.\(^{290}\) In the case of *Prosecutor v Aleksovski*, the court observed that the prohibitions of Article 3 common to the Geneva Conventions include outrages upon personal dignity as part of inhuman treatment.\(^{291}\)

In terms of Geneva law, acts infringing upon the dignity of both fighters and protected persons are

\(^{289}\)ICRC, Policy on Torture and Cruel, Inhuman or Degrading Treatment Inflicted on Persons Deprived of Their Liberty (2011); *See also* Sandesh Sivakumaran, *The Law of Non-International Armed Conflict*, OXFORD UNIV. PRESS 263 (2012).
\(^{291}\)Prosecutor v Aleksovski, Case No. IT-95-14/1-T, ¶ 49, 51, 54 (Int’l Crim. Trib. For the Former Yugoslavia June 25, 1999).
prohibited.\textsuperscript{292} To this end, courts have emphasized that acts that infringe human dignity are deplorable in terms of the laws of war.\textsuperscript{293} Likewise, Rule 90 of the ICRC Customary Law Study states that outrageous “acts upon personal dignity in particular humiliating and degrading treatment” are prohibited as a matter of customary international law.\textsuperscript{294} Courts have also found that not only is the violation of the right to dignity a grave breach of the Geneva Conventions; it is prohibited by both conventional treaties and customary international law.\textsuperscript{295}

The above acts are punishable by the founding statutes of international courts and tribunals.\textsuperscript{296} Elements of war crimes that are “outrages upon personal dignity” include those acts that humiliate and degrade the worth of a human being.\textsuperscript{297} Degrading treatment in this regard is

\textsuperscript{292} Geneva Convention Relative to the Treatment of Prisoners of War, ICRC, Aug. 12, 1949, art. 3.
\textsuperscript{293} Aleksovski, IT-95-14/1-T, at ¶ 49, 51, 54; \textit{See also} A. CLAPHAM, THE OXFORD HANDBOOK OF INTERNATIONAL LAW IN ARMED CONFLICT 399 (2014).
\textsuperscript{294} ICRC, \textit{supra} note 52 (citing rules 90). \textit{See} Rule 90 of ICRC Customary law Study; \textit{See also} HOWARD HENSEL, THE LAW OF ARMED CONFLICT: CONSTRAINTS ON THE CONTEMPORARY USE OF MILITARY FORCE 172 (2007).
\textsuperscript{296} INT’L CRIM. CT. STAT., art. 8(2)(c)(i); INT’L CRIM. TRIB. FOR RWANDA STAT., art. 4(a) & (e); SPECIAL CT. FOR SIERRA LEONE, art. 3(a) & (e).
\textsuperscript{297} Prosecutor v Aleksovski, Case No. IT-95-14/1-T, ¶ 54 (Int’l Crim. Trib. For the Former Yugoslavia June 25, 1999); \textit{See also} Prosecutor v Aleksovski, Case No. IT-95-14/1-A, ¶ 26 (Int’l Crim. Trib. For the Former Yugoslavia 2000).
prohibited even against a dead person.\textsuperscript{298}

The only way by which the life of a combatant can be taken in a dignified way is where the decision to take his or her life is made by human beings who appreciate the significance of taking someone’s life. For it to be a dignified death, death must be meaningful.\textsuperscript{299} Death can only be meaningful when it comes at the instance of a human being who appreciates the gravity of the matter, not a machine.\textsuperscript{300} By the same token, in as much as collateral damage is allowed in armed conflict, it is only dignified if the calculations of whether it is proportional are taken by a human being.\textsuperscript{301} For a robot, emotionless and without a moral sense of what it is about to do, making the fundamental decision of ending a human life is inhuman to the core.\textsuperscript{302}

Giving machines the power over life and death “risks taking humanity out of the loop.”\textsuperscript{303} Humanity, even in times of war, demands that human life should be respected with utmost sanctity, and allowing it to be taken away by a machine that does not have the qualitative human deliberation may be “inherently arbitrary and all

\begin{thebibliography}{99}
\bibitem{298} Yoram Dinstein, Non-International Armed Conflicts in International Law 180 (2014).
\bibitem{299} Asaro, \textit{supra} note 280, at 14.
\bibitem{300} Asaro, \textit{supra} note 280, at 14.
\bibitem{303} Heyns, \textit{supra} note 7, at 16.
\end{thebibliography}
resulting deaths [constituting] arbitrary deprivations of life.”

It does not matter that the person being killed is a legitimate target because even those who are condemned to death through the death penalty are entitled to a dignified death when it comes to the means by which they are killed.

In the same light of the humanity argument, Robert Sparrow espouses that allowing AWS “the power to kill seems a bit too much like setting a mousetrap for human beings; to do so would be to treat our enemies like vermin.”

This would be contrary to the important principle of humanity. The vivid mouse-analogy is fully expressed by Aaron Johnson who cites the fundamental right to dignity in objecting the idea of delegating the decision to kill to AWS.

A mouse can be caught in a mouse-trap, but a human must be treated with more dignity. A mouse-trap kills targets with certain characteristics based on certain behaviour, i.e. anything of sufficient mass eating or, at least, touching the bait. The trigger is designed to attack based on the mouse-trap’s perception of the target and its actions. The complexity of the trigger is not what we are concerned with – a mouse can be killed by a machine, as it has no inherent dignity. A robot is in a way like a high tech mouse-trap, it is not a soldier with concerns about human dignity or military honour. Therefore, a human should not be killed by a

304 Id. at 90.
machine as it would be a violation of our inherent dignity.\textsuperscript{307}

In furthering the dignity argument, Jay Strawser states that “the user [of autonomous weapon systems] fails to express his own dignity likely because he fails to respect the victims’ dignity”\textsuperscript{308} and “that in turning these decisions over to machines, human persons fail to satisfy reflexive duties to respect their own rationality, autonomy or dignity, they fail to take responsibility for their own actions.”\textsuperscript{309}

Heyns echoes the same sentiments as he states that giving robots the power to decide who to kill paints an image of “AWS as some kind of mechanized pesticide.”\textsuperscript{310} Notwithstanding whether robots can do better than humans, Heyns argues that the overriding consideration may be whether it is acceptable to let machines decide whom to kill.\textsuperscript{311} In other words, the principle of humanity is an overriding consideration in armed conflict. If an act or weapon is unacceptable in the face of humanity considerations, then “no other consideration can justify deployment of AWS no matter the level of technical competence at which they operate.”\textsuperscript{312}

In view of the above arguments, it is my considered opinion and argument that allowing AWS to decide who to kill and take life without “Meaningful Human Control” constitutes what has been referred to in case law as “a serious attack on human dignity,” as provided for in Article

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{307} Johnson, \textit{supra} note 306, at 134.
\item \textsuperscript{308} JEFF STRAWER, \textit{KILLING BY REMOTE CONTROL: THE ETHICS OF UNMANNED MILITARY} 239 (2013).
\item \textsuperscript{309} \textit{Id.} at 237.
\item \textsuperscript{310} Heyns, \textit{supra} note 7, at 18, para 95.
\item \textsuperscript{311} \textit{Id.} at 17, para 92.
\item \textsuperscript{312} \textit{Id.} at 17, para 93..
\end{itemize}
\end{footnotesize}
H. It Is Inhumane to Use Weapons That Make it Impossible to Surrender

War is in no way a relationship of man with a man but a relationship between States, in which individuals are enemies only by accident; not as men, nor even as citizens, but as soldiers (...). Since the object of war is to destroy the enemy State, it is legitimate to kill the latter’s defenders as long as they are carrying arms; but as soon as they lay them down and surrender, they cease to be enemies or agents of the enemy, and again become mere men, and it is no longer legitimate to take their lives.

The history of surrendering and its implications have been changed and greatly shaped by the rule of humanity. Significant changes are evident from the 18th century, where surrendering soldiers could be forced to fight on the side of the enemy, where surrendering no matter the conditions was a punishable offense by the sending state, and where those “who surrendered still stood a good chance of being killed,” to the 19th century where international agreements started to emerge demanding that those who surrender must not only be spared, but “fed with plain and wholesome food whenever practicable and

treated with a sense of humanity.”

Human nature is in general influenced and infused with “an absolute and natural necessity” to save one’s own life. It is that natural necessity that influences a fighter’s choice to flee or to surrender. In armed conflict, “fighting as well as flight or surrender aim at the same end; namely to the preservation of one’s life.” Thus, where a fighter surrenders or is no longer capable of fighting because of wounds or sickness, it is only humane to spare his or her life.

Now that AWS are not humans with the ability to see or discern that a fighter is about to surrender or is wounded, sick or fatigued to the extent that surrendering is inevitable, it may be argued that AWS violate the rule of humanity. If AWS make it impossible for one to surrender or at least be cared for when wounded or sick, they will defy the rule of humanity.

The law is clear that “under no circumstances should a belligerent follow an approach in terms of which an offer to surrender will not be accepted. A belligerent may not give orders of “no quarter”

317 Id.
318 Schmitt, supra note 173, at 258 (referencing an example in the case of drones is that of Mehsud who, at the time he was targeted was severely sick. He was killed by a drone missile at the time he was receiving an intravenous transfusion. It cannot be ruled out that because of his sickness he might have surrendered, or at least put hors de combat by virtue of sickness).
or “no survivor” since such orders constitute war crimes because they would be inconsistent with the principle of humanity. AWS whose mission is to kill once it is deployed, and will not stop until targets coded into its program are dead, is the equivalent of a no quarter order which is inconsistent with the principle of humanity. Creating AWS that once activated requires no further human intervention is a failure to recognize that on the battlefield, the status of a target can change in a split second from a legitimate to an illegitimate target. Constant human supervision is therefore required in this regard if the core of humanity is to be maintained.

Furthermore, humans not only have the capacity to adhere to the minimum set standard, “but they also hold the potential to adhere to higher values” unlike AWS, “which lack the capacity to rise above minimum standards” as persuaded by dictates of humanity. Aspiring to adhere to higher standards or to rise above the minimum is not possible in the case of AWS with full autonomy, which led one commentator to observe that the use of AWS is tantamount to “giving up on hope for a better world.”

I. AWS Depersonalize the Use of Force to a Point of Inhumanity

It can be argued further that AWS, just like other unmanned systems distance the fighters from the point where force is delivered. The distancing of the fighter from where force is being projected has its advantages

321 Heyns, supra note 2, at 17, para 93 (noting A/HRC/23/47).
322 Heyns, supra note 2, at 18, para 97 (noting A/HRC/23/47).
323 Asaro, supra note 181, at 697.
since the combatant or fighter is removed from harm’s way. In terms of the obligations of the state to protect and promote the right to life of its citizens, which includes armed forces, this can be considered to be a legitimate goal.

However, distancing or removing fighters away from the harm they project to others leads to the depersonalization of the use of force. In such cases, combatants or fighters may be removed both physically and psychologically from the consequences of their actions. Arguments have already been made in relation to other unmanned systems such as armed drones, that they create a videogame mentality where drone operators may not take seriously the impact of their actions because they are removed from the point of impact. This depersonalization of the use of force is taken to another level with AWS, where humans are no longer in the loop once the system is activated, which is in the case with fully autonomous systems where there is no “Meaningful Human Control”.

This distancing of humans from the decision to kill or use force, and its impact, may in the long run prove to be undesirable since the consequences and gravity of killing may become a distant factor for the state or fighter.

324 Heyns, supra note 2, at 17, para 93 (noting A/HRC/23/47).
325 DINA H SHELTON & PAOLO CAROZZA, REGIONAL PROTECTION OF HUMAN RIGHTS 742 (2013).
326 Asaro, supra note 181, at 697.
deploying these kinds of technologies.\textsuperscript{329} For these foregoing reasons, I argue that AWS without “Meaningful Human Control” may be inconsistent with the customary IHL rule of humanity.

\textit{J. Conclusion}

International Humanitarian Law rules of humanity, distinction, precaution, proportionality and military necessity are at the core of this body of law. These rules form the backbone of the law on the safeguarding of all protected persons during armed conflict. It is important that all means and methods of warfare that states seek to adopt or introduce be consistent with these rules that have customary law status.

The rule of humanity compliments all the other rules – whatever parties to a conflict choose to do, it must be in line with the demands of humanity. I have argued and come to the conclusion that in as much as soldiers have the right to kill each other, giving or delegating the decision to kill to machines is not in line with the demands of humanity, as it violates the right to dignity of those targeted.

Most of the contemporary armed conflicts occur in civilian populated areas. Further, there has been the civilianization of armed conflicts to the extent that it is difficult to distinguish those who are directly taking part in hostilities and those who are not. As a result, and more than before, human judgment and deliberation are critical when selecting targets in these unstructured environments.

AWS may not be able to comply with the

\textsuperscript{329} Asaro, \textit{supra} note 280, at 14.
customary rule of distinction due to a number of reasons: the nature of contemporary armed conflicts as already highlighted, the definitional deficiency in International Humanitarian Law that will make it impossible to translate the definitions and code them into the system of the robot, and the technological limitations currently faced.

The same arguments are applicable to other rules such as proportionality, precaution and military necessity, which all require human judgment. For this reason, AWS that do not have “Meaningful Human Control” must not be allowed for their inconsistency with the IHL rules of humanity, precaution, distinction, proportionality and military necessity.
Cybersecurity remains perhaps the greatest challenge to the economic and physical well being of governments, individuals, and businesses worldwide. During recent
months the United States has witnessed many disruptive and expensive cyber breaches. No single U.S. governmental agency or congressional committee maintains primary responsibility for the numerous issues related to cybersecurity. Good oversight stands at the core of good government. Oversight is Congress’s way of making sure that the administration is carrying out federal law in the way Congress intended. So many aspects of cybersecurity have the potential for use by: terrorists; by foreign entities as a tool to conduct industrial espionage against U.S. business; and by nation state adversaries, or others intent upon creating serious disruption. These various threats mean that cybersecurity policy in many ways must be treated just like the strategic and operational plans of a country at war.

The purpose of this article is to provide a road map of the various congressional committees exercising jurisdiction over matters relating to cybersecurity. First, a few thoughts are offered about the role of Congressional oversight. Second, for perspective, a brief outline of how the executive branch, in the absence of legislation between 2002 and December 2014, handled responsibility for all things cyber. Next, a discussion of Congressional cybersecurity oversight for the 114th Congress is provided, including an analysis of committee jurisdiction, leadership, membership, and key staff. Finally, the important role contributed by professional congressional staff, the Government Accountability Office, Congressional Budget Office, and the Library of Congress Congressional Research Service (CRS) is covered. My hope is that this article will add to the important discussion and foster greater understanding about Congressional oversight of cybersecurity.
We face a growing array of cyber threats from foreign intelligence services, terrorists, criminal groups, and hacktivists, who are increasing their capacity to steal, manipulate, or destroy information and networks in a manner that risks compromising our personal and national security. They do so via a manmade environment that is constantly evolving and through the use of techniques and capabilities that are continually changing.\(^1\)

Adm. Michael S. Rogers, USN  
*Director, National Security Agency*  
*Chief, Central Security Services*  
*Commander, U.S. Cyber Command*

\(^1\) Hearing to Consider the Nomination of Vice Admiral Michael S. Rogers, USN to be Admiral and Director, National Security Agency/Chief, Central Security Services/Commander, U.S. Cyber Command: Hearing Before the U.S. Senate, Committee on Armed Services of the, 113\(^{th}\) Cong. (2014) (Statement of Adm. Michael S. Rogers, USN).
I. Overview

To paraphrase a statement attributed to Otto von Bismarck, “nobody should ever watch the making of either sausages or laws.”

Cybersecurity remains perhaps the greatest challenge to the economic and physical well being of governments, individuals, and business worldwide. During recent months the United States has witnessed many cyber breaches of such entities as Target, Home Depot, the U.S. Postal Service, and Sony Pictures Entertainment. Of particular concern, data breaches


6 Id. at __, citing Center for Strategic & Int’l Studies, Significant
during 2015 of sensitive information at the U.S. Office of Personnel Management resulted in a serious threat to national security, since “the Social Security Numbers (SSNs) of 21.5 million individuals were stolen from the background information databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants... [and] findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints[,] [u]sernames and passwords[.]”

The terms cybersecurity and cyberattack have become broadly used without widespread acceptance as to their exact meaning. Professor David Thaw has observed that, “the terms are too-often used broadly to include all of electronic crimes,”

---


military action,\textsuperscript{9} domestic guard/homeland security activities,\textsuperscript{10} corporate risk management,\textsuperscript{11} financial security,\textsuperscript{12} and a wide spectrum of other activities related to

\textsuperscript{9} See Thaw, \textit{supra} note 8 at 287, 288, \textit{citing Hearing Before the S. Comm. on Armed Servs., 113\textsuperscript{th} Cong. (Mar. 12, 2013) (Statement of Gen. Keith B. Alexander, Commander, U.S. Cyber Command).}


\textsuperscript{12} See Thaw, \textit{supra} note 8 at 287, 288, \textit{citing} Antone Gonsalves,
computers, the Internet, privacy, and other similar topics.”\textsuperscript{13} No single U.S. governmental agency or congressional committee maintains primary responsibility for the numerous issues related to cybersecurity. It is observed that “good oversight stands at the core of good government. It is Congress’s way of making sure that the administration is carrying out federal law in the way Congress intended.”\textsuperscript{14}

The purpose of this article is to provide a road map of the various congressional committees exercising jurisdiction over matters relating to cybersecurity. First, a few thoughts are offered about the role of Congressional oversight. Second, for perspective, a brief outline of how the executive branch, in the absence of legislation between 2002 and December 2014,\textsuperscript{15} handled responsibility for all


\textsuperscript{14} \textsc{Lee H. Hamilton}, \textsc{How Congress Works and Why You Should Care}, 106 (Indiana University Press 2004).

\textsuperscript{15} See generally Mitchell S. Kominsky, \textit{The Current Landscape of
things cyber. Next, a discussion of Congressional cybersecurity oversight for the 114th Congress is provided, including an analysis of committee jurisdiction, leadership, membership, and key staff. Finally, the important role contributed by professional congressional staff, the Government Accountability Office, Congressional Budget Office, and the Library of Congress Congressional Research Service (CRS) is covered. My attempt to include an up-to-date guide to relevant congressional staff will inevitably fail. No doubt, many staffers will have moved on either before or shortly after this article is published. However, it is my hope that these pages will add to the important discussion and foster greater understanding about the Congressional oversight of cybersecurity.

II. Role of Congressional Oversight

The concept of Congressional oversight is firmly rooted as fundamental to the American system of governmental checks and balances among the three branches of government.16 Walter Oleszek observes that

“the first congressional investigation in American history, in 1792, delved into the conduct of the government in the wars against the Indians.”


Professors Cochran, Mayer, Carr and Cayer observe that

Government, first, exists to provide security from internal and external threats to the lives, liberties, and properties of its members. National defense and foreign policy are examples of this purpose. Another is crime policy, which intends to establish order and to protect citizens from each other through crime prevention and the punishment of criminals.\footnote{18}

It is often observed that “committees are where the \textit{real} work” of Congress is achieved.\footnote{19} Lee H. Hamilton, U.S. Representative from 1965 to 1999, observes that “good oversight helps Congress evaluate how programs are administered and how they perform—ferreting out waste and fraud, determining whether programs have out lived their usefulness, compelling the administration to explain or justify its policies.”\footnote{20}

While congressional oversight activity can take any of several forms,\footnote{21} “formal committee and subcommittee

---


\footnote{19}{See generally Tom Daschle & Charles Robbins, \textit{The U.S. Senate} 72 (2013); Brian D. Feinstein, Congressional Government Rebooted: Randomized Committee Assignments & Legislative Capacity, 7 Harv. Law & Pol’y Rev. 601 (2013), available at \url{http://ssrn.com/abstract=2068734}.}

\footnote{20}{Hamilton, supra note 14 at 107.}

\footnote{21}{See Feinstein supra note 16 at 6, \textit{citing Joel D. Aberbach, Keeping a Watchful Eye: The Politics of Congressional Oversight} 132 (1990) (considering the informal communication between}
oversight hearings are the most firmly rooted form of oversight.”


22 See Feinstein supra note 16 at 7, citing Cong. Research Serv., Congressional Investigations, CRS Annotated Constitution 90, available at http://www.law.cornell.edu/anncon/html/art1frag9_user.html (“The Court has long since accorded its agreement with Congress that the investigatory power is so essential to the legislative function as to be implied from the general vesting of legislative power in Congress.”); see also Jack M. Beerman, Congressional Administration, 43 SAN DIEGO L. REV. 61, 64-64 (2006) (observing that “Congress is deeply involved in the day to day administration of the law” as “insufficiently noted in legal scholarship”); Beerman, id. at 122 (explaining how the Legislative Reorganization Act of 1946 rearranged committee jurisdictions and formed professional oversight staffs for certain committees, thereby establishing long-lasting oversight institutions). But see Mark Seidenfeld, The Psychology of Accountability and
“Congress began holding oversight hearings as early as 1791[,]\(^\text{23}\) according to Arthur Schlesinger, Jr., the Constitution does not explicitly refer to Congress’s oversight authority for the simple reason that such authority was considered implicit in the body’s general legislative powers; in other words, oversight was considered a given.”\(^\text{24}\) By virtue of the oversight process, “Congress has played a crucial role in checking the abuse of executive powers… in the Teapot Dome scandal of 1923… in the cases of Watergate and Iran-Contra… members of Congress have unearthed many policy failures, saved taxpayers billions of dollars, and identified corrupt or illegal behavior.”\(^\text{25}\) Hamilton observes, “Passing legislation and providing oversight are two key functions of Congress, but almost all the attention goes to legislating. I agree with Woodrow Wilson who said ‘Quite as important as lawmaking is vigilant oversight of administration.’”\(^\text{26}\)

Almost “all legislation is referred to a committee, and

\(^{23}\) See Feinstein surra note 16 at 7 citing M. Nelson McGeary, *Congressional Investigations: Historical Development*, 18 U. Chi. L. REV. 425 (1951) (observing that the House of Representatives in 1791 convened a special committee to investigate the U.S. Army’s defeat by Native American forces in the Battle of the Wabash).

\(^{24}\) See Feinstein supra note 16 at 7 citing Arthur M. Schlesinger, Jr., *Introduction*, In CONGRESS INVESTIGATES: A DOCUMENTED HISTORY, 1792-1974, VOL. 1, xix (Arthur M. Schlesinger, Jr. & Roger Bruns eds., 1975) (“[I]t was not considered necessary to make an explicit grant of such authority. The power to make laws implied the power to see whether they were faithfully executed.”).

\(^{25}\) Hamilton, supra note 14 at 106.

