BREACH OF FAITH: A LACK OF POLICY FOR RESPONDING TO DATA BREACHES AND WHAT THE GOVERNMENT SHOULD DO ABOUT IT

Jared Burns[*]

Abstract

One data breach in the summer of 2015 against the United States government cost taxpayers more than $350 million. Since 2005, the U.S. government has lost more than 183 million personnel records and countless files containing sensitive information. Despite all of this, the government has failed to create a policy for responding to data breaches. As proof of a lack of any clear policy, this Note analyzes two recent breaches against the government and explains how the responses, or lack thereof, are at opposite ends of the response continuum.

This Note creates a policy for government response to data breaches. This policy analyzes the factors surrounding the breach, including the actor who perpetrated the breach, the information stolen, and the potential uses for that information. This Note then lays out a continuum of potential responses, from doing nothing to kinetic action. Lastly, this Note creates a decision matrix that assigns responses to breaches based on the factors of the breach. The result is a policy shell that allows government decision makers to respond to breaches in a way that instills confidence in the American public and deters potential hackers.

* Jared Burns graduated from the University of Florida Levin College of Law in May of 2017. He has a Master of Business Administration from the University of Florida and is a United States Marine.

INTRODUCTION

What do a targeted drone strike,[1] a $133 million identity monitoring contract,[2] and the resignation of the Director of the Office of Personnel Management all have in common?[3] They were all actions by the U.S. government in response to data breaches in the summer of 2015.[4] Since 2005, government entities have lost at least 183 million personnel records as a result of data breaches.[5] The Office of Personnel Management (OPM) breach in the summer of 2015 cost the U.S. taxpayers at least $350 million,[6] not to mention the risks to national security and the damage to the intelligence community.[7] Currently the government lacks any type of decisional framework for responding to data breaches, resulting in haphazard responses that range from targeted killings to doing nothing.[8]

---

1. Kimiko De Freytas-Tamura, *Briton Who Recruited Online for ISIS is Reported Killed*, N.Y. TIMES, Aug. 28, 2015, at A3.

2. News Release, Office of Pers. Mgmt., OPM, DoD Announce Identity Theft Protection and Credit Monitoring Contract (Sept. 1, 2015), https://www.opm.gov/news/releases/2015/09/opm-dod-announce-identity-theft-protection-and-credit-monitoring-contract/.

3. Erin Kelly & David Jackson, *OPM Chief Katherine Archuleta Resigns*, USA TODAY, (July 10, 2015, 4:36 PM), http://www.usatoday.com/story/news/nation/2015/07/10/opm-chief-archuleta-resigns/29965857/.

4. *See supra* notes 1–3.

5. *Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last visited Jan. 23, 2017) (providing statistics for all reported data breaches).

6. News Release, Office of Pers. Mgmt., *supra* note 2. The contract announced by OPM was listed at $133 million, however, the contract is renewable for three years and it cost OPM $20 million to notify those affected by the breach. Elizabeth Harrington, *OPM Hack Costing Taxpayers $350 Million*, WASH. FREE BEACON (Sept. 2, 2015, 10:39 AM), http://freebeacon.com/issues/opm-hack-costing-taxpayers-350-million/.

7. Dan Verton, *Impact of OPM Breach Could Last More Than 40 Years*, FED SCOOP (July 12, 2015, 4:43 PM), http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community (quoting former CIA Director Michael Hayden as saying that the threat to intelligence could last forty years, until the last of those whose information was stolen retires from federal service).

8. David Sanger, *U.S. Decides to Retaliate Against China's Hacking*, N.Y. TIMES, Aug. 1, 2015, at A6 (stating that the Obama administration has struggled to develop a response to the OPM hack).

In order to effectively defend against cyber intrusions and attacks, the government must combine nontechnical with technical means.[9] Technical means refer to the hardware and software used to protect networks, whereas nontechnical means "usually combines leadership, education, and policy development."[10] This Note will only focus on the third aspect of nontechnical means, "policy development."[11] This Note develops a range of responses to data breaches against the government, such as the OPM hack,[12] and creates a decisional framework for choosing the best response. This Note analyzes the wide range of possible responses—from full-out "kinetic"[13] war to doing nothing—and determines the best response based on the circumstances surrounding the breach. The factors that should be analyzed in determining the correct response are: the actor who committed the breach, the information taken, and the potential uses for that information.