\(^{26}\) Id. citing WOODROW WILSON, CONGRESSIONAL GOVERNMENT, 195 (1885).
sometimes to more than one. ‘Writing legislation on the floor’—sending matters directly for full Senate debate—doesn’t allow committee experts to shape the bill first, and is discouraged.’”27 With the 1946 Legislative Reorganization Act, oversight responsibility was formally recognized by Congress in requiring “that the House and Senate standing committees exercise ‘continuous watchfulness of the execution by the administrative agencies’ of any law under their jurisdiction.”28

Many cybersecurity issues are often the same or similar to those falling under the jurisdiction of the Department of Homeland Security (DHS). During an interview conducted by National Public Radio, DHS Deputy Secretary Jane Holl Lute disclosed that 108 committees and subcommittees exercised jurisdiction over DHS during the 110th Congress.29 Professors Clinton, Lewis, and Selin find that “an increase in the number of committees also undercuts the ability of Congress to respond collectively to the actions of the presidency or the bureaucracy.”30 These survey results further indicate that “when more committees are involved in monitoring and

27 See DASCHLE & ROBBINS, supra note 19 at 72.
potentially directing agency policymaking, Congress is less influential than the president for determining agency policy. Increasing the number of involved committees may maximize the electoral benefits for members and provide a platform for making public proclamations on issues of importance…”31 Although somewhat dated, Congressional Quarterly lists the following ways in which the oversight functions are exercised by Congress:

1. Hearings and investigations…
2. [Omitted, due to change in law]…
3. Authorizations…
4. Nonstatutory controls, such as informal contacts between executive officials and committee members and staff, and statements incorporated in committee reports and conference reports, hearings and floor debates…
5. [Government Accountability Office] GAO audits of agencies and programs;
6. Requirements that executive agencies submit to Congress periodic reports on program implementation;
7. Informal groups within Congress and organizations outside Congress that inform members about specific problems in administering programs;
8. The Senate confirmation process…
9. Program evaluation through the use of social science and management methodology, such as surveys, cost-benefit analysis and efficiency studies;

31 Id. at 2.
10. Casework…; and

11. Studies by congressional support agencies, including the Congressional Research Service, the Office of Technology Assessment and the Congressional Budget Office.32

A. INHERENT TENSION SURROUNDING NATIONAL SECURITY MATTERS

Sensitive information, which has national security significance, must be safeguarded to ensure the vital national security interests of any nation state. So many aspects of cybersecurity have the potential for use by: terrorists; foreign entities as a tool to conduct industrial espionage against U.S. business; and nation state adversaries, or others intent upon creating serious disruptions. These various threats mean that cybersecurity policy in many ways must be treated just like the strategic and operational plans of a country at war.33


Xerox (just to name a few). In the author’s opinion, Admiral Inman is perhaps the most experienced and thoughtful senior executive in the U.S. intelligence community. During congressional testimony, Admiral Inman counseled

For the public support, [oversight] will be critical for funding and sustaining a significant level of intelligence activities by the country in the years ahead. There has to be oversight. The media would like to do it. It’s not feasible with the issues of protection of sources and methods, so there must be mechanisms in both the Congress and the executive branch which work. Optimally, I would prefer a joint committee for oversight in the Congress. There may be other reasons that that’s simply not achievable, not practical… The oversight activities must be bipartisan in their daily conduct for them to be fully effective… I don’t have great confidence in an Inspectors General process for focusing on the broad issues. They’re good for trying to ferret out corruption, criminal activity, but the President, any President needs wise advice that constantly is assessing, are the country’s needs being met where they don’t have the requirement for institutional loyalty.34

During his Senate confirmation hearings to become Deputy Director of Central Intelligence, Robert M. Gates

34 Hearing of the Commission on the Roles and Capabilities of the United States Intelligence Community, 104th Cong. (1996) (statement of Admiral Bob Inman, USN (Retired), former Director of the National Security Agency and Deputy Director of Central Intelligence).
said, “Intelligence is a force multiplier for military operations. It more than pays for itself. There’s no sense in building new weapons if you can’t detect and assess enemy threats, or even identify targets during crisis.”

Gates believes that congressional oversight of the U.S. intelligence community and activities is “a key element in preserving intelligence programs, and in maintaining public understanding and support for intelligence.” Indeed, “the gravest danger facing intelligence is that intelligence studies, or even intelligence operations, may become influenced by policy or even political influences. Every effort must be made to see that intelligence reports and analyses are not made into props for policymakers. Intelligence has to be completely objective.”

Oversight has created an environment that fosters adherence to the rules at all levels and discourages corner cutting or abuses. The committees have contributed to improving the quality of our work and to efficiency. And, finally, the congressional committees and executive oversight organizations such as the Intelligence Oversight Board and the President’s Foreign Intelligence Advisory Board should give Americans confidence that their intelligence service is accountable, carries out its activities according to the law and that we are guided by standards and values acceptable to them.

35 Nomination of Robert M. Gates to be Deputy Director of Central Intelligence: Hearing Before the Select Committee on Intelligence of the U.S. Senate, 99th Cong. (1986) (Statement of Robert M. Gates).
36 Id.
37 Id.
The relationship between the congressional oversight committees and the intelligence community is unique in the world – the first attempt ever to conduct secret intelligence operations accountable to the people and responsible to the law and to the Congress. While the oversight process may occasionally lead to frictions in the gray area resulting from the overlap between congressional authorities and the duties of the executive, it has now been the practice of both branches of Government for 10 years now to try to resolve such difficulties in a spirit of comity and mutual understanding. This unique relationship between us depends on mutual trust, candor, and respect and I assure you I intend to conduct myself with this in mind…

Because intelligence is secret and our Agency is closed to public scrutiny, I believe we must take the initiative to reach out to policy-makers, the Congress, the private sector, and critics and experts of all stripes for help in improving the substance of our work, our efficiency and our effectiveness… Intelligence must be relevant, timely, and responsive to the real requirements of the policymaker if it is to be useful and effective. And relevance can be insured only by a close, day to day, working relationship. At the same time, intelligence must remain independent. Our very existence depends upon a reputation for integrity and for objectivity.38

38 Id. at 40.
Admiral Michael S. Rogers was questioned at length by Senators McCain, Reed, Inhofe, Wicker, Ayotte, Lee, Manchin, Blumenthal, Donnelly, Kaine and King during his confirmation hearing to become: Director of the National Security Agency; Chief, Central Security Services; and Commander, U.S. Cyber Command. When asked by Senator Tim Kayne to speak about the “unique challenges in defining ‘war’ in cyberspace, what war is, what hostilities are, what military action is,” Admiral Rogers responded

Whatever we do within the cyber arena, international law will pertain; that if we find ourselves getting to a point where we believe that cyber is taking us down an armed conflict scenario, that the rules and the law of armed conflict will pertain every bit as much in this domain as it does in any other. I don’t think cyber is inherently different in that regard. I think those sets of procedures, those sets of policies and law, as a Nation have stood us in good stead. I think they represent a good point of departure for us.

Senator KAINÉ: … Would it be your view then that pure cyber war – somebody wipes out our grid and then we think about taking activity to respond – is that not war? It could have a huge effect on human life. It could have huge effect on the economies of the two nations. Is that not war unless it then leads to armed conflict?

Admiral ROGERS: … I believe that an offensive, destructive act that has significant impact for us, I believe now we’re starting to get on the boundaries of is that an act of war. Now, everything varies on a case by case basis and I’m
always concerned about broad general statements.\(^{39}\)

Professor Frederick R. Chang, former National Security Agency (“NSA”) Director of Research said in congressional testimony that, “we are paying a heavy price for our technological dependence and the problem is worsening with the passage of time. Our trust in cyberspace has been taken from us by hackers, cybercriminals and sophisticated cyber attackers who intend to do us harm.”\(^{40}\) Towards the end of 2010 Senator John McCain observed

CYBERCOM was established… by the Secretary of Defense… Since then I have shared the concerns… about ensuring that the role, mission, legal authorities, and rules of engagement that CYBERCOM will employ are well thought out and understood… The Department must have a centralized command to address the challenges of


cyber warfare, to provide the support to the regional combatant commands, and to ensure that DOD, while focused on its own military networks and information grid, also is ready, if directed by the President, to assume a position of leadership and support to civilian authorities in this regard.

Continuing intrusions and attacks by difficult to identify and locate actors on our civilian and military networks and web sites demand not only a robust defensive capability, but the ability to respond offensively when the circumstances call for it. One need only consider the examples of cyber warfare conducted against the Republic of Georgia in 2008 and Estonia in 2007 to appreciate the nature of this form of modern warfare.41

Thoughtful observers remain mindful that “the issue of congressional oversight of intelligence is complex, combining as it does the political and structural complexities of Congress with the difficulty of monitoring something of strategic significance that, by definition, operates in the shadows.”42 Professor Jennifer Kibbe stated


that “intelligence is more crucial than ever to national security, but as the executive branch and the intelligence community try to maximize the utility of intelligence in meeting national security needs, it is imperative that the congressional overseers meet their obligations as well.”

Professor Kibbe offers the following three reasons that congressional oversight of intelligence-related issues is particularly important:

1. The first, most obvious reason is the inherent secrecy of the subject…
2. [Because] ‘the intelligence community is constrained in its ability to convince the American public that it can be trusted and deserves their support,’ Congress also plays an important role in explaining and representing the intelligence community to the public; and
3. A third-reason legislative over-sight is so important is that, done well, it helps to improve the intelligence product, whether that means collection, analysis or covert action. When administration and intelligence officials know that they will have to explain a funding choice or particular operation to Congress, it has the effect of adding a layer to their own internal vetting.

See Kibbe, supra note 42 at 25.

III. The Executive Branch and Cybersecurity

The American constitutional concept of separation of powers “is based on the notion that governmental power must be divided among counterimposed institutions in order to prevent the accumulation of power in any single part of government.”

Many scholars have written about presidential powers and congressional limits to the powers of the executive branch. Manheim and Ides also point to


the wisdom of power sharing via a system of checks and balances, wherein “the greatest security against tyranny… lies not in a hermetic division among the Branches, but in a carefully crafted system of checked and balanced power within each Branch.”

A. EXECUTIVE ORDER 13636

In the more than decade absence of cybersecurity legislation, President Obama issued on February 12, 2013, Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” directing the Executive Branch to:

1. Develop a technology-neutral voluntary cybersecurity framework;
2. Promote and incentivize the adoption of cybersecurity practices;
3. Increase the volume, timeliness and quality of cyber threat information sharing;
4. Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure; and
5. Explore the use of existing regulation to promote cyber security.

---


The 2013 Executive Order defines the term “critical infrastructure” to mean “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”49 Next, “Presidential Policy Directive-21: Critical Infrastructure Security and Resilience,” requires that the Executive Branch: “develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time; understand the cascading consequences of infrastructure failures; evaluate and mature the public-private partnership; update the National Infrastructure Protection Plan; and develop comprehensive research and development plan.”50 Executive Order 13636 mandates the “development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk.”51

49 Id. at Sec. 2.
51 See Trautman, Id., citing U.S. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL
Elsewhere, the author observes that “[d]uring December 2014, just hours before the holiday recess, the U.S. Congress passed five major legislative proposals designed to enhance U.S. cybersecurity. Following signature by the President, these became the first cybersecurity laws to be enacted in over a decade, since passage of the Federal Information Security Management Act of 2002.”


Cybersecurity Workforce Assessment Act;\textsuperscript{56} The Homeland Security Workforce Assessment Act;\textsuperscript{57} and the Cybersecurity Enhancement Act of 2014.\textsuperscript{58}

Released several weeks later, the President’s 2015 National Security Strategy states, “we will grow our investment in crucial capabilities like cyber… We will safeguard our science and technology base to keep our edge in the capabilities needed to prevail against any adversary.”\textsuperscript{59} The National Security Strategy observed, “We are working with the owners and operators of our Nation’s critical cyber and physical infrastructure across every sector—financial, energy, transportation, health, information technology, and more—to decrease vulnerabilities and increase resilience.”\textsuperscript{60} Further

Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet. Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution. Drawing on the


\textsuperscript{60} Id. at 9.
voluntary cybersecurity framework, we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure. We will continue to work with the Congress to pursue a legislative framework that ensures high standards. We will defend ourselves, consistent with U.S. and international law, against cyber attacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity. We will assist other countries to develop laws that enable strong action against threats that originate from their infrastructure. Globally, cybersecurity requires that long-standing norms of international behavior—to include protection of intellectual property, online freedom, and respect for civilian infrastructure—be upheld, and the Internet be managed as a shared responsibility between states and the private sector with civil society and Internet users as key stakeholders.\footnote{Id. at 12.}

\textbf{B. 2015 CYBERSECURITY LEGISLATIVE PROPOSAL}

During early 2015, the Administration’s updated legislative proposal is designed to promote “better cybersecurity information sharing between the private sector and the government, and it enhances collaboration and information sharing amongst the private sector.”\footnote{Press Release, The White House, SECURING CYBERSPACE – President Obama Announces New Cybersecurity Legislative Proposal}
cybersecurity proposal specifically encourages the sharing of appropriate private sector cyber threat information with DHS’s “National Cybersecurity and Communications Integration Center (NCCIC), which will then share it in as close to real-time as practicable with relevant federal agencies and with private sector-developed and operated Information Sharing and Analysis Organizations (ISAOs) by providing targeted liability protection for companies that share information with these entities.”63 With a view toward safeguarding the personal privacy information of American citizens, the proposal requires DHS and “the Attorney General, in consultation with the Privacy and Civil Liberties Oversight Board and others, to develop receipt, retention, use, and disclosure guidelines for the federal government.”64 During 2015 numerous Congressional committees proceeded to hold hearings relevant to cybersecurity legislation.65

C. 2015 NATIONAL DATA BREACH REPORTING PROPOSAL

The Administration also updated its security breach reporting consumer reporting proposal, to assist “business and consumers by simplifying and standardizing the existing patchwork of 46 state laws... that contain these requirements into one federal statute, and puts in place a

63 Id.
64 Id.
65 See discussion of hearings by specific committees and subcommittees, infra.
177 CONGRESSIONAL CYBERSECURITY . . . [2016]

single clear and timely notice requirement to ensure that companies notify their employees and customers about security breaches.” As of August 27, 2015, numerous bills were moving through the House or Senate on this subject.67

D. CYBER THREAT INTELLIGENCE INTEGRATION CENTER

On February 25, 2015, President Barack Obama announced creation of the Cyber Threat Intelligence Integration Center (CTIIC), noting that “In creating the

CTIIC, the Administration is applying some of the hard-won lessons from our counterterrorism efforts to augment that ‘whole of government’ approach by providing policymakers with a cross-agency view of foreign cyber threats, their severity, and potential attribution.” The purpose of the new CTIIC will be to provide “intelligence needed to carry out” the cybersecurity missions of agencies such as the: National Cyber Investigative Joint Task Force (NCIJTC) as it coordinates, integrates, and shares domestic cyber threat investigation information; the National Cybersecurity and Communications Integration Center (NCCIC) (network defense and incident response mission); and the U.S. Cyber Command in its stated mission of defending the nation from significant cyberspace attacks.

IV. Congressional Oversight 2015-2016

During the last two years of the Obama presidency, the Republican Party has enjoyed an expanded majority in the U.S. House of Representatives, and a newly claimed majority status during 2015 in the Senate. Widespread consensus holds that the two most recent congresses have been among the least productive, “and in a political climate today that’s far more polarized than that of the Clinton era, expectations for the 114th Congress are not high.”

---


69 Id.

70 John Stanton, Kyle Simpson, Michael Gilliland, James Wickett, Aaron Cutler, Robert Kyle, Michael House, Kate McAuliffe, Lance Bultena, Michele Farquhar, Jack Jacobson, Michael Bell, Trey Hanbury, Jared Bomberg, HOGAN LOVELLS: 114th CONGRESS
Passage of the Budget Control Act during 2011 resulted in severe across-the-board federal agency spending cuts, proving particularly difficult for the Department of Defense. In a publication by Hogan Lovells, the authors observed that “unless Congress and the Administration can agree to eliminate or reform the sequester mechanism, DOD will face deep spending cuts in 2016.” Successful repeal of the sequester is assumed in the President’s FY2016 budget, and it is believed that “Republicans in both the House and Senate are also eager to eliminate sequester cuts for defense and national security programs for FY2016 and beyond.” Despite recent unprecedented congressional gridlock, “two bills nonetheless get passed every year; an appropriations measure to fund the government, and the National Defense Authorization Act (NDAA)… Congress passes legislation authorizing hundreds of billions of dollars in defense spending year after year.”

Unlike many nation states, in the U.S. almost all critical infrastructure and cyber-sensitive assets are held in the private sector. Accordingly, the cybersecurity assets of almost every corporation that Congress seeks to protect through regulation “not only generally possess expertise useful to the rulemaking process, but in fact possess superior knowledge regarding information security threats

---


71 Id. at 46.
72 Id.
73 Id.
74 See generally Trautman, supra, note 50.
and defenses not otherwise available to regulators.”\textsuperscript{75} Therefore, Congress and “Federal regulators leverage this knowledge not only voluntarily, but in some cases by mandate engaging private entities in the rulemaking and \textit{de facto} standards-setting process.”\textsuperscript{76} This process of “management-based regulation” has developed “under which the regulated entities themselves develop and adhere to their own individualized compliance plans. While these plans must meet general guidelines, the regulatory goal becomes the development of and adherence to the plan, rather than compliance with specific technical obligations directly.”\textsuperscript{77} Using the term “management-based regulatory delegation,” Professor David Thaw depicts this contemporary regulatory process as “a deliberate encoding of regulatory capture both in the rulemaking and enforcement stages of the administrative process to engage the superior knowledge possessed by regulated entities.”\textsuperscript{78}

Committees are the mechanism Congress has designed to conduct its business. John Aldrich and David Rohde observe, “Committees, through the division of labor, permit the chamber to stretch its capabilities by having only a subset of members consider each issue [oversight] and piece of legislation in detail.”\textsuperscript{79} Jurisdiction over matters of cybersecurity is claimed by numerous committees. Presented below is a description of the various committees claiming jurisdiction, their leadership, committee

\textsuperscript{75} See Thaw, \textit{supra}, note 8 at 287, 289.
\textsuperscript{76} \textit{Id}.
\textsuperscript{77} \textit{Id.} at 290.
\textsuperscript{78} \textit{Id}.
\textsuperscript{79} John H. Aldrich & David W. Rohde, \textit{Congressional Committees in a Partisan Era}, in \textsc{Lawrence C. Dodd} & \textsc{Bruce I. Oppenheimer}, \textit{Congress Reconsidered} 249 (\textsc{CQ Press, 2005}).
membership, and key staff. Congressional staffs perform many important and necessary functions such as scheduling; communications, media and press relations; administrative support; and chamber floor operations. However, due to the size of many committee and subcommittee staffs, I have attempted to identify those staff members, generally policy and national security specialists, who may be most significantly involved in cyber-related issues.

V. The Senate

The new Republican majority in the U.S. Senate results in a reshuffling of committee chairmen for those committees having jurisdiction over various elements of cybersecurity. The work of the Senate is divided into 20 committees, 68 subcommittees, and 4 joint committees to collectively handle all the issues the Senate covers.80 Most committees are further divided into subcommittees, to focus on particular issue areas, such as the Judiciary Subcommittee on Crime and Terrorism or the Appropriations Subcommittee on Defense.81 Senators are motivated to gain appointment to and serve on committees that provide an opportunity to weigh in on issues of particular interest to themselves or their constituents.82 It is through the work of committees “where senators establish expertise and reputations, and make their imprint on American law and policy. A senator’s committee

81 See Daschle & Robbins, supra note 19 at 72.
82 Id. at 73.
assignments will determine much of his or her career, similar to choosing a major in college. Through committee work, senators dive into particular issues and make these issues their own…”

The following committees in the Senate play a role in cybersecurity oversight: Armed Services; Banking, Housing, and Urban Affairs; Committee on Commerce, Science and Transportation (Subcommittee on Communications, Technology, and the Internet); the Homeland Security and Government Affairs Committee (HSGAC); Senate Select Committee on Intelligence (SSCI); and Senate Judiciary Committee.

VI. Senate Committee On Armed Services

Established on December 10, 1816 as the “Senate Committee on Military Affairs; on the Militia; and Naval Affairs,” the committee merged over time, on several occasions, to become what is now known as the current Committee on Armed Services. The Armed Services Committee describes its jurisdiction as:

1. Aeronautical and space activities peculiar to or primarily associated with the development of weapons systems or military operations;
2. Common defense;
3. Department of Defense, the Department of the Army, the Department of the Navy, and the Department of the Air

---

83 Id.
Force, generally;
4. Maintenance and operation of the Panama Canal, including administration, sanitation, and government of the Canal Zone;
5. Military research and development;
6. National security aspects of nuclear energy;
7. Naval petroleum reserves, except those in Alaska;
8. Pay, promotion, retirement, and other benefits and privileges of members of the Armed Forces, including overseas education of civilian and military dependents;
9. Selective service system; and
10. Strategic and critical materials necessary for the common defense. The Senate has also given the committee the authority to study and review, on a comprehensive basis, matters relating to the common defense policy of the United States, and report thereon from time to time.  