Analyzing the factors requires a distinction between different types of cyber operations. All too often, all types of cyber activities are grouped under the term cyberattack.[14] However there is a distinction between cyberattacks, cybercrime, cyberterrorism, cyber hacktivism, cyber intrusions, and other cybervandalism.[15]

There have been many definitions of cyberattack. Yale Law School Professor of International Law Oona Hathaway argues that "[a] cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose."[16] Professor Hathaway goes on to distinguish a cyberattack from cyber espionage, but her argument lacks significant distinction. By claiming that "[t]o 'undermine the function' of a computer system, an actor must do more than passively observe a computer network or copy data," Professor Hathaway ignores the fact that by gaining access to a computer

9. Juan Cayón Peña & Luis Armando García, *The Critical Role of Education in Every Cyber Defense Strategy*, 41 N. KY. L. REV. 459, 465 (2014).

10. *Id.*

11. *Id.*

12. *Cybersecurity Incidents: What Happened*, OFF. PERS. MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened (last visited Jan. 23, 2017).

13. In this context, "kinetic war" refers to warfare with traditional physical actions, such as bombing and shooting, as opposed to warfare that would lack such effects (i.e., information warfare).

14. *See* P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 67–69 (2014) ("Essentially, what people too often do when discussing 'cyberattacks' is bundle together a variety of like and unlike activities, simply because they involve Internet-related technology.").

15. *See* Myriam Dunn Cavelty, *Cyberwar: Concept, Status Quo, and Limitations*, CSS ANALYSIS IN SECURITY POL'Y, Apr. 2010, at 1, 1–2.

16. Oona A. Hathaway et al., *The Law of Cyber Attack*, 100 CALIF. L. REV. 817, 826 (2012).

network, the actor has at some point undermined the function of that system.[17] This is especially true with classified networks where one of the primary functions of the network is to keep the information on it secure.[18] However, the distinction that Professor Hathaway makes between defining cyberattack in terms of its objective rather than by its means is valuable and worth pointing out.[19] By defining a cyberattack by its objective, it demonstrates that cyber operations can span multiple domains.[20]

We will continue to follow an objective- or intention-based approach in our definition of cyberattack, but will consider violence the objective. Therefore, we will define a cyberattack as a "cyber operation . . . that is reasonably expected to cause injury or death to persons, or damage or destruction to objects."[21] This definition encompasses what the Department of Defense (DOD) has used to describe as cyber operations that constitute a use of force under *jus ad bellum*[22] and the United Nations (U.N.) Article 2(4).[23] Integrating the definition of cyberattack to meet the requirements of use of force allows it to be easily distinguished from other types of harmful cyber activities.

A cyber intrusion, as distinguished from a cyberattack, can be classified as a "covert action[] employing small-scale operations against a specific computer, computer system, or user, whose individual compromise would have significant value."[24] Cyber intrusions, the focus of this Note, include data breaches, cyber espionage, and hacking. Cyber espionage, or the targeting of computers and networks to obtain otherwise confidential information,[25] is not deemed to be a violation of international law and is conducted by the United States.[26] Whether a particular cyber

17. *Id.* at 830 (emphasis omitted).

18. *See id.*

19. *Id.* at 826–28.

20. *Id.* (explaining that cyber operations can be used to assist in controlling the traditional domains of air, land, and sea).

21. Gary D. Solis, *Cyber Warfare*, 219 MIL. L. REV. 1, 12 (2014).

22. *Jus ad bellum* is the criteria used to determine whether engaging in a certain armed conflict is just. *See Jus Ad Bellum*, BLACK'S LAW DICTIONARY (10th ed. 2014). For a more detailed explanation of *jus ad bellum* and cyber warfare, see Hathaway et al., *supra* note 16, at 839–43.

23. OFFICE OF GEN. COUNSEL, U.S. DEP'T OF DEF., LAW OF WAR MANUAL 998–99 (2015).

24. Solis, *supra* note 21, at 13.

25. SINGER & FRIEDMAN, *supra* note 14, at 93; Luke Pelican, *Peacetime Cyber-Espionage: A Dangerous but Necessary Game*, 20 J. COMM. L. & POL'Y 363, 365 (2012).