Based on the Committee’s documents, several Armed Services subcommittees appear to have jurisdiction over various aspects of cybersecurity oversight, as more fully discussed below. Membership of the Senate Committee on Armed Services is as follows:  

---

85 Id., citing Standing Rules of the Senate, Rule XXV, 1(c)(1).
86 U.S. Senate Committee on Armed Services, About, Committee Members, available at http://www.armed-services.senate.gov/about/members (last viewed Sept. 2, 2015).
### MAJORITY (Republican)

- John McCain, Arizona, Chairman
- James M. Inhofe, Oklahoma
- Jeff Sessions, Alabama
- Roger F. Wicker, Mississippi
- Kelly Ayotte, New Hampshire
- Deb Fischer, Nebraska
- Tom Cotton, Arkansas
- Mike Rounds, South Dakota
- Joni Ernst, Iowa
- Thom Tillis, North Carolina
- Dan Sullivan, Arkansas
- Mike Lee, Utah
- Lindsey Graham, South Carolina
- Ted Cruz, Texas

### MINORITY (Democratic)

- Jack Reed, Rhode Island, Ranking Member
- Bill Nelson, Florida
- Claire McCaskill, Missouri
- Joe Manchin, West Virginia
- Jeanne Shaheen, New Hampshire
- Kirsten E. Gillibrand, New York
- Richard Blumenthal, Connecticut
- Joe Donnelly, Indiana
- Mazie K. Hirono, Hawaii
- Tim Kaine, Virginia
- Angus S. King, Maine
- Martin Heinrich, New Mexico

---

**Key Staff:**

*Majority and Non-Designated:*
Majority Staff Director..........................Chris Brose
Deputy Staff Director..............................Cord Sterling
Policy Director and Counsel ..............Katie Wheelbarger
Majority General Counsel......................Steven M. Barney
Senior Military Advisor.......................James Hickey
Chief Clerk..............................................Greg R. Lilly
Chief Investigator..................................Kathryn Edelman
Counsel ..................................................Samantha Clark
Communications Director......................Dustin Walker

Majority Professional Staff:

Adam J. Barker, Matt Donovan, Elizabeth Everett, Allen M. Edwards, Anish Goel, Tom W. Goffus, Bill Greenwalt, Jeremy Hayes, John Lehman, Daniel A. Lerner, Brad Patout, Jason Potter, Diem Salmon, Eric Sayers, Rob Soofer, Jennifer White

Security Manager.................................Barry Walker
Systems Administrator.............................Gary Howard
Special Assistant .................................Jackie Kerber
Research Analyst....................................Lauren Davis,
                                          ..........Natalie Nicolas
Staff Assistant......................................Brendan Sawyer,
                                          Leah Scheunemann,
                                          Robert Waisanen

Majority Staff Subject Areas:

Budget ......................................................Diem Salmon
CYBERCOM ...............................................Daniel Lerner
Combating Terrorism............................Katie Wheelbarger
Cybersecurity.........................................Daniel Lerner
Defense Laboratory Management...............Cord Sterling
Defense Security Assistance....................Adam Barker
Domestic Preparedness .......................... Adam Barker
Homeland Defense/Security ........................ Adam Barker
Information Assurance ............................. Daniel Lerner
Information Management .......................... Jeremy Hayes
Information Operations ............................. Daniel Lerner
Information Technology Systems:
  IT Acquisition Policy.......................... Bill Greenwalt
  Business Systems ............................... Jeremy Hayes
  Tactical Systems ................................ James Hickey
Intelligence Issues ............................... Katie Wheelbarger
Investigations ................................. Kathryn Edelman,
                                          Jennifer White,
                                          Brad Patout
Science and Technology ....................... Anish Goel
Strategic Programs .............................. Rob Soofer

Minority Staff:
Minority Staff Director .......................... Elizabeth L. King
Minority General Counsel ....................... Gerald J. Leeling
Counsel ........................................... William G.P. Monahan,
                                          Jonathan D. Clark,
                                          Ozge Guzelsu,
                                          Jonathan S. Epstein
Professional Staff ............................... Creighton Greene,
                                          Maggie McNamara,
                                          Thomas K. McConnell,
                                          Michael J. Kuiken,
                                          Arun A. Seraphin,
                                          William K. Sutey,
                                          Michael J. Noblet,
                                          John H. Quirk V,
                                          Carolyn A. Chuhta

Minority Staff Subject Areas:
Building Partnership Capacity
Program........................................... William G.P. Monahan
                                        Michael J. Kuiken
Senior Advisor, Budget ..................... William K. Sutey
CYBERCOM ..................................... Thomas K. McConnell
Counterterrorism Policy ..................... Michael J. Kuiken
                                        William G.P. Monahan
                                        Michael J. Noblet
                                        Thomas K. McConnell
                                        Ozge Guzelsu
Cybersecurity............................... Thomas K. McConnell,
                                        Creighton Greene
Defense Security Cooperation
Agency............................................. Michael J. Kuiken
Domestic Preparedness ...................... Carolyn A. Chuhta
Homeland Defense/Security ................. Carolyn A. Chuhta,
                                        Maggie McNamara
Information Assurance...................... Thomas K. McConnell
                                        Creighton Greene
Information Management.................... Creighton Greene
                                        Arun A. Seraphin
Information Operations ..................... Michael J. Kuiken
Information Technology Systems:
  IT Acquisition Policy...................... Arun A. Seraphin
                                        Thomas K. McConnell
  Business Systems........................... Arun A. Seraphin
Intelligence Issues......................... Thomas K. McConnell,
                                        Creighton Greene
Investigations............................... Ozge Guzelsu
Science & Technology...................... Arun A. Seraphin
Strategic Communications.................. Michael J. Kuiken
Strategic Programs ......................... Jonathan S. Epstein
A. SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

The Senate Armed Services Committee’s Subcommittee on Emerging Threats and Capabilities states that its jurisdiction includes responsibility for “Policies and programs to counter emerging threats including the proliferation of weapons of mass destruction, terrorism, and illegal drugs; homeland defense; technology base programs; special operations programs; and emerging operational concepts.”87 Membership of the Senate Committee on Armed Services Committee’s Subcommittee on Emerging Threats and Capabilities is as follows.88

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deb Fischer, Nebraska, Chair</td>
<td>Bill Nelson, Florida, Ranking Member</td>
</tr>
<tr>
<td>Kelly Ayotte, New Hampshire</td>
<td>Joe Manchin, West Virginia</td>
</tr>
<tr>
<td>Tom Cotton, Arkansas</td>
<td>Jeanne Shaheen, New Hampshire</td>
</tr>
<tr>
<td>Joni Ernst, Iowa</td>
<td>Kirsten Gillibrand, New York</td>
</tr>
<tr>
<td>Thom Tillis, North Carolina</td>
<td>Joe Donnelly, Indiana</td>
</tr>
<tr>
<td>Lindsey Graham, South Carolina</td>
<td>Tim Kaine, Virginia</td>
</tr>
<tr>
<td>Ted Cruz, Texas</td>
<td>Jack Reed,</td>
</tr>
</tbody>
</table>


88 Id.
John McCain, Arizona, Ex Officio | Rhode Island, Ex Officio

Key Staff:

*Majority Staff (Lead)*: Tom W. Goffus

*Majority Research Analyst*: Natalie Nicolas


B. SUBCOMMITTEE ON READINESS AND MANAGEMENT SUPPORT

The Senate Armed Services Committee’s Subcommittee on Readiness and Management Support states that its jurisdiction, in relevant part, includes responsibility for “Military readiness including training, logistics, and maintenance;… contracting and acquisition policy; defense industrial and technology base policies;… [and] information technology management policy.” 89 In addition, this subcommittee has oversight responsibility for the following Department of Defense offices: “Under Secretary of Defense (Acquisition, Technology, and Logistics); Department of Defense Deputy Chief

---

Management Officer; and the Chief Management Officers of the military departments.”

Membership of the Senate Committee on Armed Services Committee’s Subcommittee on Readiness and Management Support is as follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kelly Ayotte, New Hampshire, Chair</td>
<td>Tim Kaine, Virginia, Ranking Member</td>
</tr>
<tr>
<td>James M. Inhofe, Oklahoma</td>
<td>Claire McCaskill, Missouri</td>
</tr>
<tr>
<td>Deb Fischer, Nebraska</td>
<td>Jeanne Shaheen, New Hampshire</td>
</tr>
<tr>
<td>Mike Rounds, South Dakota</td>
<td>Mazie K. Hirono, Hawaii</td>
</tr>
<tr>
<td>Joni Ernst, Iowa</td>
<td>Martin Heinrich, New Mexico</td>
</tr>
<tr>
<td>Mike Lee, Utah</td>
<td>Jack Reed, Rhode Island, Ex Officio</td>
</tr>
<tr>
<td>John McCain, Arizona, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

Key Staff:
Majority Staff (Lead).......................... Bill Greenwalt
Staff Assistant: ..................... Leah Scheunemann
Minority Staff................. John H. Quirk V (Lead), Arun Seraphin, Michael J. Noblet, Ozge Guzelsu

C. SUBCOMMITTEE ON STRATEGIC FORCES

The Senate Armed Services Committee’s

---

90 Id.
91 Id.
Subcommittee on Strategic Forces has numerous areas of responsibility, including “Nuclear and strategic forces; intelligence programs; space programs; cyber space programs; Department of Energy defense nuclear and environmental programs; and ballistic missile defense.” The subcommittee’s budget oversight responsibility includes: “Procurement and RDT&E for DOD nuclear and strategic forces, missile defense, space systems, and cyberspace systems; Department of Energy defense-funded programs; intelligence activities, including the National Intelligence Program and the Military Intelligence Program.” This subcommittee is also responsible for DOD and DOE oversight of the “Under Secretary of Defense (Intelligence); Assistant Secretary of Defense for Nuclear and Chemical and Biological Defense Programs; National Nuclear Security Administration; and Assistant Secretary of Energy (Environmental Management).” Other oversight responsibilities include: “Strategic Command; space commands of the military departments; Missile Defense Agency; National Security Agency; Defense Intelligence Agency; National Reconnaissance Office; National Geospatial-Intelligence Agency; and Defense Nuclear Facilities Safety Board.”

Membership of the Senate Committee on Armed Services Committee’s Subcommittee on Strategic Forces is as follows:

93 Id.
94 Id.
95 Id.
96 Id.
MAJORITY (Republican)                  MINORITY (Democratic)
Jeff Sessions, Alabama, Chairman        Joe Donnelly, Indiana, Ranking Member
James M. Inhofe, Oklahoma               Bill Nelson, Florida
Deb Fischer, Nebraska                   Joe Manchin, West Virginia
Mike Lee, Utah                           Angus S. King, Maine
Lindsey Graham, South Carolina           Martin Heinrich, New Mexico
Ted Cruz, Texas                         Jack Reed, Rhode
John McCain, Arizona, Ex Officio        Island, Ex Officio

Key Staff:

Majority Staff (Lead)....................Rob Soofer (Lead)
Staff Assistant..................................Lauren Davis
Minority Staff....................Jonathan S. Epstein (lead),
                              Creighton Greene,
                              Thomas K. McConnell,
                              Carolyn A. Chuhta

VII. Senate Committee On Banking, Housing
And Urban Affairs

During December 2014 the Senate Committee on Banking, Housing and Urban Affairs held oversight hearings on “Cybersecurity: Enhancing Coordination to Protect the Financial Sector.” A hearing on “Oversight of

Financial Stability and Data Security” was held during February, 2014.” Membership of the Senate Committee on Banking, Housing and Urban Affairs consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richard Shelby, Alabama, Chairman</td>
<td>Sherrod Brown, Ohio, Ranking Member</td>
</tr>
<tr>
<td>Mike Crapo, Idaho</td>
<td>Jack Reed, Rhode Island</td>
</tr>
<tr>
<td>Bob Corker, Tennessee</td>
<td>Charles Schumer, New York</td>
</tr>
<tr>
<td>David Vitter, Louisiana</td>
<td>Robert Menendez, New Jersey</td>
</tr>
<tr>
<td>Patrick Toomey, Pennsylvania</td>
<td>Mark Warner, Virginia</td>
</tr>
<tr>
<td>Mark Kirk, Illinois</td>
<td>Jeff Merkley, Oregon</td>
</tr>
<tr>
<td>Dean Heller, Nevada</td>
<td>Elizabeth Warren, Massachusetts</td>
</tr>
<tr>
<td>Tim Scott, South Carolina</td>
<td>Heidi Heitkamp, North Dakota</td>
</tr>
<tr>
<td>Ben Sasse, Nebraska</td>
<td>Joe Donnelly, Indiana</td>
</tr>
<tr>
<td>Tom Cotton, Arkansas</td>
<td>Mike Rounds, South Dakota</td>
</tr>
<tr>
<td>Jerry Moran, Kansas</td>
<td></td>
</tr>
</tbody>
</table>


Key Staff:
Majority and Non-Designated:

Majority Staff Director & Counsel: William Duhnke

 Majority Deputy Staff Director ........ Dana Wade
 Majority Chief Counsel ........ Jelena McWilliams
 Majority Senior Counsel ........ Beth Zorc
 Senior Counsel (Nat’l Security)
 And Chief Investigative Counsel .... Chris Ford
 Majority Counsel .................. Travis Hill
 Senior Investigative Counsel ...... Lucas Moskowitz,
 John O’Hara
 Investigative Counsel .............. Brian Daner
 Securities Counsel .................. Elad Roisman
 Majority Chief Economist .......... Thomas Hogan
 Majority Sr. Professional Staff ...... Chad Davis,
 Shannon Hines
 Majority Professional Staff ....... Shelby Begany,
 Jennifer Deci, and Jay Dunn

Minority staff members:

Minority Staff Director ............ Mark Powden
Minority Deputy Staff Director ... Laura Swanson
Minority Policy Director ....... Colin P.J. McGinnis
Minority Chief Counsel ............ Graham Steele
Minority Senior Counsel ........... Jeanette Quick,
 Elisha Tuku
Minority Press Secretary ............ Greg Vadala
Minority Legislative Assistants ... Megan Cheney
   Phil Rudd
Minority Professional Staff ......... Erin Berry
   Homer Carlisle
 Beth Cooper and Adam Healy
VIII. Senate Commerce, Science And Transportation Committee

Through U.S. history, numerous Senate committees have held jurisdiction over subject matter currently assigned to the Committee on Commerce, Science and Transportation. As you might suspect, the Senate’s needs during colonial and frontier times were much different than today. Accordingly, over the years the jurisdiction held by today’s Committee was governed by the following progenitor committees: “Committee on Commerce and Manufactures (1816-1825); Committee on Commerce (1825-1946, 1961-1977); Committee on Manufactures (1825-1855, 1864-1946); Committee on Interstate Commerce (1885-1946); Committee on Interocanean Canals (1899-1946); Committee on Interstate and Foreign Commerce (1946-1961); and Committee on Aeronautical and Space Sciences (1958-1977).”\(^\text{100}\) The Committee reports that

In 1961, the name of the Committee on Interstate and Foreign Commerce was shortened to the Committee on Commerce. Many simply called it the "Commerce Committee," a shorthand reference to the Committee that continues to this day…

The Committee System Reorganization Amendments of 1977… changed the name of the

Committee on Commerce to the present-day Committee on Commerce, Science, and Transportation. The Committee on Aeronautical and Space Sciences was terminated in 1977; its functions were transferred to the modern-day "Commerce Committee."

This name change was made to reflect the expanded jurisdiction given the Committee… Specifically, the Committee was given responsibility for the regulation of consumer products and services for the first time. The Committee also was charged with the nation’s science, engineering, and technology policy. Related to its new science responsibilities was jurisdiction over non-military aeronautical and space science policy…

In a move related to the Committee's new science responsibilities, it also was given jurisdiction over transportation issues surrounding non-military aeronautical and space policy.\textsuperscript{101}

Membership of the Senate Commerce, Science, and Transportation Committee is as follows:\textsuperscript{102}

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Thune,</td>
<td>Bill Nelson, Florida,</td>
</tr>
<tr>
<td>South Dakota, Chairman</td>
<td>Ranking Member</td>
</tr>
</tbody>
</table>


\textsuperscript{102} U.S. Senate Committee on Commerce, Science, & Transportation, Committee Membership List, available at http://www.senate.gov/general/committee_membership/committee_memberships_SSCM.htm (last viewed Sept. 2, 2015).
Roger Wicker, Mississippi
Roy Blunt, Missouri
Marco Rubio, Florida
Kelly Ayotte, New Hampshire
Ted Cruz, Texas
Deb Fischer, Nebraska
Jerry Moran, Kansas
Dan Sullivan, Alaska
Ron Johnson, Wisconsin
Dean Heller, Nevada
Cory Gardner, Colorado
Steve Daines, Montana

Maria Cantwell, Washington
Claire McCaskill, Missouri
Amy Klobuchar, Minnesota
Richard Blumenthal, Connecticut
Brian Schatz, Hawaii
Ed Markey, Massachusetts
Cory Booker, New Jersey
Tom Udall, New Mexico
Joe Manchin, West Virginia
Gary Peters, Michigan

Key Staff:
Majority and Non-Designated:

Majority Staff Director ...........David Schwietert
Majority Deputy Staff Director ........Nick Rossi
Majority General Counsel ..........Rebecca Seidel
Majority Deputy General Counsel Jason Van Beek
Legislative Counsel..................Jennifer Dorrer
Chief Clerk..........................Anne Willis Hill
Hearing Clerk.......................Stephanie Gamache
Majority Chief Investigator.........Ashok Pinto
Majority Office Manager ..........Theresa Eugene
Maj. Communications Director ....Frederick Hill

Director of Information
Technology..........................Jonathan Bowen
Minority staff members:

Minority Staff Director ...............Kim E. Lipsky
Minority Deputy Staff Director. Christopher Day
Minority General Counsel ...............Clint Odom
Minority Investigative Counsel........ Meeran Ahn
Minority Communications Dir.......Bryan Gulley

A. SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY AND THE INTERNET

The Senate Commerce, Science, and Transportation Committee’s Subcommittee on Communications, Technology, and the Internet states that its jurisdiction includes

jurisdiction over legislation, congressional action, and other matters relating to communications. For these purposes, “communications” includes telephones, cell phones, the Internet, commercial and noncommercial television, cable, satellite broadcast, satellite communications, wireline and wire-less broadband, radio, consumer electronic equipment associated with such services, and public safety communications. The Subcommittee also is responsible for oversight of the Federal Communications Commission (FCC), the Corporation for Public Broadcasting (CPB), and the National Telecommunications and Information Administration (NTIA) at the Department of Commerce, which is the administration primarily responsible for the management of government
spectrum and advising the President on telecommunications policy.\footnote{103}

Membership of the Senate Commerce, Science, and Transportation Committee’s Sub-committee on Communications, Technology, and the Internet consists of:\footnote{104}

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roger Wicker, Mississippi, Chairman</td>
<td>Brian Schatz, Hawaii, Ranking Member</td>
</tr>
<tr>
<td>Roy Blunt, Missouri</td>
<td>Maria Cantwell, Washington</td>
</tr>
<tr>
<td>Marco Rubio, Florida</td>
<td>Claire McCaskill, Missouri</td>
</tr>
<tr>
<td>Kelly Ayotte, New Hampshire</td>
<td>Amy Klobuchar, Minnesota</td>
</tr>
<tr>
<td>Ted Cruz, Texas</td>
<td>Richard Blumenthal, Connecticut</td>
</tr>
<tr>
<td>Deb Fischer, Nebraska</td>
<td>Edward J. Markey, Massachusetts</td>
</tr>
<tr>
<td>Jerry Moran, Kansas</td>
<td>Cory Booker, New Jersey</td>
</tr>
<tr>
<td>Dan Sullivan, Alaska</td>
<td>Tom Udall, New Mexico</td>
</tr>
<tr>
<td>Ron Johnson, Wisconsin</td>
<td>Joe Manchin, West Virginia</td>
</tr>
<tr>
<td>Dean Heller, Nevada</td>
<td>Gary C. Peters, Michigan</td>
</tr>
<tr>
<td>Cory Gardner, Colorado</td>
<td>Bill Nelson,</td>
</tr>
<tr>
<td>Steve Daines, Montana</td>
<td></td>
</tr>
<tr>
<td>John Thune,</td>
<td></td>
</tr>
</tbody>
</table>


Key Staff:

Majority staff members:
Majority Policy Director..........David Quinalty
Majority Counsel....................Jeffrey Farrah,
                                 Gregory Orlando,
                                 Jason Van Beek
Advisor to Chmn. Wicker..........Crystal Tully
Majority Research Asst...........Matthew Plaster
Additional Staff....................Jamie Susskind
Minority staff members:
Minority Senior Counsel...........John Branscome
Minority Counsel....................Shawn Bone
Minority Legislative Asst..........Simone Hall
Advisor to Ranking Member SchatzMelika Carroll

B. SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE AND DATA SECURITY

The Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security has jurisdiction over matters involving the protection of consumers. Regarding the fairness of consumer transactions, the Subcommittee “S]eeks to prevent scams and fraud, and promotes the safety of products people buy. In the modern economy, commerce increasingly includes the exchange of sensitive personal information, either
online or in consumer-facing settings.”

Membership of the Senate Commerce, Science, and Transportation Committee’s Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jerry Moran, Kansas, Chairman</td>
<td>Richard Blumenthal, CT, Ranking Member</td>
</tr>
<tr>
<td>Roy Blunt, Missouri</td>
<td>Claire McCaskill, Missouri</td>
</tr>
<tr>
<td>Ted Cruz, Texas</td>
<td>Amy Klobuchar, Minnesota</td>
</tr>
<tr>
<td>Deb Fischer, Nebraska</td>
<td>Edward J. Markey, Massachusetts</td>
</tr>
<tr>
<td>Dean Heller, Nevada</td>
<td>Cory Booker, New Jersey</td>
</tr>
<tr>
<td>Cory Gardner, Colorado</td>
<td>Tom Udall, New Mexico</td>
</tr>
<tr>
<td>Steve Daines, Montana</td>
<td>Bill Nelson, Florida, Ex Officio</td>
</tr>
<tr>
<td>John Thune, South Dakota, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

**Majority Staff Members:**

*Majority Counsel* ......................... Peter Feldman

*Majority Investigator* ................. Cherilyn Pascoe

*Staff Research Assistant* .............. Andrew Timm

**Minority Staff Members:**

*Minority Senior Counsel* ............. Christian Fjeld

---


The Subcommittee on Science, Space and Competitiveness is charged with oversight responsibility for issues impacting science, technology, engineering, and math research and development and policy; standards and measurement; and civil space policy. The Subcommittee conducts oversight on the National Science Foundation, the National Aeronautics and Space Administration, the National Institute of Standards and Technology, the Office of Science and Technology Policy, and the National Technical Information Service. Advancements in science and technology are vital to the nation’s continued economic security, innovation, and competitiveness.\footnote{See U.S. Senate Committee on Commerce, Science, & Transportation, Subcommittee on Science, Space and Competitiveness, available at http://www.commerce.senate.gov/public/index.cfm?p=ScienceandSpace (last viewed Sept. 2, 2015).}

Membership of the Senate Commerce, Science, and Transportation Committee’s Sub-committee on Science, Space and Competitiveness consists of:\footnote{Id.}

\begin{itemize}
\item MAJORITY (Republican)  
\item MINORITY (Democratic)
\end{itemize}
<table>
<thead>
<tr>
<th>Ted Cruz, Texas, Chairman</th>
<th>Gary Peters, Michigan, Ranking Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marco Rubio, Florida</td>
<td>Edward J. Markey, Massachusetts</td>
</tr>
<tr>
<td>Jerry Moran, Kansas</td>
<td>Cory Booker, New Jersey</td>
</tr>
<tr>
<td>Dan Sullivan, Alaska</td>
<td>Tom Udall, New Mexico</td>
</tr>
<tr>
<td>Cory Gardner, Colorado</td>
<td>Brian Schatz, Hawaii</td>
</tr>
<tr>
<td>Steve Daines, Montana</td>
<td>Bill Nelson, Florida, Ex Officio</td>
</tr>
<tr>
<td>John Thune, South Dakota, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

*Majority Staff Members* ........... Bailey Edwards, Suzanne Matwyshen-Gillen Missye Brickell

*Staff Assistant* ......................... Jaclyn Keshian

*Minority Staff Director* .......... Nick Cummings

*Minority Professional Staff* .......... Alicia Brown

*Staff Assistant* ......................... Owen Berger

IX. Senate Homeland Security And Governmental Affairs Committee (HSGAC)

Following passage of the Homeland Security Act of 2002, this Committee changed its name from its former designation as the Senate Governmental Affairs Committee to reflect its expanded jurisdiction which now includes “homeland security issues. In addition to governmental affairs, the Committee now oversees and receives legislation, messages, petitions, and memorials on all matters relating to the Department of Homeland Security, except for appropriations, the Coast Guard, the Transportation Security Administration, immigration,
customs revenue, commercial operations, and trade.”  