26. OFFICE OF GEN. COUNSEL, *supra* note 23, at 999 ("[T]o the extent that cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber operations would likely be treated similarly under international law. The United States conducts such activities via cyberspace, and such operations are governed by long-standing and well-established

intrusion is classified as cyber espionage or something more will be an important determination for developing an appropriate response.

The focus of this Note is on responses that the government should take against a perpetrator of a cyber intrusion and not on the responses that help those affected by the breach.[27] This Note develops a framework for analyzing and responding to breaches against the government and does not address breaches against private institutions.[28] This Note will lay out the decisional framework in three parts. First, it will look at two recent breaches against the government: the hack by the Chinese against the OPM and the public release of U.S. Military service members' personal information by a terrorist hacker.[29] The responses to these two cases illustrate the bookends for the array of responses the government could take.[30] Part II looks at the different factors that should be analyzed in assessing the severity of a breach. Part II begins by discussing the different types of actors and then explores the types of data taken and its potential uses. Part III examines the different responses that the government could take. Lastly this Note concludes by putting together the decisional framework.

---

considerations, including the possibility that those operations could be interpreted as a hostile act." (footnote omitted)).

27. *See* Joe Davidson, *Months After OPM Hack, 21.5 Million People Are Formally Being Advised, and Offered Help*, WASH. POST, Oct. 2, 2015, at A19 (explaining the actions that OPM was taking to help those potentially affected by the theft of their personal information). *See generally* Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion, and the Modern Data Breach*, 69 FLA. L. REV. 771 (explaining the various privacy laws and legal options for those affected by data breaches).

28. Although excluding breaches against private institutions, it includes government information held by private institutions. For example, the Chinese government stole classified information regarding the F-35 Joint Strike Fighter aircraft. *China's Cyber-Theft Jet Fighter*, WALL ST. J. (Nov. 12, 2014, 7:32 PM), http://www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777. Although the data breach was against Lockheed Martin's information systems and not the U.S. government's, the breach stole U.S. secrets and thus is classified as a data breach against the government. *Id.* However, it will not encompass breaches against private institutions that had government employees' personal information stolen if the private institution had the government employees' information because they were a private consumer. This means that this Note will not discuss the Target or Ashley Madison breaches, even though government employees had their personal information stolen as a result. *See* Cory Bennett, *15,000 Government Emails Revealed in Ashley Madison Leak*, HILL (Aug. 19, 2015, 9:55 AM), http://thehill.com/policy/cybersecurity/251431-ashley-madison-leak-appears-real-includes-thousands-of-government-emails (explaining that more than 15,000 of the email accounts revealed belonged to government employees and military members).

29. *See infra* Part I.

30. The Obama administration has not publicly responded to the Chinese for their theft of personal information demonstrating that, although unwise, the government can choose to do nothing. *See* Sanger, *supra* note 8. At the other end of the spectrum, the government used a drone strike against a terrorist who published online service members' personal information. *See* De Freytas-Tamura, *supra* note 1.

I. RECENT CASES

This Part analyzes two recent data breaches against the U.S. government and the actions that the government took in response to those breaches.

A. *The Office of Personnel Management Hacks*

On June 4, 2015, OPM released a memorandum stating that sensitive personal information for approximately four million federal employees was stolen from OPM computer systems.[31] Further investigations revealed two separate but related intrusions into OPM computer systems.[32] Those intrusions compromised sensitive information on more than twenty-one million current and former federal employees.[33] The United States government has refused to publicly name a culprit.[34] However, some public officials, such as the Director of National Intelligence James Clapper, have acknowledged that China is responsible.[35] The government has done nothing publicly to respond.[36] The Obama Administration had the difficult task of determining the appropriate response for different types of cyberattacks.[37]

B. *Daesh Hacking and the Drone-Strike Response*

On August 15, 2015, the terrorist group Daesh, also known as ISIS (Islamic State of Iraq and Syria), ISIL (Islamic State of Iraq and the Levant), or IS (Islamic State),[38] released online a second list containing

---

31. News Release, Office of Pers. Mgmt., OPM to Notify Employees of Cybersecurity Incident (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.

32. *Cybersecurity Incidents: What Happened*, *supra* note 12.

33. *Id.*

34. Ellen Nakashima, *U.S. Decides Against Publicly Blaming China for Data Hack*, WASH. POST (July 21, 2015), https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html.

35. Sanger, *supra* note 8 (quoting James Clapper as saying, "you have to salute the Chinese for what they did").

36. *Id.*

37. *See id.*

38. I chose to call the group Daesh, which is the acronym created from the group's name in Arabic ("al-Dawla al-Islamiya fil Iraq wa al-Sham"). The terrorist organization does not like being called Daesh because it has negative connotations in Arabic. Faisal Irshaid, *Isis, Isil, IS, or Daesh? One Group, Many Names*, BBC NEWS (Dec. 5, 2015), http://www.bbc.com/news/world-middle-east-27994277. I prefer to not give the organization legitimacy by calling them ISIS, ISIL, or IS, because their goal of establishing an authoritarian Islamic state is based on a perverted form of Islam. *See id.*

military service members' personal information.[39] The list was reportedly distributed by well-known Daesh hacker Junaid Hussain.[40] Hussain, a British citizen, was the leader of a group known as the Cyber Caliphate, which provided online recruiting and hacking for Daesh.[41] Additionally, he took responsibility for hacking into U.S. Central Command's Twitter and YouTube accounts and posting threats against military members.[42] On August 25, 2015, the U.S. Military killed Hussain in a targeted drone strike.[43] The debate over the legality of using targeted drone strikes is outside the scope of this Note.[44] However, the use of kinetic force, to include drone strikes, is an option for responding to data breaches.

Although there are differences between Hussain's actions and the OPM hack, the responses to each, targeted killing and doing nothing, are extreme opposites and show the lack of any clear government policy for responding to data breaches.[45] The decision matrix introduced in this Note is a starting point to rectify this lack of policy.

II. DECIDING WHAT TO DO MADE EASY—A DECISION MATRIX

The decision matrix introduced below should be used by government decision makers to determine the appropriate response to data breaches. Doing so will limit the indecisiveness and confusion expressed by the Obama administration.[46] The decision matrix, depicted in Figure 1, intersects actors of the breach with the severity of the information stolen. The "actors" are listed along the Y-axis and the "severity of the information stolen" is listed along the X-axis. The inside boxes list Roman Numerals that correspond to the appropriate response options based upon the two factors associated with the breach. The factors and responses are analyzed in Parts III and IV, respectively, but it is important to introduce the decision matrix beforehand to provide context.

Once the government obtains the appropriate information, using the decision matrix is easy. The first step is to identify the actor and determine to which Y-axis classification they belong.[47] The next step is

39. *ISIS Claims to Release Another U.S. Military "Hit List,"* CBS NEWS (Aug. 12, 2015, 1:38 PM) [hereinafter CBS NEWS], http://www.cbsnews.com/news/isis-claims-to-release-another-us-military-hit-list/.

40. *Id.*; *see also* De Freytas-Tamura, *supra* note 1.

41. *See* De Freytas-Tamura, *supra* note 1.

42. Dan Lamothe, *Islamic State Loyalists Hack U.S. Military Social Media*, WASH. POST, Jan. 13, 2015, at A01.

43. De Freytas-Tamura, *supra* note 1.

44. *See generally* Oren Gross, *The New Way of War: Is There a Duty to Use Drones?*, 67 FLA. L. REV. 1, 25–30 (2015).

45. *See* De Freytas-Tamura, *supra* note 1; Sanger, *supra* note 8.

46. *See* Sanger, *supra* note 8.

47. *See infra* Part III (explaining the different classifications of actors who conduct data

to determine the severity of the breach. The severity, which is rated from insignificant to extreme, is determined through the totality of the circumstances—focusing on the information stolen and the potential uses of that information.[48] The box where the actor and severity level intersect contains the appropriate types of responses that can be taken. The types of potential responses, as described below, often encompass many different actions the government could take and should be scrutinized with the specifics of the actor and breach.

Figure 1

		Severity of Information Taken				
		Insignificant	**Negligible**	**Moderate**	**Extensive**	**Extreme**
Actor	**Terrorist**	II. or VI.	II., IV., & V.	II., IV., & V.	I., II., IV., & V.	I., II., IV., & V.
	State Actor	III. or VI.	III.	II. or III. or IV.	II., III., & IV.	I., II., III., & IV.
	Criminal Groups	V. or VI.	V.	V.	V.	II. & V.
	Hacktivist	V. or VI.	V.	V.	V.	II. & V.