As the Senate’s primary oversight committee, the HSGAC has general broad jurisdiction over government operations, and particularly over the Department of Homeland Security. The primary responsibilities of the HSGAC include: “to study the efficiency, economy, and effectiveness of all agencies and departments of the federal government; evaluate the effects of laws enacted to reorganize the legislative and executive branches of government; and study the intergovernmental relationships between the U.S. and states and municipalities… and international organizations,” where the United States has membership.  

The four Subcommittees of the HSGAC are: the Permanent Subcommittee on Investigations (PSI); Financial and Contracting Oversight (FCO); The Efficiency and Effectiveness of Federal Programs and the Federal Workforce (FPFW); and the Emergency Management, Intergovernmental Relations and the District of Columbia (EMDC).  

With respect to cyber-security, the HSGAC has held numerous hearings, including on the topic of “Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies.”

---

110 Id.
111 Id.

that “Senator Johnson has said that he is interested in using the committee’s investigative powers to pursue ‘border security and illegal immigration, cybersecurity, homegrown terrorist threats, securing the electrical grid, streamlining oversight of the DHS and the regulation of American businesses – particularly the energy sector.’” On January 28, 2015 hearings were held by the HSGAC on the subject of “Protecting America from Cyber Attacks: The Importance of Information Sharing.” Other important cyber related hearings include those on the topics of: The IRS Data Breach: Steps to Protect Americans’ Personal Information, and Under Attack: Federal Cybersecurity and the OPM Data Breach. Membership of the Senate


Homeland Security and Government Affairs Committee is as follows:  

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ron Johnson, Wisconsin, Chairman</td>
<td>Thomas R. Carper, Delaware, Ranking Member</td>
</tr>
<tr>
<td>John McCain, Arizona</td>
<td>Claire McCaskill, Missouri</td>
</tr>
<tr>
<td>Rob Portman, Ohio</td>
<td>Jon Tester, Montana</td>
</tr>
<tr>
<td>Rand Paul, Kentucky</td>
<td>Tammy Baldwin, Wisconsin</td>
</tr>
<tr>
<td>James Lankford, Oklahoma</td>
<td>Heidi Heitkamp, North Dakota</td>
</tr>
<tr>
<td>Michael B. Enzi, Wyoming</td>
<td>Cory A. Booker, New Jersey</td>
</tr>
<tr>
<td>Kelly Ayotte, New Hampshire</td>
<td>Gary C. Peters, Michigan</td>
</tr>
<tr>
<td>Joni Ernst, Iowa</td>
<td></td>
</tr>
<tr>
<td>Ben Sasse, Nebraska</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

**Majority and Non-Designated:**

*Majority Staff Director* ................................. Keith Ashdown

*Majority Chief Counsel* ................................. Christopher Hixon

*Majority Chief Counsel (Gov. Affairs)* ................................. Patrick Bailey

*Majority Deputy Chief Counsel (Governmental Affairs)* ................................. Gabrielle Singer

*Majority Chief Counsel (for Investigations)* ................................. David Brewer


During May 2014, the Permanent Subcommittee on Investigations held a hearing, “Online Advertising and Hidden Hazards to Consumer Security and Data Privacy,”
“investigate data collection processes and security vulnerabilities that have inflicted significant costs on Internet users and American businesses.”

Membership of the Senate HSGAC’s Permanent Subcommittee on Investigations consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rob Portman, Ohio, Chairmen</td>
<td>Claire McCaskill, MO, Ranking Member</td>
</tr>
<tr>
<td>John McCain, Arizona</td>
<td>Jon Tester, Montana</td>
</tr>
<tr>
<td>Rand Paul, Kentucky</td>
<td>Tammy Baldwin, Wisconsin</td>
</tr>
<tr>
<td>James Lankford, Oklahoma</td>
<td>Heidi Heitkamp, North Dakota</td>
</tr>
<tr>
<td>Kelly Ayotte, New Hampshire</td>
<td></td>
</tr>
<tr>
<td>Ben Sasse, Nebraska</td>
<td></td>
</tr>
</tbody>
</table>

Key Staff:

Majority Staff Director ............... Brian Callanan
Majority Chief Counsel .................. Derek Lyons
Majority Senior Counsel ................. Mark Angehr
Majority Counsel ........................ Philip Alito, Andrew Polesovsky


Majority Policy Director............ Brent Bombach

C. Minority Staff Members:
Minority Staff Director ............. Margaret Daum
Minority Counsel ...................... Joseph Eaton,
Sarah Garcia,
Robert Roach,
Brandon Reavis

Minority Professional Staff..... Adam Henderson

X. Senate Select Committee on
Intelligence

Given the continued growth of suspected nation state involvement in cyberattacks, the Senate Select Committee on Intelligence (SSCI) plays an important role in the fabric of congressional cybersecurity oversight.\textsuperscript{120} The SSCI was created during 1976 as the appropriate committee to “oversee and make continuing studies of [U.S.] intelligence activities and programs…,” to “submit…appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs,” and to “provide vigilant legislative oversight over the intelligence activities… to assure that such activities are… Constitutional and [lawful].”\textsuperscript{121} As a

\textsuperscript{120} U.S. Senate Select Committee on Intelligence, About the Committee, Overview of the Senate Select Committee on Intelligence: Responsibilities and Activities, available at http://www.intelligence.senate.gov/about.html (last viewed Sept. 2, 2015).

\textsuperscript{121} U.S. Senate Select Committee on Intelligence, About the Committee, Overview of the Senate Select Committee on Intelligence: Responsibilities and Activities, available at http://www.intelligence.senate.gov/about.html (last viewed Sept. 2, 2015).
“select” rather than “standing” committee, the Senate majority and minority leaders are responsible for choosing SSCI members “rather than determined in the party caucuses that preceded each new Congress. The committee’s chairman and vice chairman would be selected by their respective caucus but could not, at the same time, serve as chairman or ranking minority member of a major standing committee.”

Committee membership is set at 15: “eight from the majority party and seven from the minority. The one-seat majority is dictated by Senate resolution and, unlike most other committees, does not change in proportion with the overall Senate ratio of majority to minority membership.” The SSCI is intentionally structured to promote bipartisanship, with “two members (one per side) from the Appropriations, Armed Services, Foreign Relations, and Judiciary Committees in order to ensure appropriate coordination with those Committees. The Senate Majority and Minority Leaders and the Chairman and Ranking Member of the Armed Services Committee serve as ex officio SSCI members.” The SSCI describes its activities as follows


123 U.S. Senate Select Committee on Intelligence, About the Committee, Overview of the Senate Select Committee on Intelligence: Responsibilities and Activities, available at http://www.intelligence.senate.gov/about.html (last viewed Sept. 2, 2015).

124 Id.
Hearings: The Committee meets roughly twice a week for 1 1/2 to 2 hours, generally in closed session. Most hearings involve appearances by senior Intelligence Community officials—heads of agencies, senior program managers, and senior intelligence analysts—who present testimony and answer Senators’ questions. The topics for hearings include agency activities, intelligence collection programs, and intelligence analysis on a geographic region or issue (e.g., stability in the Middle East, Iran’s nuclear program, terrorism threats). The Committee occasionally meets in open session, such as annual hearings to receive intelligence testimony on the national security threats to the United States, and for the Committee to consider the President’s nominees to intelligence positions requiring Senate confirmation.

Legislation: The Committee writes an annual intelligence authorization bill that authorizes funding levels for intelligence activities (these set caps for agency funding) and provides legislative provisions that limit or allow intelligence conduct. The Committee also periodically considers stand-alone legislation, including laws governing surveillance of U.S. citizens (such as the Foreign Intelligence Surveillance Act, known as “FISA”). On occasion,
the Committee reviews intelligence aspects of treaties as part of the Senate’s ratification process.

- Investigations and Reviews: The Committee conducts reviews of intelligence programs or events, ranging from routine and continuing study (the conduct of covert action programs and intelligence operations) to formal inquiries.

- Confirmations: The Committee considers and makes recommendations to the Senate for the President’s nominees to serve in intelligence positions requiring the Senate’s confirmation.

- Analysis: The Committee receives and reviews intelligence analysis on a broad range of topics to inform policy decisions.

- Daily Oversight: The Committee, through its staff, tracks the regular collection and analysis activities of the Intelligence Community, enabling the Committee to engage with the Intelligence Community early on if it becomes aware of an issue. The Committee’s Audit and Oversight staff conducts longer-term oversight projects.\(^\text{125}\)

\(^{125}\) Id. See also Nicholas R. Seabrook & Nick Cole, Secret Law: The Politics of Appointments to the U.S. Foreign Intelligence Surveillance Court (unpublished manuscript, on file with author).
During March 2015, the Senate Intelligence Committee passed the *Cybersecurity Information Sharing Act (S.754)*, creating “additional incentives to increase sharing of cybersecurity threat information while protecting individual privacy and civil liberties interests and offering liability protection to the private sector.”

Membership of the Senate Select Committee on Intelligence for the 114th Congress is as follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richard Burr, North Carolina, Chairman</td>
<td>Dianne Feinstein, Calif., Vice Chairman</td>
</tr>
<tr>
<td>James Risch, Idaho</td>
<td>Ron Wyden, Oregon</td>
</tr>
<tr>
<td>Dan Coats, Indiana</td>
<td>Barbara Mikulski, Maryland</td>
</tr>
<tr>
<td>Marco Rubio, Florida</td>
<td>Mark Warner, Virginia</td>
</tr>
<tr>
<td>Susan Collins, Maine</td>
<td>Martin Heinrich, New Mexico</td>
</tr>
<tr>
<td>Roy Blunt, Missouri</td>
<td></td>
</tr>
<tr>
<td>James Lankford, Oklahoma</td>
<td>Angus King, Maine</td>
</tr>
<tr>
<td>Tom Cotton, Arkansas</td>
<td>Mazie Hirono, Hawaii</td>
</tr>
<tr>
<td>Mitch McConnell, Kentucky, Ex Officio</td>
<td>Harry Reid, Nevada, Ex Officio</td>
</tr>
<tr>
<td>John McCain, Arizona, Ex Officio</td>
<td>Jack Reed, Rhode Island,</td>
</tr>
</tbody>
</table>


Key Staff:
Majority Staff Director .................... Chris Joyner
Majority Deputy Staff Director ........ Jack Livingston
Majority General Counsel ............... Michael Geffroy
Minority Staff Director ................. David Grannis
Minority Deputy Staff Director .......... Kerry Sutten
Counsel ................................. Michael Buchwald,
                                      Brett Freedman

Professional Staff ......................... Nate Adler
Director of Technology &
Information management ............... Oliver Galloway
Court Reporter .......................... Mark Egan
Senior Staff Assistant .................. Nicolette Fedorov
Subject Matter Experts ................. Josh Alexander,
                                      .................................................. Walter Weiss

Bipartisan Professional Staff: ......... Jennifer Barrett, Randy
Bookout, Jim Catella, Christian Cook, John Dickas, Evan
Gottesman, Tressa Guenov, Emily Harding, Dan Jones,
Ryan Kaldahl, John Matchison, Paul Matulic, Tara
McFeely, Hayden Milberg, Brian Miller, Matt Pollard, Jon
Rosenwasser, Chad Tanner, Lorne Teitelbaum, Ryan Tully,
Brian Walsh, and Ryan White

XI.  SENATE JUDICIARY COMMITTEE

Established in 1816 as one of the original Senate
standing committees, the influential Senate Committee on
the Judiciary enjoys broad legislative jurisdiction, thus
assuring “its primary role as a forum for the public
discussion of social and constitutional issues. The
Committee is also responsible for oversight of key
activities of the executive branch, and is responsible for the
initial stages of the confirmation process of all judicial nominations for the federal judiciary.”

Regarding jurisdiction, the Committee states:

In addition to its critical role in providing oversight of the Department of Justice and the agencies under the Department's jurisdiction, including the Federal Bureau of Investigation, and the Department of Homeland Security, the Judiciary Committee plays an important role in the consideration of nominations and pending legislation... Executive nominations for positions and... select nominations for the Department of Homeland Security and the Department of Commerce are referred to the Senate Judiciary Committee... In addition to its role in conducting oversight and consideration of nominations, the Senate Judiciary Committee also considers legislation, resolutions, messages, petitions, memorials and other matters, as provided for in the Standing Rules of the Senate. These areas include: Civil liberties... Government information... Judicial proceedings, civil and criminal, generally... Patent Office; Patents, copyrights, and trademarks... and Protection of trade and commerce against unlawful restraints and monopolies.

---

129 United States Senate Committee on the Judiciary, Jurisdiction,
Presented below is the Senate Judiciary Committee membership:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chuck Grassley, Iowa, Chairman</td>
<td>Patrick Leahy, Vermont, Ranking Member.</td>
</tr>
<tr>
<td>Orrin G. Hatch, Utah</td>
<td>Dianne Feinstein, California</td>
</tr>
<tr>
<td>Jeff Sessions, Alabama</td>
<td>Charles Schumer, New York</td>
</tr>
<tr>
<td>Lindsey Graham, South Carolina</td>
<td>Dick Durbin, Illinois</td>
</tr>
<tr>
<td>John Cornyn, Texas</td>
<td>Sheldon Whitehouse, Rhode Island</td>
</tr>
<tr>
<td>Michael S. Lee, Utah</td>
<td>Amy Klobuchar, Minnesota</td>
</tr>
<tr>
<td>Ted Cruz, Texas</td>
<td>Al Franken, Minnesota</td>
</tr>
<tr>
<td>Jeff Flake, Arizona</td>
<td>Christopher A. Coons, Delaware</td>
</tr>
<tr>
<td>David Vitter, Louisiana</td>
<td>Richard Blumenthal, Connecticut</td>
</tr>
</tbody>
</table>

Key Staff:

Majority and Non-Designated:

Majority Staff Director ........................................ Kolan Davis
Majority Deputy Staff Director ................................. Rita Lari
Majority Chief Counsel (for Nominations) .................... Ted Lehman
Chief Investigative Counsel ................................. Jason Foster
Majority Investigative Counsel .................... Josh Flynn-Brown
Paul Junge, Jay Lim,


A. SUBCOMMITTEE ON CRIME AND TERRORISM

The Senate Judiciary Committee’s Subcommittee on Crime and Terrorism describes its jurisdiction as follows:

(1) Oversight of the Department of Justice's (a) Criminal Division, (b) Drug Enforcement Administration, (c) Executive Office for U.S. Attorneys, (d) Office on Violence Against Women, (e) U.S. Marshals Service, (f) Community Oriented Policing Services and related law enforcement grants, (g) Bureau of Prisons, (h) Office of the Pardon Attorney, (i) U.S. Parole Commiss-ion, (j) Federal Bureau of Investig-ation, and (k) Bureau of Alcohol, Tobacco, Firearms, and Explosives, as it relates to crime or drug policy; (2) Oversight of the U.S. Sentencing Commission; (3) Youth violence and directly related
issues; (4) Federal programs under the Juvenile Justice and Delinquency Prevention Act of 1974, as amended (including the Runaway and Homeless Youth Act); (5) Criminal justice and victims' rights policy; (6) Oversight of the Office of National Drug Control Policy; (7) Oversight of the U.S. Secret Service; (8) Corrections, rehabilitation, reentry and other detention-related policy; and (9) Parole and probation policy; (10) Oversight of anti-terrorism enforcement and policy; (11) Oversight of Department of Homeland Security functions as they relate to anti-terrorism enforcement and policy; (12) Oversight of State Department consular operations as they relate to anti-terrorism enforcement and policy; (13) Oversight of encryption policies and export licensing; and (14) Oversight of espionage laws and their enforcement.¹³¹

Membership of the Judiciary Committee’s Subcommittee on Crime and Terrorism is presented below.¹³²

¹³² United States Senate Committee on the Judiciary, Members,
The Senate Judiciary Committee’s Subcommittee on Privacy, Technology and the Law provides the following description regarding its jurisdiction:

(1) Oversight of laws and policies governing the collection, protection, use and dissemination of commercial information by the private sector, including online behavioral advertising, privacy within social networking websites and other online privacy issues;

(2) Enforcement and implementation of commercial information privacy laws and policies; (3) Use of technology by the private sector to protect privacy, enhance transparency and encourage innovation; (4) Privacy standards for the collection, retention, use and dissemination of personally identifiable commercial information; and (5) Privacy implications of new or emerging technologies.\[^{133}\]

Presented below is a list of membership of the Judiciary Committee’s Subcommittee on Privacy, Technology and the Law.\[^{134}\]

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeff Flake, Arizona, Chairman</td>
<td>Al Franken, Ranking Member</td>
</tr>
<tr>
<td>Orrin G. Hatch, Utah</td>
<td>Dianne Feinstein, California</td>
</tr>
<tr>
<td>David Perdue, Georgia</td>
<td>Charles Schumer, New York</td>
</tr>
<tr>
<td>Michael S. Lee, Utah</td>
<td>Sheldon Whitehouse, Rhode Island</td>
</tr>
<tr>
<td>Thom Tillis, North Carolina</td>
<td>Christopher Coons, Delaware</td>
</tr>
<tr>
<td>Lindsey Graham, South Carolina</td>
<td>Patrick Leahy, Vermont, Ex</td>
</tr>
</tbody>
</table>


XII. The House

Professor Charles Jones observes that Congressional committees form “the framework within which legislative populations are formed for participating in cross-institutional networks.”135 The following committees in the House are expected to play a role in cybersecurity oversight during the 114th Congress: Armed Services; Energy and Commerce; Homeland Security; Oversight and Government Reform; Permanent Select Committee on Intelligence; and Science and Space Technology.

XIII. Armed Services Committee

The House Committee on Armed Services has exclusive jurisdiction over matters of “defense policy generally, ongoing military operations, the organization and reform of the Department of Defense and Department of Energy, counter-drug programs, acquisition and industrial

base policy, technology transfer and export controls, joint interoperability, the Cooperative Threat Reduction program, Department of Energy nonproliferation programs, and detainee affairs and policy.”

Membership of the House Committee on Armed Services for the 114th Congress is as follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Thornberry, Texas, Chairman</td>
<td>Adam Smith, Wash., Ranking Member</td>
</tr>
<tr>
<td>Walter B. Jones, North Carolina</td>
<td>Loretta Sanchez, California</td>
</tr>
<tr>
<td>J. Randy Forbes, Virginia</td>
<td>Robert A. Brady, Pennsylvania</td>
</tr>
<tr>
<td>Jeff Miller, Florida</td>
<td>Susan A. Davis, California</td>
</tr>
<tr>
<td>Joe Wilson, South Carolina</td>
<td>James R. Langevin, Rhode Island</td>
</tr>
<tr>
<td>Frank A. LoBiondo, New Jersey</td>
<td>Rick Larsen, Washington</td>
</tr>
<tr>
<td>Rob Bishop, Utah</td>
<td>Jim Cooper, Tennessee</td>
</tr>
<tr>
<td>Michael R. Turner, Ohio</td>
<td>Madeleine Z. Bordallo, Guam</td>
</tr>
<tr>
<td>John Kline, Minnesota</td>
<td>Joe Courtney, Connecticut</td>
</tr>
<tr>
<td>Mike Rogers, Alabama</td>
<td>Niki Tsongas, Massachusetts</td>
</tr>
<tr>
<td>Trent Franks, Arizona</td>
<td>John Garamendi, California</td>
</tr>
<tr>
<td>Bill Shuster, Pennsylvania</td>
<td>Henry C. “Hank” Johnson Jr., Georgia</td>
</tr>
<tr>
<td>K. Michael Conaway, Texas</td>
<td>Jackie Speier, California</td>
</tr>
<tr>
<td>Doug Lamborn, Colorado</td>
<td>Joaquin Castro, Texas</td>
</tr>
<tr>
<td>Robert J. Wittman, Virginia</td>
<td>Tammy Duckworth, Illinois</td>
</tr>
<tr>
<td>Duncan Hunter, California</td>
<td>Scott H. Peters, California</td>
</tr>
<tr>
<td>John Fleming, Louisiana</td>
<td></td>
</tr>
<tr>
<td>Mike Coffman, Colorado</td>
<td></td>
</tr>
</tbody>
</table>

Chris P. Gibson, New York  
Vicky Hartzler, Missouri  
Joseph J. Heck, Nevada  
Austin Scott, Georgia  
Mo Brooks, Alabama  
Richard B. Nugent, Florida  
Paul Cook, California  
Jim Bridenstine, Oklahoma  
Brad R. Wenstrup, Ohio  
Jackie Walorski, Indiana  
Bradley Byrne, Alabama  
Sam Graves, Missouri  
Ryan Zinke, Montana  
Elise Stefanik, New York  
Martha McSally, Arizona  
Steve Knight, California  
Tom MacArthur, New Jersey  
Steve Russell, Oklahoma

Marc A. Veasey, Texas  
Tulsi Gabbard, Hawaii  
Timothy Walz, Minnesota  
Beto O’Rourke, Texas  
Donald Norcross, New Jersey  
Ruben Gallego, Arizona  
Mark Takai, Hawaii  
Gwen Graham, Florida  
Brad Ashford, Nebraska  
Seth Moulton, Massachusetts  
Pete Aguilar, California

**Key Staff:**

**Majority and Non-Designated:**

*Majority Staff Director* .................................................. Robert Simmons  
*Majority Deputy Staff Director* .............................. Jenness Simler  
*Exec. Assistant to Staff Director* ..................... Candace Wagner  
*Majority General Counsel* .............................. Catherine McElroy  
*Majority Counsel* .......................................................... Tim Morrison  
*Majority Director of Communications* .............................. Claude Chafin  
*Majority Press Secretary* ......................................... Nick Mikula  
*Majority Spokesperson* ........................................ Alison Lynn  
*Majority Professional Staff*: ............ Heath Bope, Christopher Bright, Jaime Beth Cheshire, Everett Coleman, Elizabeth Conrad, Ryan Crumpler, Alexander Gallo, Kevin
The subcommittee on Oversight and Investigations conducts investigations and studies of all jurisdictional areas held by “the House Armed Services Committee,
including inquiries into allegations of waste, fraud, abuse, and wrongdoing and inefficiencies within the Department of Defense. Members and staff conduct comprehensive oversight studies of major programs and issues and produce reports for the Committee and DOD providing recommendations and improvements of these programs.”

Membership of the House Committee on Armed Services Committee’s Subcommittee on Oversight and Investigations is as follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vicky Hartzler, Missouri,</td>
<td>Jackie Speier, California,</td>
</tr>
<tr>
<td>Chairman</td>
<td>Ranking Member</td>
</tr>
<tr>
<td>Jeff Miller, Florida</td>
<td>Jim Cooper, Tennessee</td>
</tr>
<tr>
<td>K. Michael Conaway, Texas</td>
<td>Henry C. “Hank” Johnson</td>
</tr>
<tr>
<td>Joseph J. Heck, Nevada</td>
<td>Jr., Georgia</td>
</tr>
<tr>
<td>Austin Scott, Georgia</td>
<td>Gwen Graham, Florida</td>
</tr>
<tr>
<td>Martha McSally, Arizona</td>
<td>Adam Smith, Washington,</td>
</tr>
<tr>
<td>Mac Thornberry, Texas, Ex</td>
<td>Ex Officio</td>
</tr>
<tr>
<td>Officio</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

*Majority Staff Director* .................... Christopher Bright

*Majority Professional* ........................ Heath Bope,
                          Elizabeth Conrad

*Other* ................................. Darreisha Bates

*Minority Staff Director* ........................ Mike Amato

---


138 Id.
B. SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Responsibilities of the subcommittee on Emerging Threats and Capabilities include “overseeing counter-terrorism programs and initiatives and counter proliferation of weapons of mass destruction. Additionally, this subcommittee oversees U.S. Special Operations Forces, the Defense Advanced Research Projects Agency (DARPA), information technology and programs, force protection policy and oversight, and related intelligence support … [ensuring protection] against terrorist attacks and unconventional threats.” Membership of the House Committee on Armed Services Committee’s Subcommittee on Emerging Threats and Capabilities is as follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe Wilson, South Carolina,</td>
<td>James R. Langevin, Rhode</td>
</tr>
<tr>
<td>Chairman</td>
<td>Island,</td>
</tr>
<tr>
<td>John Kline, Minnesota</td>
<td>Ranking Member</td>
</tr>
<tr>
<td>Bill Shuster, Pennsylvania</td>
<td>Jim Cooper, Tennessee</td>
</tr>
<tr>
<td>Duncan Hunter, California</td>
<td>John Garamendi, California</td>
</tr>
<tr>
<td>Richard B. Nugent, Florida</td>
<td>Joaquin Castro, Texas</td>
</tr>
<tr>
<td>Ryan Zinke, Montana</td>
<td>Marc A. Veasey, Texas</td>
</tr>
<tr>
<td>Trent Franks, Arizona</td>
<td>Donald Norcross, New Jersey</td>
</tr>
<tr>
<td>Doug Lamborn, Colorado</td>
<td>Brad Ashford, Nebraska</td>
</tr>
<tr>
<td>Mo Brooks, Alabama</td>
<td>Pete Aguilar, California</td>
</tr>
<tr>
<td>Bradley Byrne, Alabama</td>
<td></td>
</tr>
</tbody>
</table>


140 Id.
Elise Stefanik, New York
Mac Thornberry, Texas, Ex Officio

Adam Smith, Washington, Ex Officio

**Key Staff:**
- *Majority Staff Director* ......................... Peter Villano
- *Majority Professional Staff* ..................... Kevin Gates
- *Minority Staff Director* ......................... Lindsay Kavanaugh
- *Minority Professional Staff* ..................... Brian Garrett

XIV. **Energy & Commerce Committee**

Created on December 14, 1795, the oldest House standing legislative committee is the Committee on Energy and Commerce (E&C). The Energy and Commerce Committee “is vested with the broadest jurisdiction of any congressional authorizing committee. Today it has responsibility for the nation’s telecommunications, consumer protection, food and drug safety, public health research, environmental quality, energy policy, and interstate and foreign commerce.” The E&C Committee has oversight jurisdiction of multiple independent agencies and cabinet-level departments, including the Departments of Commerce, Energy, Health and Human Services, and Transportation—and Environmental Protection Agency (EPA), Federal Communications Commission (FCC), Federal Trade Commission (FTC), and Food and Drug

---

Administration (FDA).142

Energy and Commerce Committee Chairman Fred Upton observes that “Sadly, every American is now aware of the economic havoc that hacking can wreak on American soil… It is a threat to private investment, public companies, jobs, economic freedom, and overall growth. The Sony incident underscores the clear and present threat to America’s thriving digital economy.”143 Accordingly, Chairman Upton announced that “the Energy and Commerce Committee will continue its active examination of this growing threat to jobs, whether from foreign nations, state enterprises, or other criminal elements. The economic damage is real, and we must work to protect American jobs and commerce.”144 Ranking member Frank Pallone states that the committee “will continue looking at ways to protect personal data from hackers, but we also need to craft new ways to make it harder for thieves and hackers to use personal information when it is stolen.”145

The committee’s previous cybersecurity threat and

142 Id.
144 Id.
security work has included such topics as: agency data protection; consumer information protection; intellectual property and technology protection; Internet governance and security; and supply chain security.\footnote{Id.} Subcommittees having jurisdiction over cybersecurity matters include: Commerce, Manufacturing, and Trade; Communications and Technology; Energy and Power; Health; and Oversight and Investigations.\footnote{United States House of Representatives, Energy & Commerce Committee, Subcommittees, available at http://energycommerce.house.gov/subcommittees (last viewed Sept. 2, 2015).} Membership of the House Energy & Commerce Committee is as follows.\footnote{United States House of Representatives, Energy & Commerce Committee, E&C Membership, available at http://energycommerce.house.gov/about/membership (last viewed Sept. 2, 2015).}

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fred Upton, Michigan, Chairman</td>
<td>Frank Pallone, Jr., N. J., Ranking Member</td>
</tr>
<tr>
<td>Joe Barton, Texas, Chairman Emeritus</td>
<td>Bobby L. Rush, Illinois</td>
</tr>
<tr>
<td>Ed Whitfield, Kentucky</td>
<td>Anna G. Eshoo, California</td>
</tr>
<tr>
<td>Joseph R. Pitts, Pennsylvania</td>
<td>Gene Green, Texas</td>
</tr>
<tr>
<td>Tim Murphy, Pennsylvania</td>
<td>Diana DeGette, Colorado</td>
</tr>
<tr>
<td>Michael C. Burgess, Texas</td>
<td>Lois Capps, California</td>
</tr>
<tr>
<td>Marsha Blackburn,</td>
<td>Michael F. Doyle, Pennsylvania</td>
</tr>
</tbody>
</table>

\footnote{Id.}
<table>
<thead>
<tr>
<th>Tennessee, Vice Chair</th>
<th>Jan Schakowsky, Illinois</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steve Scalise, Louisiana</td>
<td>G. K. Butterfield, North Carolina</td>
</tr>
<tr>
<td>Bob Latta, Ohio</td>
<td>Doris O. Matsui, California</td>
</tr>
<tr>
<td>Cathy McMorris Rodgers, Washington</td>
<td>Kathy Castor, Florida</td>
</tr>
<tr>
<td>Gregg Harper, Mississippi</td>
<td>John Sarbanes, Maryland</td>
</tr>
<tr>
<td>Leonard Lance, New Jersey</td>
<td>Jerry McNerney, California</td>
</tr>
<tr>
<td>Brett Guthrie, Kentucky</td>
<td>Peter Welch, Vermont</td>
</tr>
<tr>
<td>Pete Olson, Texas</td>
<td>Ben Ray Lujan, New Mexico</td>
</tr>
<tr>
<td>David McKinley, West Virginia</td>
<td>Paul Tonko, New York</td>
</tr>
<tr>
<td>Mike Pompeo, Kansas</td>
<td>John Yarmuth, Kentucky</td>
</tr>
<tr>
<td>Adam Kinzinger, Illinois</td>
<td>Yvette D. Clarke, New York</td>
</tr>
<tr>
<td>Morgan Griffith, Virginia</td>
<td>David Loeb, New York</td>
</tr>
<tr>
<td>Gus Bilirakis, Florida</td>
<td>David Loebsack, Iowa</td>
</tr>
<tr>
<td>Bill Johnson, Ohio</td>
<td>Kurt Schrader, Oregon</td>
</tr>
<tr>
<td>Billy Long, Missouri</td>
<td>Joseph P. Kennedy III, Massachusetts</td>
</tr>
<tr>
<td>Renee Ellmers, North Carolina</td>
<td>Tony Cardenas, California</td>
</tr>
<tr>
<td>Larry Bucshon, Indiana</td>
<td></td>
</tr>
<tr>
<td>Bill Flores, Texas</td>
<td></td>
</tr>
<tr>
<td>Susan Brooks, Indiana</td>
<td></td>
</tr>
<tr>
<td>Markwayne Mullin, Oklahoma</td>
<td></td>
</tr>
<tr>
<td>Richard Hudson, North Carolina</td>
<td></td>
</tr>
<tr>
<td>Chris Collins, New York</td>
<td></td>
</tr>
<tr>
<td>Kevin Cramer, North Dakota</td>
<td></td>
</tr>
</tbody>
</table>

*Key Staff:*
Majority and Non-Designated:

Majority Staff Director ................................................................. Gary Andres
Majority Deputy Staff Director .................................................... Alexa Marrero
Majority General Counsel ............................................................ Karen Christian
Majority Deputy General Counsel .............................................. Peter Kielty
Majority Chief Counsel .............................................................. Charles Ingebretson

(Oversight & Investigations)
Tom Hassenboehler

Majority Sr. Energy Counsel ....................................................... Mary Neumayr
Majority Counsel ........................................................................ Patrick Currier,
Graham Default,
Melissa Froelich,
John Stone

Majority Senior Professional Staff................................. Jerry Couri,
Marty Dannenfelser, Paul Edattel, Robert Horne, Carly
McWilliams, Brandon Mooney, Katie Novaria, John Ohly,
Tim Pataki, Tara Rothschild, Peter Spencer, Olivia Trusty,
and Andy Zach

Majority Professional Staff
Majority Senior Policy Advisor ....................................................... Ray Baum
Majority Policy Coordinators ......................................................... Allison Busbee,
James Decker, Mark Ratner
Christopher Santini,
Chris Sarley,
Nick Abraham

Majority Legislative Clerks ......................................................... Will Batson,
Brittany Havens,
Kirby Howard,
Charlotte Savercool,
Jessica Wilkerson,

Majority Communications
Director ................................................................. Sean C. Bonyun
Majority Press Secretary .................................................... Noelle Clemente,
A. SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

The E&C Subcommittee on Commerce, Manufacturing, and Trade states that it “has consistently focused on sensible consumer protections for the 21st century. The panel leads the committee’s efforts to address complex questions of individual privacy in the online ecosystem.” Membership of the House Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade consists of:
Key Staff:

Majority Staff Director .................................... Paul Nagle
Minority Chief Counsel................................. Michelle Ash
Counsel ....................................................... Lisa Goldman

B. SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

The E&C Subcommittee on Communications and Technology states that its jurisdiction includes

Electronic communications, both

Interstate and foreign, including voice, video, audio and data, whether transmitted
by wire or wirelessly, and whether transmitted by tele-communications, commercial or private mobile service, broadcast, cable, satellite, microwave, or other mode; technology generally; emergency and public safety commun-ications; cybersecurity, privacy, and data security; the Federal Commun-ications Commission, the National Telecommunications and Information Administration, the Office of Emergency Communications in the Department of Homeland Security; and all aspects of the above-referenced jurisdiction related to the Department of Homeland Security.149

Membership of the House Energy & Commerce Committee, Subcommittee on Communications and Technology is as follows:150

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greg Walden, Oregon, Chairman</td>
<td>Anna G. Eshoo, California, Ranking Member</td>
</tr>
<tr>
<td>Bob Latta, Ohio,</td>
<td>Michael F. Doyle,</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vice Chairman</th>
<th>Pennsylvania</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Shimkus, Illinois</td>
<td>Peter Welch, Vermont</td>
</tr>
<tr>
<td>Marsha Blackburn, Tennessee</td>
<td>John Yarmuth, Kentucky</td>
</tr>
<tr>
<td>Steve Scalise, Louisiana</td>
<td>Yvette D. Clarke, New York</td>
</tr>
<tr>
<td>Leonard Lance, New Jersey</td>
<td>David Loebsack, Iowa</td>
</tr>
<tr>
<td>Brett Guthrie, Kentucky</td>
<td>Bobby L. Rush, Illinois</td>
</tr>
<tr>
<td>Pete Olson, Texas</td>
<td>Diana DeGette, Colorado</td>
</tr>
<tr>
<td>Mike Pompeo, Kansas</td>
<td>G. K. Butterfield, North Carolina</td>
</tr>
<tr>
<td>Adam Kinzinger, Illinois</td>
<td>Doris O. Matsui, California</td>
</tr>
<tr>
<td>Gus Bilirakis, Florida</td>
<td>Jerry McNerney, California</td>
</tr>
<tr>
<td>Bill Johnson, Ohio</td>
<td>Ben Ray Lujan, New Mexico</td>
</tr>
<tr>
<td>Billy Long, Missouri</td>
<td>Frank Pallone, Jr., New Jersey, Ex Officio</td>
</tr>
<tr>
<td>Renee Ellmers, North Carolina</td>
<td></td>
</tr>
<tr>
<td>Chris Collins, New York</td>
<td></td>
</tr>
<tr>
<td>Kevin Cramer, North Dakota</td>
<td></td>
</tr>
<tr>
<td>Joe Barton, Texas</td>
<td></td>
</tr>
<tr>
<td>Fred Upton, Michigan, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

*Majority Chief Counsel* ........................................... David Redl

*Majority Counsel* ........................................... Kelsey Guyselman, Grace Koh

*Majority Senior Policy Advisor* .............................. Ray Baum

*Majority Other Staff* ........................................ Gene Fullano

*Minority Chief Counsel* ........................................ David Goldman

*Minority Policy Analyst* ...................................... Ryan Skukowski
C. SUBCOMMITTEE ON ENERGY AND POWER

The E&C Subcommittee on Energy and Power has broad jurisdiction over matters involving “energy information... cybersecurity... all laws, programs, and government activities affecting energy matters, including all aspects of the above-referenced jurisdiction related to the Department of Homeland Security.”151 Membership of the House Energy & Commerce Committee, Subcommittee on Energy and Power consists of:152

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ed Whitfield, Kentucky, Chairman</td>
<td>Bobby L. Rush, Illinois, Ranking Member</td>
</tr>
<tr>
<td>Pete Olson, Texas, Vice Chair</td>
<td>Jerry McNerney, California</td>
</tr>
<tr>
<td>John Shimkus, Illinois</td>
<td>Paul Tonko, New York</td>
</tr>
<tr>
<td>Joseph R. Pitts, Pennsylvania</td>
<td>Eliot L. Engel, New York</td>
</tr>
<tr>
<td>Bob Latta, Ohio</td>
<td>Gene Green, Texas</td>
</tr>
<tr>
<td>Gregg Harper, Mississippi</td>
<td>Lois Capps, California</td>
</tr>
<tr>
<td>David McKinley, West Virginia</td>
<td>Michael F. Doyle, Pennsylvania</td>
</tr>
<tr>
<td>Mike Pompeo, Kansas</td>
<td>Kathy Castor, Florida</td>
</tr>
<tr>
<td>Adam Kinzinger, Illinois</td>
<td>John Sarbanes, Maryland</td>
</tr>
<tr>
<td>Morgan Griffith, Virginia</td>
<td>Peter Welch, Vermont</td>
</tr>
<tr>
<td>Bill Johnson, Ohio</td>
<td>John Yarmuth, Kentucky</td>
</tr>
<tr>
<td>Billy Long, Missouri</td>
<td>David Loebsack, Iowa</td>
</tr>
<tr>
<td></td>
<td>Frank Pallone, Jr., N. J., Ex Officio</td>
</tr>
</tbody>
</table>

---


152 Id.
During August 2015, the Subcommittee on Health published the results of a year-long investigation, detailing “serious structural flaws at HHS and its operating divisions, including the Food and Drug Administration and the National Institutes of Health, which have led to poor information security. These problems have left HHS vulnerable to cyberattacks, which the report outlines have been numerous the past few years.”

E&C Subcommittee on Health is as follows:\footnote{154}{United States House of Representatives, Energy & Commerce Committee, Subcommittees, Health, available at \url{http://energycommerce.house.gov/subcommittees/health} (last viewed Sept. 2, 2015).}

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe Pitts, Texas, Chairman</td>
<td>Gene Green, Texas, Ranking Member</td>
</tr>
<tr>
<td>Brett Guthrie, Kentucky, Vice Chairman</td>
<td>Eliot L. Engel, New York</td>
</tr>
<tr>
<td>Ed Whitfield, Kentucky</td>
<td>Lois Capps, California</td>
</tr>
<tr>
<td>John Shimkus, Illinois</td>
<td>Jan Schakowsky, Illinois</td>
</tr>
<tr>
<td>Tim Murphy, Pennsylvania</td>
<td>G. K. Butterfield, North Carolina</td>
</tr>
<tr>
<td>Michael C. Burgess, Texas</td>
<td>Kathy Castor, Florida</td>
</tr>
<tr>
<td>Marsha Blackburn, Tennessee</td>
<td>John Sarbanes, Maryland</td>
</tr>
<tr>
<td>Cathy McMorris Rodgers, Washington</td>
<td>Doris O. Matsui, California</td>
</tr>
<tr>
<td>Leonard Lance, New Jersey</td>
<td>Ben Ray Lujan, New Mexico</td>
</tr>
<tr>
<td>Morgan Griffith, Virginia</td>
<td>Kurt Schrader, Oregon</td>
</tr>
<tr>
<td>Gus Bilirakis, Florida</td>
<td>Joseph P. Kennedy III, Massachusetts</td>
</tr>
<tr>
<td>Billy Long, Missouri</td>
<td>Tony Cardenas, California</td>
</tr>
<tr>
<td>Renee Ellmers, North Carolina</td>
<td>Frank Pallone, Jr., N. J., Ex Officio</td>
</tr>
<tr>
<td>Larry Bucshon, Indiana</td>
<td></td>
</tr>
<tr>
<td>Susan Brooks, Indiana</td>
<td></td>
</tr>
<tr>
<td>Chris Collins, New York</td>
<td></td>
</tr>
<tr>
<td>Kevin Cramer, North Dakota</td>
<td></td>
</tr>
</tbody>
</table>
Key Staff:

Majority Chief Counsel.............................. Clay Alspach
Majority Policy Advisor.............................. Heidi Stirrup
Other ........................................... Michelle Rosenberg, Traci Vitek
Minority Counsel .................................... Arielle Woronoff
Majority Policy Advisor.............................. Rachel Pryor
Policy Analyst ...................................... Ziky Ababiya

E. SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

The E&C Subcommittee on Oversight and Investigations states that it has “responsibility for oversight of agencies, departments and programs within the jurisdiction of the full committee, and for conducting investigations within such jurisdiction.” 155

Membership of the House Energy & Commerce Committee, Subcommittee on Oversight and Investigations is as follows: 156

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tim Murphy,</td>
<td>Diana DeGette, Colorado,</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pennsylvannia, Chairman</th>
<th>Ranking Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>David McKinley, West Virginia, Vice Chairman</td>
<td>Jan Schakowsky, Illinois</td>
</tr>
<tr>
<td>Michael C. Burgess, M.D., Texas</td>
<td>Kathy Castor, Florida</td>
</tr>
<tr>
<td>Marsha Blackburn, Tennessee</td>
<td>Paul Tonko, New York</td>
</tr>
<tr>
<td>Morgan Griffith, Virginia</td>
<td>John Yarmuth, Kentucky</td>
</tr>
<tr>
<td>Larry Bucshon, Indiana</td>
<td>Yvette D. Clarke, New York</td>
</tr>
<tr>
<td>Bill Flores, Texas</td>
<td>Joseph P. Kennedy, III, Massachusetts</td>
</tr>
<tr>
<td>Susan Brooks, Indiana</td>
<td>Gene Green, Texas</td>
</tr>
<tr>
<td>Markwayne Mullin, Oklahoma</td>
<td>Peter Welch, Vermont</td>
</tr>
<tr>
<td>Richard Hudson, North Carolina</td>
<td>Frank Pallone, Jr., New Jersey, (Ex Officio)</td>
</tr>
<tr>
<td>Chris Collins, New York</td>
<td></td>
</tr>
<tr>
<td>Kevin Cramer, North Dakota</td>
<td></td>
</tr>
<tr>
<td>Joe Barton, Texas</td>
<td></td>
</tr>
<tr>
<td>Fred Upton, Michigan, (Ex Officio)</td>
<td></td>
</tr>
</tbody>
</table>

Key Staff:

- **Majority Chief Counsel**: Charles Ingebretson
- **Minority Staff Director**: Chris Knauer
- **Minority Counsel**: Una Lee
- **Minority Professional Staff**: Debbie Letter

XV. House Committee on Financial Services

During oversight hearings on the topic “A Global Perspective on Cyber Threats,” Frank J. Cilluffo testified
that a single U.S. bank confronted 30,000 cyber-attacks during the prior week alone. \(^{157}\) Every day, an attack is mounted on average every 34 seconds, “and these attacks are just the attacks that the bank actually knows about, by virtue of a known malicious signature or IP address. As for the source of the known attacks, approximately 22,000 came from criminal organizations; and 400 from nation-states.” \(^{158}\) On June 24, 2015 the House Committee on Financial Services held hearings on “Evaluating the security of the U.S. Financial Sector.” \(^{159}\) Membership of the House Committee on Financial Services consists of: \(^{160}\)

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeb Hensarling, Texas, Chairman</td>
<td>Maxine Waters, California, Ranking Member</td>
</tr>
<tr>
<td>Peter T. King, New York</td>
<td>Carolyn B. Maloney, New York</td>
</tr>
<tr>
<td>Edward R. Royce,</td>
<td>Nydia M. Velázquez, New</td>
</tr>
</tbody>
</table>


\(^{158}\) Id.