Recommended Actions
I. Kinetic Action
II. Retaliatory Countermeasures
III. Diplomatic Action
IV. Economic Sanctions
V. Criminal Prosecution

breaches against the United States).

48. *See infra* Part IV (explaining the different types of information stolen and how to determine its severity level).

III. FACTORS FOR ANALYZING THE SEVERITY OF A BREACH

This Part begins by looking at the different types of actors who commit data breaches. Next, this Part analyzes the types of data that can be taken from a data breach and the potential uses for that data. This information is then used to assign a severity level to the breach. The severity level is based on assessing the totality of the circumstances for each factor. Once a severity level has been assigned, the potential responses that correlate with that level can be chosen.

A. *Actors*

The first factor to analyze in determining the severity of the intrusion is the actor. This information will not always be readily available as attribution is extremely difficult in cyber operations.[49] This is so because it is easy for hackers to mask where they are, what their nationality is, and what organization they represent.[50] If an actor can be identified, the actor can be classified into one of two main groups: state or non-state actor. Determining whether a known perpetrator of a cyber intrusion is a state actor is relatively straightforward—was the perpetrator of the attack acting on behalf of a state government? Non-state actors encompass many different types of groups including individuals, terrorist organizations, belligerents,[51] and others. The Government Accountability Office (GAO), which reports on cybersecurity for Congress, defines the types of attackers by their motive rather than by their means.[52] The GAO breaks up actors into six different categories: bot-network operators, criminal groups, hackers/hacktivists, insiders, nations, and terrorists.[53] Although each group is defined by motive, the groups are not mutually exclusive.[54] This Note will focus on state actors, terrorists, criminal groups, and hacktivists. We will not look at bot-network operators nor insiders because they fit within the other groups.[55]

---

49. *See* SINGER & FRIEDMAN, *supra* note 14, at 73–74 (explaining that it is easy to obscure where a cyber operation originated from, thus making it very difficult to determine who is responsible).

50. *Id.*

51. *See* OFFICE OF GEN. COUNSEL, *supra* note 23, at 102–06 (describing the different types of belligerents and their qualifications).

52. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-758T, INFORMATION SECURITY: CYBER THREATS AND DATA BREACHES ILLUSTRATE NEED FOR STRONGER CONTROLS ACROSS FEDERAL AGENCIES 4 (2015).

53. *Id.*

54. *See id.*

55. *See id.* The GAO defines a bot-network operator as someone who uses a network of remotely controlled systems to coordinate attacks. *Id.* However, bot-net operation is more a method of hacking than a type of actor. Terrorists, hacktivists, state actors, or criminals could all use bot-networks to conduct their attacks and therefore there is no need for the distinction in this

Classifying the actor is important because different classes of actors should receive different types of treatment based on the information stolen and its potential uses. This is evident through the two examples provided earlier.[56] When Hussain, a terrorist, stole personal information of military members, he was sought out and killed in a drone strike.[57] Alternatively, when the Chinese government stole personal information of federal employees, many of whom were military members, there was no official response.[58] This distinction is also important because the government should be far less likely to respond with kinetic force against a state actor than a non-state actor.

1. State Actors

State actors primarily use cyber intrusions for espionage.[59] However, some advanced nations such as China and Russia are developing sophisticated information warfare "doctrine, programs, and capabilities," which would allow them to use cyber weapons to disrupt and destroy vital assets.[60] Cyber espionage by state actors has a major distinction from traditional espionage in that traditional espionage usually required someone to be put in harm's way—such as a spy or surveillance aircraft.[61] In contrast, cyber espionage can be conducted from the relative safety of the spy's own home millions of miles away.[62] This ability to spy from safety, combined with the attribution problem,[63] decreases the deterrent factor of being caught.[64] Although China[65] and Russia[66] have received most of the criticism for cyber espionage, many countries have the ability

---

Note. *Id.* Similarly, insiders reveal more about the "how" than the "who." *Id.* To further explain, any insider who uses the information would be classified as a criminal, terrorist, hacktivist, or spy depending on how they use the information, and thus there is again no need for the distinction. *Id.*

56. *See supra* Part I (discussing recent hacks against the government).

57. De Freytas-Tamura, *supra* note 1.

58. Sanger, *supra* note 8.

59. *See* Pelican, *supra* note 25, at 365.

60. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 52, at 4.

61. Pelican, *supra* note 25, at 384.

62. *See id.*

63. *See* SINGER & FRIEDMAN, *supra* note 14, at 73–74.

64. *See* Pelican, *supra* note 25, at 384 (explaining that the risk of harm to the spy or host state is minimal if they are discovered because they are operating from a foreign country).

65. *See* Paul Eckert & Daniel Magnowski, *Kissinger, Huntsman: U.S., China Need Cyber Détente*, REUTERS (June 14, 2011, 2:48 AM), http://www.reuters.com/article/2011/06/15/us-china-kissinger-cyber-idUSTRE75D62Q20110615.

66. *See* Tom Vanden Brook & Michael Winter, *Hackers Penetrated Pentagon Email*, USA TODAY (Aug. 7, 2015, 12:19 PM), http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/ (blaming Russia for taking down the Joint Chiefs of Staff's unclassified network for two weeks).

to, and do, conduct cyber espionage.[67] Cyber intrusions by state actors are difficult to respond to because of the complex nature of relationships among countries, especially if the intrusion was against a friendly nation.[68]

2. Terrorists

A second category of actor is terrorists. Terrorists are individuals or groups who use violence, or the threat of violence, to intimidate civilian populations, influence government policy through coercion, or alter government conduct.[69] It is important to note that to be classified as a terrorist, one must use or threaten to use violence.[70] Therefore, someone cannot be classified as a terrorist simply by conducting data breaches, even if their aims are similar to terrorists. Thus, data breaches are simply a tool used by terrorists to help them in their objectives of mass civilian panic, political manipulation, and governmental disruption.[71]

Terrorists often use cyber intrusions to generate funds,[72] recruit individuals to their cause, damage public morale, or threaten national security.[73] Terrorist organizations steal personal data from individuals and sell that information or use it fraudulently to acquire funds.[74] Additionally, terrorists can use stolen identities to access government facilities, avoid detection, or purchase dangerous supplies such as firearms.[75] Recently, terrorist cyber breaches against the U.S.

---

67. S*ee* Siobhan Gorman, *Navy Hacking Blamed on Iran Tied to H-P Contract*, WALL ST. J. (Mar. 6, 2014, 7:24 PM), http://www.wsj.com/articles/SB10001424052702304732804579423611224344876 (discussing an Iranian hack of a Navy and Marine Corps unclassified network); *see also* OFFICE OF GEN. COUNSEL, *supra* note 23, at 999.

68. *See* Eyder Peralta, *Germany Closes Probe into Alleged U.S. Hacking of Merkel's Phone*, NPR (June 12, 2015), http://www.npr.org/sections/thetwo-way/2015/06/12/413866194/germany-closes-probe-into-alleged-u-s-hacking-of-merkels-phone (explaining that the "allegations and probe strained the relations between the two allies").

69. 18 U.S.C. § 2331 (2012); *Terrorist*, BLACK'S LAW DICTIONARY (10th ed. 2014).

70. *See* 18 U.S.C. § 2331.

71. *See id.*

72. CATHERINE A. THEOHARY & JOHN ROLLINS, CONG. RESEARCH SERV., R41674, TERRORIST USE OF THE INTERNET: INFORMATION OPERATIONS IN CYBERSPACE 2 (2011) ("Cybercrime has now surpassed international drug trafficking as a terrorist financing enterprise.").

73. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 52, at 4.

74. DEMOCRATIC STAFF OF THE HOMELAND SEC. COMM., 109TH CONG., IDENTITY THEFT & TERRORISM 9–10 (2005).

75. *Id.* (explaining how terrorists have created fake identities using stolen information to remain undetected or to gain access to government facilities).

government[76] were conducted to damage public morale,[77] demonstrate power, [78] and recruit lone wolf actors to their cause.[79]

3. Criminal Groups

Criminal groups are a third type of actor that attempts to breach government data systems.[80] The GAO defines cyber-criminal groups as those who "seek to attack systems for monetary gain."[81] This definition, however, can cross over with other types of actors, particularly state actors and terrorists.[82] Therefore the distinction should be that cyber-criminals' ultimate goal is monetary gain, whereas state actors and terrorists have additional objectives. Claims against the Chinese government for trade secret theft from U.S. companies is a prime example of a state actor that attacks computer systems for financial gain.[83] Although cyber criminals are more likely to go after individuals and businesses,[84] they could still steal information from the government for monetary gain.[85] Just as personally identifiable information (PII) can be

76. *See* CBS NEWS, *supra* note 39.