<table>
<thead>
<tr>
<th>California</th>
<th>York</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frank D. Lucas, Oklahoma</td>
<td>Brad Sherman, California</td>
</tr>
<tr>
<td>Scott Garrett, New Jersey</td>
<td>Gregory W. Meeks, New</td>
</tr>
<tr>
<td>Randy Neugebauer, Texas</td>
<td>York</td>
</tr>
<tr>
<td>Patrick T. McHenry, North</td>
<td>Michael E. Capuano,</td>
</tr>
<tr>
<td>Carolina, Vice Chairman</td>
<td>Massachusetts</td>
</tr>
<tr>
<td>Stevan Pearce, New Mexico</td>
<td>Rubén Hinojosa, Texas</td>
</tr>
<tr>
<td>Bill Posey, Florida</td>
<td>Wm. Lacy Clay, Missouri</td>
</tr>
<tr>
<td>Michael G. Fitzpatrick,</td>
<td>Stephen F. Lynch,</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>Massachusetts</td>
</tr>
<tr>
<td>Lynn A. Westmoreland,</td>
<td>David Scott, Georgia</td>
</tr>
<tr>
<td>Georgia</td>
<td>Al Green, Texas</td>
</tr>
<tr>
<td>Blaine Luetkemeyer,</td>
<td>Emanuel Cleaver, Missouri</td>
</tr>
<tr>
<td>Missouri</td>
<td>Gwen Moore, Wisconsin</td>
</tr>
<tr>
<td>Bill Huizenga, Michigan</td>
<td>Keith Ellison, Minnesota</td>
</tr>
<tr>
<td>Sean P. Duffy, Wisconsin</td>
<td>Ed Perlmutter, Colorado</td>
</tr>
<tr>
<td>Robert Hurt, Virginia</td>
<td>James A. Himes,</td>
</tr>
<tr>
<td>Steve Stivers, Ohio</td>
<td>Connecticut</td>
</tr>
<tr>
<td>Stephen Lee Fincher,</td>
<td>John C. Carney, Jr.,</td>
</tr>
<tr>
<td>Tennessee</td>
<td>Delaware</td>
</tr>
<tr>
<td>Marlin A. Stutzman, Indiana</td>
<td>Terri A. Sewell, Alabama</td>
</tr>
<tr>
<td>Mick Mulvaney, South Carolina</td>
<td>Bill Foster, Illinois</td>
</tr>
<tr>
<td>Randy Hultgren, Illinois</td>
<td>Daniel T. Kildee, Michigan</td>
</tr>
<tr>
<td>Dennis A. Ross, Florida</td>
<td>Patrick Murphy, Florida</td>
</tr>
<tr>
<td>Robert Pittenger, North</td>
<td>John K. Delaney, Maryland</td>
</tr>
<tr>
<td>Carolina</td>
<td>Kyrsten Sinema, Arizona</td>
</tr>
<tr>
<td>Ann Wagner, Missouri</td>
<td>Joyce Beatty, Ohio</td>
</tr>
<tr>
<td>Andy Barr, Kentucky</td>
<td>Denny Heck, Washington</td>
</tr>
<tr>
<td>Keith J. Rothfus, Pennsylvania</td>
<td>Juan Vargas, California</td>
</tr>
</tbody>
</table>
Luke Messer, Indiana
David Schweikert, Arizona
Frank Guinta, New Hampshire
Scott Tipton, Colorado
Roger Williams, Texas
Bruce Poliquin, Maine
Mia Love, Utah
French Hill, Arkansas
Tom Emmer, Minnesota

**Key Staff:**

**Majority:**

*Majority Staff Director* .................. Shannon McGahn
*Majority Deputy Staff Director* ........... Kirsten Mork,
.............................................................. Jeff Emerson (Communications)
*Majority Policy Director* ..................... Ed Skala
*Majority Chief Counsel* ............................. Jim Clinger
*Majority Deputy Chief Counsel* ............ Frank Medina
*Majority General Counsel And Parliamentarian* ........................ Joseph Clark
*Majority Chief Oversight Counsel* ........... Uttam Dhillon
*Majority Senior Counsel and Chief Advisor, Regulatory Policy* .......... Ron Rubin
*Majority Senior Counsel* .......................... Kevin Edgar,
................................................................. Brian Johnson,
............................................................................ Clinton Jones
*Majority Counsel* ....................................... Joe Gammello,
............................................................................ Rebekah Goshorn,
............................................................................ Brett Sisto

*Majority Senior Professional Staff* ........ Anthony Chang,
................................................................. Tallman Johnson,
......................................................................... Joe Pinder
Majority Professional Staff: Brian Anderson, Jon Blum, Chris Brown, Katelyn Christ, Marliss McManus, Pete Meachum, Brian O’Shea, Jared Sawyer, Bryan Wood

Majority Chief Economist: Dino Falaschetti
Majority Legislative Assistant: Chase Burgess
Majority Research Analyst: Drew Davidhizar
Majority Communications Director: David Popp
Majority Communications Assistant: Maria Kim
Majority Digital Director: Scott Schmidt
Majority Administrative Assistant: Angela Gambo

Minority Staff:
Minority Staff Director: Charla Ouertatani
Minority Deputy Staff Director: Amanda Fischer
Minority Deputy Legislative Director and Counsel: Lisa Peto
Minority Senior Policy Director: Erika Jeffers
Minority Senior Counsel: Katelynn Bradley, Jarrod Loadholt

Minority Counsel: Esther Kahng, Jason Lynch

Minority Senior Professional Staff: Kris Erickson, Corey Frayer, Daniel McGlinchey, Kirk Schwarzbach

Minority Professional Staff: Ola Williams
Minority Communications Director: Christopher Spina
XVI. House Committee on Homeland Security

The House Committee on Homeland Security was chartered during 2002 to conduct hearings, craft necessary legislation on matters specific to homeland security, and to provide oversight over the U.S. Department of Homeland Security. Each of the Committee’s six subcommittees appears to have some relationship to the issues germane to cybersecurity: Subcommittee on Border and Maritime Security; Subcommittee on Counterterrorism and Intelligence; Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies; Subcommittee on Emergency Preparedness, Response and Communications; Subcommittee on Oversight and Management Efficiency; and Subcommittee on Transportation Security.161 During early 2015, the Committee on Homeland Security unanimously passed H.R. 1731, the National Cybersecurity Protection Advancement (NCPA) Act of 2015,162 and sent it to the full

House where it subsequently achieved passage.\textsuperscript{163}

Membership of the House Committee on Homeland Security for the 114\textsuperscript{th} Congress follows:\textsuperscript{164}

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael McCaul, Texas, Chairman</td>
<td>Bennie Thompson, Mississippi,</td>
</tr>
<tr>
<td>Lamar Smith, Texas</td>
<td>Ranking Member</td>
</tr>
<tr>
<td>Peter King, New York</td>
<td>Loretta Sanchez, California</td>
</tr>
<tr>
<td>Mike Rogers, Alabama</td>
<td>Sheila Jackson Lee, Texas</td>
</tr>
<tr>
<td>Candice S. Miller, Michigan</td>
<td>James R. Langevin, Rhode Island</td>
</tr>
<tr>
<td>Jeff Duncan, South Carolina</td>
<td>Brian Higgins, New York</td>
</tr>
<tr>
<td>Tom Marino, Pennsylvania</td>
<td>Cedric L. Richmond, Louisiana</td>
</tr>
<tr>
<td>Lou Barletta, Pennsylvania</td>
<td>William R. Keating, Massachusetts</td>
</tr>
<tr>
<td>Scott Perry, Pennsylvania</td>
<td>Donald M. Payne Jr., New Jersey</td>
</tr>
<tr>
<td>Curtis Clawson, Florida</td>
<td>Filemon Vela, Texas</td>
</tr>
<tr>
<td>John Katko, New York</td>
<td>Bonnie Watson Coleman, New Jersey</td>
</tr>
<tr>
<td>Will Hurd, Texas</td>
<td>Kathleen M. Rice,</td>
</tr>
<tr>
<td>Earl L. “Buddy” Carter, Georgia</td>
<td></td>
</tr>
<tr>
<td>Mark Walker, North Carolina</td>
<td></td>
</tr>
<tr>
<td>Barry Loudermilk, Georgia</td>
<td></td>
</tr>
</tbody>
</table>


Key Staff:

Majority and Non-Designated:

Majority Staff Director ........................... Brendan Shields
Executive Asst. to the Director.............Madeline Matthews
Majority Deputy Staff Director .............. Eric Heighberger
Majority General Counsel ....................... Joan O’Hara,
                                            Katy Flynn (Deputy)
Majority Sr. Professional Staff .............. Luke Burke,
                                            Alan Carroll,
                                            Jason Miller
Majority Professional Staff .................... Kate Bonvechio,
                                            Chad Carlough,
                                            Nicole Halavik,
                                            Kyle Klein,
                                            Erik Peterson,
                                            Miles Taylor

Majority Communications Director .......... Susan Phalen
Majority Deputy Press Secretary ............ Margaret Moore
Majority Senior Advisor ........................... Laura Fullerton (Strategy),
                                            James Murphy
Majority Clerk ........................................ Dennis Terry
Majority Security Director ..................... Kyle McFarland
Majority Staff Other ............................... Tina Garcia,
                                            Jason Olin,
                                            Keith Robinson
An example of the Subcommittee on Counterterrorism and Intelligence providing valuable cyber oversight is illustrated by the hearings held on the topic “Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland.”165 Membership of the House Committee on Homeland Security’s Subcommittee on Counterterrorism and Intelligence follow:166

166 United States House of Representatives, The House Committee on Homeland Security, Subcommittees: Counterterrorism and Intelligence,
Key Staff:

Majority Staff Director ...................... Mandy Bowers
Majority Professional Staff ..................... John Neal

Minority Director / Counsel .................. Nicole Tisdale
Minority Professional Staff .................... Lori Stith

B. SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND SECURITY TECHNOLOGIES

One of many examples of subcommittee oversight, during 2015, the Committee on Homeland Security’s Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies held hearings on the subject of “Emerging Threats and Technologies to Protect the

Membership of the House Committee on Homeland Security’s Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies follow:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Ratcliffe, Texas, Chairman</td>
<td>Cedric L. Richmond, Louisiana, Ranking Member</td>
</tr>
<tr>
<td>Peter King, New York</td>
<td>Loretta Sanchez, California</td>
</tr>
<tr>
<td>Tom Marino, Pennsylvania</td>
<td>Sheila Jackson Lee, Texas</td>
</tr>
<tr>
<td>Scott Perry, Pennsylvania</td>
<td>James R. Langevin, Rhode Island</td>
</tr>
<tr>
<td>Curtis Clawson, Florida</td>
<td>Bennie Thompson, Massachusetts, Ex Officio</td>
</tr>
<tr>
<td>Dan Donovan, New York</td>
<td></td>
</tr>
<tr>
<td>Michael McCaul, Texas, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

Key Staff:

- **Majority Staff Director**                      Brett DeWitt
- **Majority Professional Staff**                  Bradley Saull
- **Majority Staff Other**                        David DeCroix

---


C. SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE AND COMMUNICATIONS

An example of the Subcommittee on Emergency Preparedness, Response and Communications’ oversight role is found in their previous hearings on the topic, “Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management.” Membership of the House Committee on Homeland Security’s Subcommittee on Emergency Preparedness, Response and Communications follow:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Martha McSally, Arizona, Chair</td>
<td>Donald M. Payne Jr., New Jersey,</td>
</tr>
<tr>
<td>Tom Marino, Pennsylvania</td>
<td>Ranking Member</td>
</tr>
<tr>
<td>Mark Walker, North Carolina</td>
<td>Bonnie Watson Coleman, New Jersey</td>
</tr>
</tbody>
</table>


Journal of Law and Cyber Warfare [2016]

Barry Loudermilk, Georgia  
Dan Donovan,  
New York  
Michael McCaul, Texas, Ex Officio  
Kathleen M. Rice,  
New York  
Bennie Thompson,  
Massachusetts,  
Ex Officio

**Key Staff:**

*Majority Staff Director* ....................... Kerry Kenirons  
*Majority Professional Staff* ............... Kate Bonvechio,  
................................................................. Natalie Matson

*Minority Staff Director* .......................... Moira Bergin  
*Minority Professional Staff* ................. Ashley Delgado

**D. SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY**

One of many examples of subcommittee oversight, during 2013, the Committee on Homeland Security’s Subcommittee on Oversight and Management Efficiency held hearings on the topic of DHS Information Technology: How Effectively Has DHS Harnessed IT to Secure Our Borders and Uphold Immigration Laws?″

Membership of the House Committee on Homeland Security’s Subcommittee on Oversight and Management Efficiency follow:

---


172 United States House of Representatives, The House Committee on
Key Staff

Majority Staff Director ....................... Ryan Consaul
Maj. Sr. Professional Staff .................... Luke Burke
Majority Professional Staff ..................... Diana Bergwin
Majority Staff Other ............................ Emily Gunn
Minority Professional Staff .................... Deborah Mack

XVII. House Judiciary Committee

The Committee on the Judiciary was created on June 3, 1813 as a standing committee “to consider legislation relating to judicial proceedings.” Since then, the scope of the Committee’s jurisdiction has encompassed


a wide range of subjects – “Particularly important in our time is the Committee’s oversight responsibility for the Departments of Justice and Homeland Security.” Committee membership has customarily consisted of those having a background in the law, given the legal focus of the committee’s work. Because of rapid scientific progress and technological change, “an expanding list of issues, including intellectual property, cloning, and the internet, require committee members to possess a wide breadth of knowledge in order to effectively address concerns from these and other new areas.” Membership of the House Judiciary Committee for the 114th Congress follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob Goodlatte, Virginia, Chairman</td>
<td>John Conyers, Michigan, Ranking Member</td>
</tr>
<tr>
<td>Jim Sensenbrenner, Wisconsin</td>
<td>Jerry Nadler, New York</td>
</tr>
<tr>
<td>Lamar Smith, Texas</td>
<td>Zoe Lofgren, California</td>
</tr>
<tr>
<td>Steve Chabot, Ohio</td>
<td>Shelia Jackson Lee, Texas</td>
</tr>
<tr>
<td>Darrell Issa, California</td>
<td>Steve Cohen, Tennessee</td>
</tr>
<tr>
<td>Randy Forbes, Virginia</td>
<td>Hank Johnson, Georgia</td>
</tr>
<tr>
<td>Steve King, Iowa</td>
<td>Pedro Pierluisi, Puerto Rico</td>
</tr>
<tr>
<td>Trent Franks, Arizona</td>
<td>Judy Chu, California</td>
</tr>
<tr>
<td>Louie Gohmert, Texas</td>
<td>Ted Deutch, Florida</td>
</tr>
<tr>
<td>Jim Jordan, Ohio</td>
<td>Luis Gutierrez, Illinois</td>
</tr>
<tr>
<td>Ted Poe, Texas</td>
<td></td>
</tr>
</tbody>
</table>

174 Id.
175 Id.
<table>
<thead>
<tr>
<th>Jason Chaffetz, Utah</th>
<th>Karen Bass, California</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Marino, Pennsylvania</td>
<td>Cedric Richmond, Louisiana</td>
</tr>
<tr>
<td>Trey Gowdy, South Carolina</td>
<td>Suzan DelBene, Washington</td>
</tr>
<tr>
<td>Raul Labrador, Idaho</td>
<td>Hakeem Jeffries, New York</td>
</tr>
<tr>
<td>Blake Farenthold, Texas</td>
<td>David Cicilline, Rhode Island</td>
</tr>
<tr>
<td>Doug Collins, Georgia</td>
<td>Scott Peters, California</td>
</tr>
<tr>
<td>Ron DeSantis, Florida</td>
<td></td>
</tr>
<tr>
<td>Mimi Walters, California</td>
<td></td>
</tr>
<tr>
<td>Ken Buck, Colorado</td>
<td></td>
</tr>
<tr>
<td>John Ratcliffe, Texas</td>
<td></td>
</tr>
<tr>
<td>Dave Trott, Michigan</td>
<td></td>
</tr>
<tr>
<td>Mike Bishop, Michigan</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

**Majority and Non-Designated:**

**Chief of Staff and General Counsel** .................................................. Shelley Husband

**Deputy Chief of Staff and Chief Counsel** ........................................... Branden Ritchie

**General Counsel and Parliamentarian** ............................................... Allison Halataei

**Senior Counsel** .................................................................................. Jason Cervenak

**Counsel** ................................................................................................. Stephanie Gadbois

**Professional Staff** ............................................................................... John Manning

**Communications Director** ................................................................. Kathryn Rexrode

**Deputy Communications Director** ....................................................... Jessica Collins

**Public Affairs** ....................................................................................... Bryan Alphin

**Other Staff** ............................................................................................ Doug Alexander,

Patrick Baugh,

Allen Jamerson,

Tim Pearson,

Joe Russo,

Tom Ullrich,
Membership on the House Committee on the Judiciary’s Subcommittee on Courts, Intellectual Property and the Internet is as follows:

A. SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY AND THE INTERNET
<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Darrell Issa, California, Chairman</td>
<td>Jerry Nadler, New York, Ranking Member</td>
</tr>
<tr>
<td>Doug Collins, Georgia, Vice Chairman</td>
<td>Judy Chu, California</td>
</tr>
<tr>
<td>Jim Sensenbrenner, Wisconsin</td>
<td>Ted Deutch, Florida</td>
</tr>
<tr>
<td>Lamar Smith, Texas</td>
<td>Karen Bass, California</td>
</tr>
<tr>
<td>Steve Chabot, Ohio</td>
<td>Cedric Richmond, Louisiana</td>
</tr>
<tr>
<td>Randy Forbes, Virginia</td>
<td>Suzan DelBene, Washington</td>
</tr>
<tr>
<td>Trent Franks, Arizona</td>
<td>Hakeem Jeffries, New York</td>
</tr>
<tr>
<td>Jim Jordan, Ohio</td>
<td>David Cicilline, Rhode Island</td>
</tr>
<tr>
<td>Ted Poe, Texas</td>
<td>Scott Peters, California</td>
</tr>
<tr>
<td>Jason Chaffetz, Utah</td>
<td>Zoe Lofgren, California</td>
</tr>
<tr>
<td>Tom Marino, Pennsylvania</td>
<td>Steve Cohen, Tennessee</td>
</tr>
<tr>
<td>Blake Farenthold, Texas</td>
<td>Hank Johnson, Georgia</td>
</tr>
<tr>
<td>Ron DeSantis, Florida</td>
<td>John Conyers, Michigan, Ex Officio</td>
</tr>
<tr>
<td>Mimi Walters, California</td>
<td></td>
</tr>
<tr>
<td>Bob Goodlatte, Virginia, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

*Majority Chief Counsel*.................................Joe Keeley

*Senior Counsel*...........................................Vishal Amin

*Counsel*..................................................David Whitney

*Minority Chief Counsel*.................................Jason Everett

*Counsel*..................................................Norberto Salinas
B. SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

Membership on the House Committee on the Judiciary’s Subcommittee on Crime, Terrorism, Homeland Security, and Investigations consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jim Sensenbrenner, Wisconsin, Chairman</td>
<td>Shelia Jackson Lee, Texas,</td>
</tr>
<tr>
<td>Louie Gohmert, Texas</td>
<td>Ranking Member</td>
</tr>
<tr>
<td>Steve Chabot, Ohio</td>
<td>Pedro Pierluisi, Puerto Rico</td>
</tr>
<tr>
<td>Randy Forbes, Virginia</td>
<td>Judy Chu, California</td>
</tr>
<tr>
<td>Ted Poe, Texas</td>
<td>Luis Gutierrez, Illinois</td>
</tr>
<tr>
<td>Jason Chaffetz, Utah</td>
<td>Karen Bass, California</td>
</tr>
<tr>
<td>Trey Gowdy, South Carolina</td>
<td>Cedric Richmond, Louisiana</td>
</tr>
<tr>
<td>Raul Labrador, Idaho</td>
<td>John Conyers, Michigan, Ex Officio</td>
</tr>
<tr>
<td>Ken Buck, Colorado</td>
<td></td>
</tr>
<tr>
<td>Mike Bishop, Michigan</td>
<td></td>
</tr>
<tr>
<td>Bob Goodlatte, Virginia, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

Key Staff:

Majority Chief Counsel..................................Caroline Lynch
Counsel ..................................................................Sarah Allen,
.................................................................................Robert Parmiter
Clerk..................................................................Alicia Church

Minority Chief Counsel..........................Joe Graupensperger
Other .................................................................Vanessa Chen,
                                                Kurt May
During the 114th Congress this committee will be under the chairmanship of Rep. Jason Chaffetz (R-Utah). Of the Committee’s six subcommittees, three have jurisdiction over issues impacted by cybersecurity (in alphabetical order): the Subcommittee on Governmental Operations; Information Technology; and National Security. Some outside the government have characterized Rep. Chaffetz as “very tech-savvy and tech-friendly. We expect the committee will conduct oversight on government IT infrastructure and procurement and cyber-security. A key indication of this is the announcement that the committee is creating a new subcommittee to deal with these specific issues.”

Membership of the House Committee on Oversight and Government Reform for the 114th Congress follows:

---


### MAJORITY (Republican)

Jason Chaffetz, Utah, Chairman  
John Mica, Florida  
Michael Turner, Ohio  
John Duncan, Tennessee  
Jim Jordan, Ohio  
Tim Walberg, Michigan  
Justin Amash, Michigan  
Paul Gosar, Arizona  
Scott DesJarlais, Tennessee  
Trey Gowdy, South Carolina  
Blake Farenthold, Texas  
Cynthia Lummis, Wyoming  
Thomas Massie, Kentucky  
Mark Meadows, North Carolina  
Ron DeSantis, Florida  
Mick Mulvaney, South Carolina  
Ken Buck, Colorado  
Mark Walker, North Carolina  
Rod Blum, Iowa  
Jody Hice, Georgia  
Steve Russell, Oklahoma  
Buddy Carter, Georgia  
Glenn Grothman, Wisconsin  
William Hurd, Texas  
Gary J. Palmer, Alabama

### MINORITY (Democratic)

Elijah Cummings, Maryland, Ranking Member  
Carolyn Maloney, New York  
Eleanor Holmes Norton, District of Columbia  
William Lacy Clay, Missouri  
Stephen Lynch, Massachusetts  
Jim Cooper, Tennessee  
Gerald E. Connolly, Virginia  
Matt Cartwright, Pennsylvania  
Tammy Duckworth, Illinois  
Robin Kelly, Illinois  
Brenda Lawrence, Michigan  
Ted Lieu, California  
Bonnie Watson, New Jersey  
Stacey E. Plaskett, Virgin Islands  
Mark DeSaulnier, California  
Brendan F. Boyle, Pennsylvania  
Peter Welch, Vermont  
Michelle Lujan Grisham, New Mexico

**Key Staff:**
Majority and Non-Designated:

Majority Staff Director ......................... Sean McLaughlin

Executive Asst. to Majority Staff

Director ................................................. Olivia Lee
Deputy Staff Director ................................. Rachel Weaver
Majority General Counsel ....................... Andy Dockham
Deputy General Counsel ............................. Steve Castor

Director, Oversight &
Investigations ........................................ Machalagh Carr
Deputy Director, Oversight &
Investigations ........................................ Henry Kerner
Counsel ...................................................... Jennifer Barblan,
                                            Mike Howell,
                                            Cordell Hull,
                                            Tristan Leavitt

Senior Military Professional

Staff ......................................................... Ryan Hambleton,
                                           Tyler Grimm,
                                           Ari Wisch

Minority Staff:

Minority Staff Director ............................... David Rapallo
Chief Investigative Counsel ......................... Meghan Berroya
Policy Director ........................................ Lucinda Lessley
Policy Advisor ......................................... Jimmy Fremgen
Counsel ...................................................... Portia Bamiduro,
                                            Beverly Britton-Fraser,
                                            Lena Chang,
                                            Courtney French,
                                            Tim Lynch,
                                            Brian Quinn,
                                            Valerie Shen,
A. SUBCOMMITTEE ON GOVERNMENT OPERATIONS

Chaired during the 114th Congress by Rep. Mark Meadows (R-N.C.), the Subcommittee on Government Operations has primary jurisdiction over federal property, data standards, and federal information technology and “oversees the efficiency and management of government operations and activities, working to ensure public access to information through its oversight of the Freedom of Information Act, the Federal Advisory Committee Act, the Presidential Records Act, and the National Archives and Records Administration.” Membership of the House Committee on Oversight and Government Reform’s Subcommittee on Government Operations follow:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark Meadows, North Carolina, Chairman</td>
<td>Gerald E. Connolly, Virginia, Ranking Member</td>
</tr>
<tr>
<td>Jim Jordan, Ohio</td>
<td>Carolyn Maloney, New York</td>
</tr>
<tr>
<td>Tim Walberg, Michigan</td>
<td></td>
</tr>
</tbody>
</table>


181 Id.
Trey Gowdy, South Carolina  
Thomas Massie, Kentucky  
Mick Mulvaney, South Carolina  
Ken Buck, Colorado  
Buddy Carter, Georgia  
Glenn Grothman, Wisconsin  
Jason Chaffetz, Utah, Ex Officio  

Eleanor Holmes Norton, District of Columbia  
William Lacy Clay, Missouri  
Stacey E. Plaskett, Virgin Islands  
Stephen Lynch, Massachusetts  
Elijah Cummings, Maryland, Ex Officio

Key Staff:  
Majority Staff Director .................. Jennifer Hemingway  
Deputy Majority Staff Director .................. Jeff Post  
Senior Counsel .................. Julie Dunne  
Counsel .................. Howard Denis, Katy Rother  
Professional Staff .................. Alexa Armstrong, Christopher D’Angelo  

Minority Staff Counsel .................. Lena Chang

B. SUBCOMMITTEE ON INFORMATION TECHNOLOGY

Rep. Will Hurd (R-Texas) will serve as chair of the Subcommittee on Information Technology during the 114th Congress. The Information Technology Subcommittee “will focus on federal IT procurement... cybersecurity, IT infrastructure, emerging technologies, and intellectual
property, among other issues.” Membership of the House Committee on Oversight and Government Reform’s Subcommittee on Information Technology follow:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>William Hurd, Texas, Chairman</td>
<td>Robin Kelly, Illinois, Ranking Member</td>
</tr>
<tr>
<td>Blake Farenthold, Texas</td>
<td>Gerald E. Connolly, Virginia</td>
</tr>
<tr>
<td>Mark Walker, North Carolina</td>
<td>Tammy Duckworth, Illinois</td>
</tr>
<tr>
<td>Rod Blum, Iowa</td>
<td>Ted Lieu, California</td>
</tr>
<tr>
<td>Paul Gosar, Arizona</td>
<td>Elijah Cummings, Maryland, Ex Officio</td>
</tr>
<tr>
<td>Jason Chaffetz, Utah, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

Key Staff:

* Majority Staff Director .......................... Troy Stock
  * Majority Counsel ................................. Mike Flynn

  * Minority Counsel ............................... Brian Quinn

C. SUBCOMMITTEE ON NATIONAL SECURITY

Rep. Ron De Santis (R-Florida) will serve as chair of the Subcommittee on National Security during the 114th Congress. This Subcommittee “is primarily responsible for overseeing the Departments of State, Defense and Homeland Security, and the United States Agency for

---

182 Chaffetz Press Release, supra note 177.
During the 114th Congress, the Subcommittee will also focus on areas related to the “VA, DOJ, and the intelligence community.” To discharge these duties, the Subcommittee “holds hearings and conducts investigations of policies, personnel and procedures within these executive entities… [and] has legislative jurisdiction over drug policy, and oversees the policies of the Office of National Drug Control Policy (ONDCP).” Membership of the House Committee on Oversight and Government Reform’s Subcommittee on National Security consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ron DeSantis, Florida,</td>
<td>Stephen Lynch, Massachusetts,</td>
</tr>
<tr>
<td>Chairman</td>
<td>Ranking Member</td>
</tr>
<tr>
<td>John Mica, Florida</td>
<td>Ted Lieu, California</td>
</tr>
<tr>
<td>John Duncan, Tennessee</td>
<td>Robin Kelly, Illinois</td>
</tr>
<tr>
<td>Jody Hice, Georgia</td>
<td>Brenda Lawrence, Michigan</td>
</tr>
<tr>
<td>Steve Russell, Oklahoma</td>
<td>Elijah Cummings, Maryland</td>
</tr>
<tr>
<td>William Hurd, Texas</td>
<td></td>
</tr>
</tbody>
</table>

187 Id.
The U.S. House Permanent Select Committee on Intelligence (HPSCI) “is charged with the oversight of the United States Intelligence Community, which includes the intelligence and intelligence related activities of 17 elements of the U.S. Government, and the Military Intelligence Programs.”188 The HPSCI has four subcommittees for the 114th Congress: the CIA Subcommittee; Department of Defense Intelligence and Overhead Architecture Subcommittee; Emerging Threats Subcommittee; and NSA and Cybersecurity Subcommittee.189 During early 2015, favorably reported the Protecting Cyber Networks Act (H.R. 1560) to the full House of Representatives.190 Membership of the House

---


190 Press Release, U.S. House of Representatives, The Permanent Select Committee on Intelligence, HPSCI Passes Cyber Bill Out of
Permanent Select Committee on Intelligence for the 114th Congress is as follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devin Nunes, California, Chairman</td>
<td>Adam Schiff, California, Ranking Member</td>
</tr>
<tr>
<td>Jeff Miller, Florida,</td>
<td>Luis Gutierrez, Illinois</td>
</tr>
<tr>
<td>Mike Conaway, Texas</td>
<td>Jim Himes, Connecticut</td>
</tr>
<tr>
<td>Peter King, New York</td>
<td>Terri Sewell, Alabama</td>
</tr>
<tr>
<td>Frank LoBiondo, New Jersey</td>
<td>Andre Carson, Indiana</td>
</tr>
<tr>
<td>Lynn Westmoreland, Georgia</td>
<td>Jackie Speier, California</td>
</tr>
<tr>
<td>Tom Rooney, Florida</td>
<td>Mike Quigley, Illinois</td>
</tr>
<tr>
<td>Joe Heck, Nevada</td>
<td>Eric Swalwell, California</td>
</tr>
<tr>
<td>Mike Pompeo, Kansas</td>
<td>Patrick Murphy, Florida</td>
</tr>
<tr>
<td>Ileana Ros-Lehtinen, Florida</td>
<td></td>
</tr>
<tr>
<td>Michael Turner, Ohio</td>
<td></td>
</tr>
<tr>
<td>Brad Wenstrup, Ohio</td>
<td></td>
</tr>
<tr>
<td>Chris Stewart, Utah</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

*Majority Staff Director* ......................... Jeff Shockey

*Majority Deputy Staff Director* ............ Jennifer Miller

*Majority Senior Counsel & Policy Director* ........................................... Michael Ellis

*Majority Senior Counsel* .................... Andrew Peterson

*Majority Senior Advisor* .................... Damon Nelson

*Professional Staff* ......................... Chelsey Campbell, Geoffrey Kahn,

A. CIA SUBCOMMITTEE

Membership of the HPSCI CIA Subcommittee.191

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frank LoBiondo, New Jersey, Chairman</td>
<td>Eric Swalwell, California, Ranking Membr</td>
</tr>
<tr>
<td>Mike Conaway, Texas</td>
<td>Luis Gutierrez, Illinois</td>
</tr>
<tr>
<td>Peter King, New York</td>
<td>Jim Himes, Connecticut</td>
</tr>
<tr>
<td>Lynn Westmoreland,</td>
<td>Andre Carson, Indiana</td>
</tr>
</tbody>
</table>

Key Staff:

Majority Staff: ......................... Jack Langer (Nunes)
Minority Staff: ......................... Patrick Boland (Schiff)

B. DEPARTMENT OF DEFENSE INTELLIGENCE AND OVERHEAD ARCHITECTURE SUBCOMMITTEE

Membership of the HPSCI Department of Defense Intelligence and Overhead Architecture Subcommittee consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe Heck, Nevada, Chairman</td>
<td>Terri Sewell, Alabama, Ranking Member</td>
</tr>
<tr>
<td>Jeff Miller, Florida</td>
<td>Luis Gutierrez, Illinois</td>
</tr>
<tr>
<td>Ileana Ros-Lehtinen, Florida</td>
<td>Eric Swalwell, California</td>
</tr>
<tr>
<td>Michael Turner, Ohio</td>
<td>Patrick Murphy, Florida</td>
</tr>
<tr>
<td>Brad Wenstrup, Ohio</td>
<td>Adam Schiff, California, Ex Officio</td>
</tr>
<tr>
<td>Chris Stewart, Utah</td>
<td>Devin Nunes, California, Ex Officio</td>
</tr>
</tbody>
</table>

---

*Key Staff:*

**Majority Staff:**......................... Jack Langer (Nunes)

**Minority Staff:**......................... Patrick Boland (Schiff)

### C. EMERGING THREATS SUBCOMMITTEE

Membership of the HPSCI Emerging Threats Subcommittee is as follows:193

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Rooney, Florida, Chairman</td>
<td>Mike Quigley, Illinois, Ranking Member</td>
</tr>
<tr>
<td>Frank LoBiondo, New Jersey</td>
<td>Terri Sewell, Alabama</td>
</tr>
<tr>
<td>Joe Heck, Nevada</td>
<td>Andre Carson, Indiana</td>
</tr>
<tr>
<td>Michael Turner, Ohio</td>
<td>Jackie Speier, California</td>
</tr>
<tr>
<td>Brad Wenstrup, Ohio</td>
<td>Adam Schiff, California, Ex Officio</td>
</tr>
<tr>
<td>Chris Stewart, Utah</td>
<td>Devin Nunes, California, Ex Officio</td>
</tr>
</tbody>
</table>

*Key Staff:*

**Majority Staff:**......................... Jack Langer (Nunes)

**Minority Staff:**......................... Patrick Boland (Schiff)

### D. NSA AND CYBERSECURITY SUBCOMMITTEE

Membership of the HPSCI NSA and Cybersecurity Subcommittee consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lynn Westmoreland, Georgia, Chairman</td>
<td>Jim Himes, Connecticut, Ranking Member</td>
</tr>
<tr>
<td>Jeff Miller, Florida, Mike Conaway, Texas</td>
<td>Jackie Speier, California</td>
</tr>
<tr>
<td>Peter King, New York Mike Pompeo, Kansas</td>
<td>Mike Quigley, Illinois</td>
</tr>
<tr>
<td>Ileana Ros-Lehtinen, Florida Devin Nunes, California, Ex Officio</td>
<td>Patrick Murphy, Florida Adam Schiff, California, Ex Officio</td>
</tr>
</tbody>
</table>

**Key Staff:**

*Majority Staff*................................. Jack Langer (Nunes)

*Minority Staff*................................. Patrick Boland (Schiff)

**XX. House Committee on Science, Space, and Technology**

With respect to cybersecurity, jurisdiction of the House Committee on Science, Space, and Technology covers “all energy research[;]… all federally owned or operated non-military energy laboratories; National Institute of Standards and Technology; National Science Foundation… science scholarships; scientific research, develop-ment, and demonstration, and projects therefor;
shall review and study on a continuing basis laws, programs, and Government activities relating to non-military research and development.”

While the Committee has five subcommittees, primary focus here will be on: the Subcommittee on Oversight; and Subcommittee on Research and Technology. Membership of the House Committee on Science, Space, and Technology for the 114th Congress consists of:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lamar Smith, Texas, Chairman</td>
<td>Eddie Bernice Johnson, Texas, Ranking</td>
</tr>
<tr>
<td>F. James Sensenbrenner, Wisconsin, Chair Emeritus</td>
<td>Member</td>
</tr>
<tr>
<td>Dana Rohrabacher, California</td>
<td>Zoe Lofgren, California</td>
</tr>
<tr>
<td>Frank D. Lucas, Oklahoma, Vice Chair</td>
<td>Daniel Lipinski, Illinois</td>
</tr>
<tr>
<td>Randy Neugebauer, Texas</td>
<td>Donna Edwards, Maryland</td>
</tr>
<tr>
<td>Michael T. McCaul, Texas</td>
<td>Suzanne Bonamici, Oregon</td>
</tr>
<tr>
<td>Mo Brooks, Alabama</td>
<td>Eric Swalwell, California</td>
</tr>
<tr>
<td>Randy Hultgren, Illinois</td>
<td>Alan Grayson, Florida</td>
</tr>
<tr>
<td>Bill Posey, Florida</td>
<td>Ami Bera, California</td>
</tr>
<tr>
<td>Thomas Massie, Kentucky</td>
<td>Elizabeth Esty, Connecticut</td>
</tr>
<tr>
<td>Jim Bridenstine, Oklahoma</td>
<td>Marc Veasey, Texas</td>
</tr>
<tr>
<td>Randy Weber, Texas</td>
<td>Katherine Clark, Massachusetts</td>
</tr>
<tr>
<td></td>
<td>Don Beyer, Virginia</td>
</tr>
<tr>
<td></td>
<td>Ed Perlmutter, Colorado</td>
</tr>
<tr>
<td></td>
<td>Paul Tonko, New York</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bill Johnson, Ohio</th>
<th>Mark Takano, California</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Moolenaar, Michigan</td>
<td>Bill Foster, Illinois</td>
</tr>
<tr>
<td>Steve Knight, California</td>
<td></td>
</tr>
<tr>
<td>Brian Babin, Texas</td>
<td></td>
</tr>
<tr>
<td>Bruce Westerman, Arkansas</td>
<td></td>
</tr>
<tr>
<td>Barbara Comstock, Virginia</td>
<td></td>
</tr>
<tr>
<td>Dan Newhouse, Washington</td>
<td></td>
</tr>
<tr>
<td>Gary Palmer, Alabama</td>
<td></td>
</tr>
<tr>
<td>Barry Loudermilk, Georgia</td>
<td></td>
</tr>
<tr>
<td>Ralph Lee Abrahams,</td>
<td></td>
</tr>
<tr>
<td>Louisiana</td>
<td></td>
</tr>
</tbody>
</table>

**Key Staff:**

**Majority and Non-Designated:**

- **Majority Chief of Staff** ................................ Jennifer Brown
- **Policy Director, Coalitions Director** ................. Chris Shank
- **Policy Assistant** ........................................... Brian Corcoran
- **Legislative Director** ................................. Christopher Wydler
- **General Counsel & Parliamentarian** ................. Molly Boyl
- **Communications Director** .................... Zachary Kurz
- **Press Secretary** ........................................... Laura Crist
- **Speechwriter & Legal Assistant** .................. James Danford
- **Executive Assistant** .................................... Thea McDonald

**Minority Staff:**

- **Minority Staff Director** ....................... Richard Obermann
- **Chief Counsel** .................................................. John Piazza
- **Deputy Chief Counsel** .............................. Russell Norman
- **Admin. & Communications** ...................... Kristin Kopshever
- **Press Secretary & Policy** ...................... Joe Flarida

**A. SUBCOMMITTEE ON OVERSIGHT**

The House Committee on Science, Space, and Technology’s Subcommittee on Oversight is granted
“general and special investigative authority on all matters within the jurisdiction of the Committee on Science, Space and Technology.”¹⁹⁷ Membership of the House Committee on Science, Space, and Technology Committee’s Subcommittee on Oversight is as follows:¹⁹⁸

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barry Loudermilk, Georgia, Chairman</td>
<td>Don Beyer, Virginia, Ranking Member</td>
</tr>
<tr>
<td>Bill Johnson, Ohio, Vice Chairman</td>
<td>Alan Grayson, Florida</td>
</tr>
<tr>
<td>F. James Sensenbrenner, Wisconsin</td>
<td>Zoe Lofgren, California</td>
</tr>
<tr>
<td>Bill Posey, Florida</td>
<td>Eddie Bernice</td>
</tr>
<tr>
<td>Thomas Massie, Kentucky</td>
<td>Johnson, Texas, Ex Officio</td>
</tr>
<tr>
<td>Jim Bridenstine, Oklahoma</td>
<td>Lamar Smith, Texas, Ex Officio</td>
</tr>
</tbody>
</table>

**Key Staff:**

*Majority Staff Director* ................................. Tim Doyle  
*Policy Assistant* .......................... Brian Corcoran  
*Counsel* ............................... Lamar Echols  
*Professional Staff* ............................... Drew Colliatie  

*Minority Staff Director* ............................... Pearson  
*Chief Investigator* ............................... Doug Pasternak

B. SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

Jurisdiction, investigative authority and general oversight of the Subcommittee on Research and Technology includes

[L]egislative jurisdiction and general oversight and investigative authority on all matters relating to science policy and science education; the Office of Science and Technology Policy; all scientific research, and scientific and engineering resources (including human resources); all matters relating to science, technology, engineering and mathematics education; intergovernmental mechanisms for research, development, and demonstration and cross-cutting programs; international scientific cooperation; National Science Foundation, university research policy, including infrastructure and overhead; university research partnerships, including those with industry; science scholarships; computing, communications, networking, and information technology; research and development relating to health, biomedical, and nutritional programs; research, development, and demonstration relating to nano-science, nano-engineering, and nanotechnology; agricultural, geological, biological and life sciences research; materials research, development,
demonstration, and policy; all matters relating to competitiveness, technology, standards, and innovation; standardization of weights and measures, including technical standards, standardization, and conformity assessment; measurement, including the metric system of measurement; the Technology Administration of the Department of Commerce; the National Institute of Standards and Technology; the National Technical Information Service; competitiveness, including small business competitiveness; tax, antitrust, regulatory and other legal and governmental policies related to technological development and commercialization; technology transfer, including civilian use of defense technologies; patent and intellectual property policy; international technology trade; research, development, and demonstration activities of the Department of Transportation; surface and water transportation research, development, and demonstration programs; earthquake programs and fire research programs, including those related to wildfire proliferation research and prevention; biotechnology policy; research, development, demonstration, and standards-related activities of the Department of Homeland Security; Small Business Innovation Research and Technology Transfer; voting technologies and standards; other appropriate matters as referred by the
CONGRESSIONAL CYBERSECURITY . . . [2016]

Chairman; and relevant over-sight.”

Membership of the House Committee on Science, Space, and Technology Committee’s Subcommittee on Research and Technology is as follows:

<table>
<thead>
<tr>
<th>MAJORITY (Republican)</th>
<th>MINORITY (Democratic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barbara Comstock, Virginia, Chair</td>
<td>Daniel Lipinski, Illinois, Ranking Member</td>
</tr>
<tr>
<td>John Moolenaar, Michigan</td>
<td>Elizabeth Esty, Connecticut</td>
</tr>
<tr>
<td>Frank D. Lucas, Oklahoma</td>
<td>Katherine Clark, Massachusetts</td>
</tr>
<tr>
<td>Michael T. McCaul, Texas</td>
<td>Paul Tonko, New York</td>
</tr>
<tr>
<td>Randy Hultgren, Illinois</td>
<td>Suzanne Bonamici, Oregon</td>
</tr>
<tr>
<td>Bruce Westerman, Arkansas</td>
<td>Eric Swalwell, California</td>
</tr>
<tr>
<td>Dan Newhouse, Washington</td>
<td>Eddie Bernice</td>
</tr>
<tr>
<td>Gary Palmer, Alabama</td>
<td>Johnson, Texas, Ex Officio</td>
</tr>
<tr>
<td>Ralph Lee Abraham, Louisiana</td>
<td></td>
</tr>
<tr>
<td>Lamar Smith, Texas, Ex Officio</td>
<td></td>
</tr>
</tbody>
</table>

Key Staff:

- Majority Staff Director .................. Cliff Shannon
- Deputy Majority Staff Director ............ Raj Bharwani
- Policy Assistant ............................ Christian Rice
- Professional Staff ........................... Sarah Grady,

......................................................... Jennifer Wickre

---


200 Id.
XXI. Role of Leadership

A comprehensive discussion of the leadership mechanisms and power structure of the House and Senate is beyond the scope of this paper. However, a brief overview is presented. Frank Cummings writes, “In theory, the only ‘laws’ governing the Congress are the Constitution, Statutes such as the Legislative Reorganization Act, and the rules of each chamber. But in practice, voting blocks have been developed, with varying degrees of formality and voting discipline.” Historically, the party caucuses have been perhaps the strongest of these blocks, and the party holding majority membership in each body exerts the most power. Cummings observes that “the caucus system tends to block cross-party coalitions which might constitute an absolute majority of the House but for the exercise of voting discipline by the caucus… this sort of discipline… seems to work almost absolutely on the election of committee chairmen.”

---

202 FRANK CUMMINGS, CAPITOL HILL MANUAL 79 (2nd ed. 1984).
203 Id. at 80.
A. THE HOUSE

Leadership positions in the House provide a schematic for how the House organizes itself and conducts its business. The top leadership positions of each party are described below. In terms of influence and potential ability to move legislation through Congress, the majority party will generally have the most influence. Below the top party leadership, committee chairmen, subcommittee chairmen and ranking minority members of both full committees and subcommittees provide and constitute leadership. As of this writing, the Republican Party is the majority party in both the House and Senate.

B. HOUSE MAJORITY (CURRENTLY REPUBLICAN) LEADERSHIP

Majority elected leadership positions in the House of Representatives consists of: the Speaker of the House; House Majority Leader; House Majority Whip; Chair of the House Republican Conference; Chair of the National Republican Congressional Committee; Chair of the House Republican Policy Committee; Vice-Chair, and Secretary of the Republican Conference. Designated Republican Leaders include: the Chair of the House Committees on Rules; Ways and Means; Appropriations; Budget; Energy

---


and Commerce; the Chief Deputy Whip; and, one member each from the sophomore and freshman class, elected by members of their respective classes. The House Republican Steering Committee is a subdivision of the House Republican Conference. Under post 1994 rules, the House party leader receives five votes on the committee.

Speaker of the House

John Boehner

Key Staff:

Chief of Staff .............................................. Mike Sommers
Special Assistant ............................... Thomas Andrews
Director of Communications .................. Kevin Smith
Deputy Director of Communications ........ Mike Ricci
Assistant Communications Director ........ Katie Boyd
Press Secretary ........................................... Cory Fritz
Assistant Press Secretary ..................... Heather Reed
Communications Advisor ...................... Matt Wolking
Director of Public Liaison ................. Maria Lohmeyer
Policy Director ......................................... Dave Stewart
General Counsel/ Legislation .......... Jo-Marie St. Martin
Assistant General Counsel ................. Greg Robinson
Assistant for Policy ............................... Maryam Brown,

---


283 CONGRESSIONAL CYBERSECURITY . . . [2016]

Natasha Hammond,  
Becky Tallent,  
Policy Advisor ......................................Cindy Herrie,  
Jennifer Stewart  
Research Assistant ..................................Justin Lampert

House Majority Leader  
House Majority Leader ....................Kevin McCarthy

Key Staff:  
Chief of Staff ........................................... Tim Berry  
Deputy Chief of Staff .................................. James Min  
Deputy Chief of Staff (Policy) ...................... Elizabeth Karr  
Director of Communications ..........................Mike Long  
Press Secretary ......................................... Matt Sparks  
Speechwriter ............................................. Alec Torres  
Director of External Affairs .......................... Danielle Burr  
Executive Assistant ................................. Kristin Stipicevic  
Director of Legislative Operations ...............Kelly Dixon  
Director of Oversight ............................... Rob Borden  
Senior policy Advisor ............................... Jeff Dressler,  
Roger Mahan,  
Wes McClelland,  
Other ......................................................... Chris Bien,  
Alexandra Gourdikian,  
Lawson Kluttz

House Majority Whip  
House Majority Whip ................................. Stephen Scalise  
Chief Deputy Majority Whip .......................Patrick McHenry

Key Staff:  
Chief of Staff ...........................................Lynnel Ruckert  
Assistant to the Chief of Staff .................... Christopher Bond  
Deputy Communications Director ............ Thomas Tatum
Policy Director................................. William Hughes
Policy Advisor............................... Daniel Sadlosky
Legislative Counsel......................... Martin Reiser
Dir. of Member Services/Policy........... Eric Zulkosky
Other ........................................... Connor Brace, Brenden DeLuke
Chief of Staff (Deputy McHenry)......... Parker Poling
Special Assistant ............................ Tanner Black

House Republican Conference
Chairwoman................................. Cathy McMorris Rodgers
Vice Chair ..................................... Lynn Jenkins
Secretary ...................................... Virginia Foxx

Key Staff:
Chief of Staff ............................... Jeremy Deutsch
Deputy Chief of Staff ....................... Nathan Hodson
Policy Director .............................. Evan McMullin
Policy Coordinator ......................... David Smentek
Senior Advisors ............................ Nicolas Magallanes, Rebecca Mark
Communications Director ................ Riva Litman
Deputy Communications Director ..... Pam Stevens

House Republican Policy Committee
Chairman ..................................... Allen Lucas Messer

House Leadership
Speaker ........................................... John Boehner
Majority Leader .............................. Kevin McCarthy
Majority Whip ............................... Steve Scalise
Conference Chair ......................... Cathy McMorris Rodgers
NRCC Chair .................................. Greg Walden
Conference Vice Chair .................... Lynn Jenkins
Conference Secretary.......................... Virginia Foxx
Chief Deputy Whip............................. Patrick McHenry

Committee Chairs
Pete Sessions, Chair, Rules
Paul Ryan, Chair, Ways and Means
Hal Rogers, Chair, Appropriations
Tom Price, Chair, Budget
Fred Upton, Chair, Energy and Commerce

Class Leadership
Ann Wagner,
Sophomore Class leadership representative
Mimi Walters,
Freshman Class leadership representative

Regional Representatives
Cresent Hardy, Region 1
TBD, Region 2
Mike Bost, Region 3
Reid Ribble, Region 4
Keith Rothfus, Region 5
John Katko, Region 6
Rick Crawford, Region 7
Gary Palmer, Region 8
Mark Walker, Region 9
Steve Knight, Region 10
Gus Bilirakis, Region 11
Bruce Poliquin, Small State Region
Blake Farenthold, Texas Region.

Class Leadership Representatives
Elise Stefanik, Freshman class
Markwayne Mullin, Sophomore class
Brad Wenstrup, Sophomore class
Committee Appointments
Jeff Denham, Agriculture
Chris Stewart, Appropriations
Austin Scott, Armed Services
Rob Woodall, Budget
Rick Allen, Education and the Workforce
Richard Hudson, Energy and Commerce
Susan Brooks, Ethics
Andy Barr, Financial Services
Joe Wilson, Foreign Affairs
Steven Palazzo, Homeland Security
Rodney Davis, House Administration
Jim Jordan, Judiciary
Paul Gosar, Natural Resources
Mark Meadows, Oversight and Government Reform
Doug Collins, Rules
Randy Hultgren, Science, Space, and Technology
Steve King, Small Business
Don Young, Transportation and Infrastructure
Jackie Walorski, Veterans’ Affairs
Tom Reed, Ways and Means

At-Large Members:
Barbara Comstock, Virginia
Renee Ellmers, North Carolina
Mike Fitzpatrick, Pennsylvania
Morgan Griffith, Virginia
Bradley Byrne, Alabama
Robert Hurt, Virginia
Adam Kinzinger, Illinois
Dan Newhouse, Washington
Randy Weber, Texas
Bruce Westerman, Arkansas
C. HOUSE REPUBLICAN STEERING COMMITTEE

Judy Schneider describes the composition of the House Republican Steering Committee as consisting of “party leaders, selected committee leaders, class leaders, and regional representatives.” The primary role of the House Republican Steering Committee is to nominate chairmen or ranking minority members of all standing committees. These nominations are then sent to the full Republican Conference for ratification. Schneider observes that “In recent Congresses, the Steering Committee ‘interviewed’ prospective candidates for ranking slots. Some of the new ranking members were the most senior members of the committee, others were not.” The House Republican Steering Committee for the 114th Congress is as follows:

Speaker.......................... John Boehner (5 votes)
Majority Leader............... Kevin McCarthy (2 votes)
Majority Whip...................... Steve Scalise
Chief Deputy Whip............... Patrick McHenry
Conference Chair............... Cathy McMorris Rodgers
Conference Secretary.............. Virginia Foxx
Republican Policy Chairman..... Allen Lucas Messer

209 Id.
210 Id.
NRCC Chair, former chair ....................... Tom Cole
NRCC Chair........................................ Greg Walden
Appropriations Committee Chair .............. Hal Rogers
Budget Committee Chair........................ Tom Price
Energy and Commerce Committee Chair ........ Fred Upton
Financial Services Committee Chair ......... Jeb Hensarling
Rules Committee Chair....................... Pete Sessions
Ways and Means Committee Chair.............. Paul Ryan
Texas Representative .............................. Lamar Smith
Regional Representatives...................... Joe Hecht, Kevin Yoder, John Shimkus, Candice Miller, Bill Shuster, Pat Tiberi, Steve Womack, Lynn Westmoreland, Bob Goodlatte, Devin Nunes, Jeff Miller, Cynthia Lummis
Class Representatives ......................... Jeff Denham, Richard Hudson

D. HOUSE MINORITY (CURRENTLY DEMOCRATIC) LEADERSHIP

Minority leadership positions in the House of Representatives consist of: the House Minority Leader; House Assistant Minority Leader; and House Minority Whip.

House Minority Leader
House Minority Leader............... Nancy Pelosi
Key Staff:

Chief of Staff .............................................. Nadeam Elshami
Assistant to the Chief of Staff ........... Ethan McClelland
Deputy Chief of Staff ............................... Diane Dewhirst
Deputy Chief of Staff .............................. George Kundanis
Policy Director ......................................... Dick Meltzer
National Security Policy Advisor .......... Wyndee Parker
Policy Advisors ................................. Margaret Capron, Kenneth DeGraff, April Greener, Patricia Ross
Counsel .................................................... Bernard Raimo, Michael Tecklenburg
Senior Advisor ............................................ Michael Bloom, Michael Long
Communications Director ....................... Drew Hammill
Deputy Communications Director .................. Evangeline George
Press Secretary ................................. Jorge Antonio Aguilar
Press Advisor .............................................. Stephanie Cherry
Senior Press Assistant ....................... Ned Adriance
Press Assistant ................................. Taylor Griffin
Sr. Advisor & Digital Director .................. Kat Skiles
Director of Speechwriting ....................... Henry Connelly
Deputy Director of Speechwriting ........... Malaika Robinson
Special Assistant ................................. Bina Surgeon
Executive Assistants ................. Emily Berret, Emma Kaplan
Staff Assistants ................................. Nicole MacDougall, Nikolas Youngsmith

House Assistant Minority Leader
House Assistant Minority Leader .............. James Clyburn
Key Staff:
E. The Senate

Top Leadership in the Senate Consists of: the Vice President of the United States who also serves as President of the Senate; and President Pro Tempore.
President of the Senate
Vice President of the United States and President of the Senate.......................... Joseph Biden, Jr.

Key Staff:
Chief of Staff........................................ Steven Ricchetti
Assistant to the Vice President............... Kathy Chung
Advisor to the Vice President.................. Michael Schrum
Staff Assistant..................................... Anne Marie Person
Senior Advisor..........................Greg Schultz
Counselor........................................ Don Graves
Policy Director.................................. Jamie Lyons
National Security Advisor.................. Colin Kahl
Senior. Advisor to Nat’l Security
Advisor ........................................... Alice Cosgrove
Executive Secretary & Special Advisor for National Security ............... Maj. Kristen Bakotic
Special Advisor, Europe & Russia ...............Michael Carpenter
Special Advisor, Homeland Security & Counterterrorism ........... CDR Laura Dickey
Director of Programs............................. Ward Dirksen
Special Assistant, National Security .................. Frances Castro
Counsel ............................................. John McGrail
Deputy Counsel...................... Alexander Mackler
Director of Research..................Nicole Lamberson
Deputy Director of Research .............. Kevin Higham
Director of Legislative Affairs ...........Tonya Williams
Special Assistant, Legislative Affairs ..................Lorea Stallard

President Pro Tempore
President Pro Tempore.......................... Orrin Hatch

Key Staff:
F. SENATE MAJORITY (CURRENTLY REPUBLICAN) LEADERSHIP

Majority leadership in the U.S. Senate consists of: the Senate Majority Leader; Senate Majority Whip; Secretary for the Majority; Senate Republican Conference; Senate Republican Policy Committee; and National Republican Senatorial Committee.211

Senate Majority Leader

Addison “Mitch” McConnell

Key Staff:

Chief of Staff .................................. Sharon Soderstrom
Deputy Chief of Staff .......................... Donald Stewart
Chief Counsel ................................. John Abegg
Legal Counsel ................................. Brian Lewis
National Security Advisor ................. Tom Hawkins
Policy Director ............................... Hazen Marshall
Policy Advisor & Counsel .................. Brendan Dunn
Policy Advisor ............................... Jonathan Burks,
                                        Neil Chatterjee,
                                        Scott Raab,
                                        Erica Suares,
                                        Terry Van Doren

Communications Director ................. Michael Brumas,
                                        Brian Forest (Deputy)

Staff Assistants
Suzanne Burton, Emily Costanzo, Mallory Shoffner

Senate Majority Whip
Senate Majority Whip John Cornyn
Key Staff:
Chief of Staff Russ Thomasson
Deputy Chief of Staff Monica Popp
Policy Advisor John Chapuis, Jonathan Slemrod

Secretary for the Majority
Secretary for the Majority Laura Dove

Senate Republican Conference
Chairman John Thune
Vice Chairman Roy Blunt

Key Staff:
Staff Director Brendon Plack
Communications Director Chandler Smith
Senior Writer Mary Katherine Ascik

Senate Republican Policy Committee
Chairman John Barrasso
Key Staff:
Staff Director Dan Kunsman
Policy Director Arjun Mody
Policy Analysts Dana Barbieri, Brian Blasé, Mitch Kominsky, Spencer Wayne
Policy Counsel Matt Leggett, Michael Stransky,
National Republican Senatorial Committee

Chairman .................................................. Roger Wicker
Vice Chairman ............................................. Tom Cotton
Vice Chairman ............................................. Joni Ernst
Vice Chairman ............................................. Dean Heller

Key Staff:
Executive Director ....................................... Ward Baker
Assistant to Executive Director ....................... Kevin Golden
Assistant to Deputy Executive Director ............. Alex Clark
General Counsel .......................................... Matthew Raymer
Research Director ....................................... Mark McLaughlin

G. SENATE MINORITY (CURRENTLY DEMOCRATIC) LEADERSHIP

Minority leadership in the U.S. Senate consists of: the Senate Minority Leader; Senate Minority Whip and Assistant Minority Leader; Senate Democratic Conference; Senate Democratic Policy and Communications Center; Democratic Senatorial Campaign Committee, and Democratic Steering and Outreach Committee.

Senate Minority Leader

---

Senate Minority Leader.................................Harry Reid

Key Staff:
Chief of Staff...........................................Drew Willison
Executive Assistant to Chief of Staff........................................Devon Brown
Deputy Chief of Staff................................David McCallum
Deputy Chief of Staff (Policy)...........................William Dauster
Executive Assistant to Minority Leader ........................................Adelle Cruz
Senior National Security Advisor.......................Jessica Lewis
Deputy National Security Advisor .....................Julie Klein
Chief Counsel......................................................Ayesha Khanna
Counsel........................................................................Wendy Helgemo
Policy Advisor.......................................................Ryan Mulvenon
Legislative Director......................................................Jason Unger
Senior Advisor, Intergovernmental & External Affairs..................................Portia White

Senate Minority Whip and Assistant Minority Leader
Senate Minority Whip / Assistant Minority Leader ........................................Dick Durbin
Key Staff:
Chief of Staff ..................................................Patrick Souders
Communications Director................................Ben Marter,
                                               Christina Mulka (Deputy)

Secretary for the Minority
Secretary for the Minority.........................Gary Myrick
Assistant Secretary for the Minority ............Tim Mitchell

Senate Democratic Conference
Senate Democratic Leader.............................Harry Reid
Vice Chair of the Conference.......................Charles Schumer
Established in 1947 as the Democratic Polity Committee (DPC), the Democratic Policy and Communications Center (DPCC), serves “as an advisory board to the Democratic Leadership and as a research, policy-formulating, and communications arm of Senate Democrats.”

Chairman ........................................ Charles Schumer
Vice Chairman ................................. Debbie Stabenow

Key Staff:
Staff Director ........................................ Mike Lynch
Policy Director ................................. Ryan McConaghy,
............................................................. Gerry Petrella
Policy Advisor ................................. Charlie Ellsworth
............................................................. Julie Klein
Policy Assistant ......................... Karlee Tebbutt
Research Director ......................... Dan Yoken
Communications Director ................. Matt House

I. DEMOCRATIC SENATORIAL CAMPAIGN COMMITTEE

The purpose of the Democratic Senatorial Campaign Committee is to foster election of a Democratic Senate. 216

Chairman .................................................. Jon Tester

J. DEMOCRATIC STEERING AND OUTREACH COMMITTEE

The purpose of the Democratic Steering and Outreach Committee is to foster “dialogue between Senate Democrats and leaders from across the nation. Each year, the Steering Committee hosts numerous meetings with advocates, policy experts, and elected officials to discuss key priorities and enlist their help in the development of the Senate Democratic agenda.” 217 Leadership of the Democratic Steering and Outreach Committee is as follows:

Chair .................................................... Amy Klobuchar
Vice Chair .............................................. Jeanne Shaheen

Key Staff:
Staff Director ........................................ Patrick Hayes

Little understood or fully appreciated outside the halls of the U.S. Congress is the importance of the professional congressional staffs. For example, the Senate Select Committee on Intelligence reports that “The Committee’s staff reviews intelligence reports, budgets, and activities; investigates matters on behalf of the Committee; prepares legislation; and receives briefings.” It is the diligent behind-the-scenes hard work of congressional staff on both sides of the aisle that serves as the foundation for educating members of congress about issues before them, facilitating congressional oversight, and formulating legislation. Congressional Quarterly observes that, “The influence of the staff-bureaucracy has grown over the years as many members, swamped with a workload of increasing bulk and complexity, rely on their aides for policy recommendations and professional


219 U.S. Senate Select Committee on Intelligence, About the Committee, Overview of the Senate Select Committee on Intelligence Responsibilities and Activities, Staff, available at http://www.intelligence.senate.gov/about.html (last viewed Sept. 2, 2015).
Congressional committee staff is credited by Congressional Quarterly with performing the following essential functions:

1. Organizing hearings…
2. Oversight and Investigations. Much original research is conducted by staff members on issues that come before a committee. This usually involves a critique of existing legislation, court decisions and current practices…
3. Bill markup and Amendment…
4. Preparing Reports…
5. Preparation for Floor Action…
6. Conference Committee Work…
7. Liaison With Executive Branch, Special Interests… [and]
8. Press Relations…

One former U.S. Senator observes that
A politically minded young person can rise to apposition of responsibility as a Hill staffer faster than almost anywhere else. But just as for their bosses, the pace and the work are brutal and the pay is generally low. Some Senate staffers burn out or move on after a few years, having gained vital experience and insight on how government works. For those who stay on the Hill, some move from ‘personal staff,’ based in a senator’s office, to a ‘professional’ committee staff, joining a team of issue experts, typically through appointment from a senator to a committee on which he serves. The

---

220 CONGRESSIONAL QUARTERLY, supra note 28 at 105.
221 Id. at 107.
committee staffer will cover meetings for senators, advise them on issues and votes and negotiate legislation.222

XXIII. Government Accountability Office

Established in 1921 as The General Accounting Office, on July 7, 2004 it was renamed The Government Accountability Office (GAO), and “is the largest of the three agencies that provide staff support, research, review and analysis for Congress.”223 Professor Anne Joseph O’Connell reports that “Congress subsequently gave the GAO substantial additional authority after Watergate… the GAO now investigates, culls, and synthesizes stances on a multitude of policy programs and expenditures on its own initiative, by legislative mandate, and at the request of congressional committees and individual members of congress.”224

Professor Samuel Workman observes that, “For systems of any type, information on current and past performance forms an important source of feedback for decision-making. In the case of policymaking systems, an important form of feedback is policy analysis… Feedback is also fundamental to depictions of policy change in the

222 See DASCHLE & ROBBINS, supra note 19 at 53.
During recent years, many governments have shifted focus from how revenues are raised to “the efficiency with which money is spent.” However, the institution of Congress is not “well-structured to conduct policy analysis,’ because it is too political a body to bring systematic, unbiased evidence to bear on policy decisions. Congress is a representative assembly, not a research bureau. Its internal organization is inconsistent with analytical perceptions and definitions of policy issues.”

Many reasons are given for Congresses’ lack of policy analysis capability, including the parochial nature of Congressional members, where “geographical representation and single-member districts compel lawmakers to respond to local pressures, and undermine the incentive to legislate in the national interest. Congress also caters to the demands of interest groups, and regularly makes economic decisions that policy analysts find indefensible on efficiency grounds.”

XXIV. Congressional Budget Office

---

228 Id.
The strictly nonpartisan Congressional Budget Office (CBO) since 1975 “has produced independent analyses of budgetary and economic issues to support the Congressional budget process. Each year, the agency’s economists and budget analysts produce dozens of reports and hundreds of cost estimates for proposed legislation.”

In addition, the CBO “conducts objective, impartial analysis; and hires its employees solely on the basis of professional competence without regard to political affiliation. CBO does not make policy recommendations, and each report and cost estimate summarizes the methodology underlying the analysis.”

Eric Ghysels and Nazire Ozkan observe that, “Under its routine procedures, the CBO prepares baseline projections incorporating the assumption that current laws generally remain in place; those projections are designed to serve as a benchmark that policymakers can use when considering possible changes to those laws.”

XXV. Library of Congress

Created in 1914, and now known as the Congressional Research Service (CRS) of the Library of Congress, the CRS states its mission as to serve “the Congress throughout the legislative process by providing


230 Id.

comprehensive and reliable legislative research and analysis that are timely, objective, authoritative and confidential, thereby contributing to an informed national legislature.”

Operating as shared staff to Members of Congress and congressional committees, CRS “Staff members analyze current policies and present the impact of proposed policy alternatives… [such as:] reports on major policy issues; tailored confidential memoranda, briefings and consultations; seminars and workshops; expert congressional testimony; and responses to individual inquiries.”

During FY2012, the CRS responded to 698,179 requests from congressional members and committees for services such as: over “71,000 requests for analysis, information, and research; more than 9,000 congressional participants in seminars, institutes, and training sessions, and nearly 618,000 client visits to the CRS Web site home page that resulted in more than 1 million copies of CRS products viewed on the CRS Web site.” The Library of Congress reports that

CRS analysts work in a collaborative, multidisciplinary environment to prepare detailed explanations of complex

---

policy issues, identify and assess policy approaches, develop and analyze legislative options, conduct legal analysis of pending legislation and administrative actions, provide in-person consultations on public policy issues, and assist with legislative procedures as well as processes relating to the federal budget and appropriations. Analysts also deliver expert testimony before congressional committees, support hearings and investigations, identify prospective witnesses, prepare products on current legislative issues, and respond to specific requests with confidential memoranda.  

Regarding legal issues pertaining to cybersecurity legislation, “Among the issues CRS attorneys analyzed were the use of smart meters, computer crime, the authority of the federal government to block access to certain Internet sites, privacy effects of information-sharing regimes, protection of federal networks, and the Fourth Amendment implications of government network-monitoring programs.”

XXVI. Call to Action

A major question about effective congressional oversight is whether congress as an institution can react in a timely matter to the increasing rate of technological change. Scott Shackelford observes that on a global basis,

\footnote{Id.}

\footnote{Id. at 22.}
“internet governance is fracturing, which makes addressing cybersecurity challenges all the more difficult.”

Just as technology has brought disruptive change to many aspects of modern life, congressional leadership must ask and examine whether the institution is effectively adapting as currently structured.

XXVII. Conclusion

Congressional oversight is a process whereby Congressional committees exercise a crucial role in monitoring and holding administrative agencies accountable for matters relating to cybersecurity and national defense. So many aspects of cybersecurity have the potential for use by: terrorists; by foreign entities as a tool to conduct industrial espionage against U.S. business; and by nation state adversaries, or others intent upon creating serious disruption. These various threats mean that cybersecurity policy in many ways must be treated just like the strategic and operational plans of a country at war.

---

About the Journal of Law and Cyber Warfare
The Journal of Law and Cyber Warfare is published twice per year by top legal professionals and scholars from the law, technology, security, and business industries. The views expressed in the Journal of Law and Cyber Warfare are those of the authors and not necessarily of the Journal of Law and Cyber Warfare or the Lexeprint Inc — the publishing company.

Submissions
The Journal welcomes submissions from legal scholars, technologists, mathematicians, analysts, academics, policy makers, practitioners, lawyers, judges and social scientists.

Form: Citations conform to The Bluebook: A Uniform System of Citation (20th ed. 2015). Please cite the Journal of Law and Cyber Warfare as: 6 J.L. & CYBER WARFARE __ (2016).

Copyright: All articles copyright © 2012-2016 by the Journal of Law and Cyber Warfare except where otherwise expressly indicated. For all articles to which it holds copyright, the Journal of Law and Cyber Warfare permits copies to be made for classroom use, provided that (1) the author and the Journal of Law and Cyber Warfare are identified, (2) the proper notice of copyright is affixed to each copy, (3) each copy is distributed at or below cost, and (4) the Journal of Law and Cyber Warfare is notified of the use.

Electronic submissions are encouraged. Submissions by email and attachment should be directed to submissions@jlcw.org.

Subscriptions: The cost of an annual subscription is $250. Subscription requests should be e-mailed to info@jlcw.org.