77. *See* Ashley Frantz, *As ISIS Threats Online Persist, Military Families Rethink Online Lives*, CNN (Mar. 23, 2015, 7:00 PM), http://www.cnn.com/2015/03/23/us/online-threat-isis-us-troops/ (quoting military spouses who now fear attacks against them as a result of Daesh posting their names and addresses online).

78. *See* Jenny Vaughan, *US Marine Corps Urges 'Vigilance' After Online Islamist Threat*, YAHOO! NEWS (Mar. 22, 2015, 9:26 AM), http://news.yahoo.com/us-marine-corps-urges-vigilance-hacking-threat-103621598.html (quoting NATO Commander Phillip Breedlove calling the hacks an attempt by the organization to detract attention away from their recent military defeats).

79. Pamela Brown & Jim Sciutto, *FBI Warns Military of ISIS Threat*, CNN (Dec. 1, 2014 8:30 PM), http://www.cnn.com/2014/12/01/politics/fbi-warns-military-of-isis-threat/ ("The FBI issued a warning Sunday to members of the U.S. military that ISIS is calling for attacks against them, according to a law enforcement source, saying that 'overseas based individuals are looking for like-minded individuals in the U.S. to carry out these attacks.'").

80. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 52, at 4.

81. *Id.*

82. *See id.*

83. *See* Indictment at 1–2, United States v. Dong, No. 14-118 (W.D. Pa. May 1, 2014); Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

84. *See* CTR. FOR STRATEGIC & INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 13 (2014) ("This means that the lost revenues from the theft of IP through hacking could be almost as much as the value of legitimate IP transactions.").

85. If the OPM hack was conducted by a non-state actor whose goal was to steal the identity of the individuals whose information was taken, then that would be cybercrime against the government, because the information was still stolen from the government. *See* Dave Lee, *Chinese Man Pleads Guilty to US Military Hack*, BBC (Mar. 23, 2016), http://www.bbc.com/news/technology-35888106.

stolen from individuals or businesses and used for identity theft, the government is also susceptible to this threat from criminal groups.[86]

4. Hacktivists

Hacktivists are another category of actor that can be used in developing a response to a data breach against the government. Hackers illegally access networks "for the challenge, revenge, stalking, or monetary gain."[87] Hacktivism "involves the use of technology hacking mechanisms . . . to effect particular political and/or social change."[88] Although hacktivists seek political change, they are different from terrorists because they do not use violence to achieve their objectives. Hacktivists have mixed support often based on their mixed motives.[89] The most notable hacking group is Anonymous, a loosely connected group that conducts cyberattacks for various political and social causes.[90] Hacktivists often attack government computers through distributed denial of service (DDoS)[91] attacks, in order to send a political message.[92] Data breaches against the government by hacktivists have been in the news in the wake of the leaks by Bradley (now Chelsea) Manning and National Security Agency (NSA) contractor Edward Snowden.[93] Although both Manning and Snowden have been charged with crimes,[94] I have chosen

86. *See* News Release, Office of Pers. Mgmt., *supra* note 31 (explaining that individuals whose personal information was stolen would receive free credit monitoring and identity-theft protection).

87. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 52, at 4.

88. Xiang Li, Note, *Hacktivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime*, 27 HARV. J.L. & TECH. 301, 302 (2013).

89. *See id.* at 303–04.

90. *See id.* Anonymous has supported many different social and political causes since its founding in 2003. *Id.* However, recently Anonymous and its offshoot, GhostSec, have begun waging a cyberwar against ISIS by attacking its social media accounts and websites. *See* Katie Rogers, *Anonymous Hackers Fight ISIS but Reactions Are Mixed*, N.Y. TIMES (Nov. 25, 2015), https://www.nytimes.com/2015/11/26/world/europe/anonymous-hackers-fight-isis-but-reactions-are-mixed.html.

91. A DDoS attack is when a hacker uses multiple computers under their control to send traffic to a server at a rate faster than the server can handle the traffic, thus denying service to the server's intended customers. *DDoS*, NEWTON'S TELECOM DICTIONARY 349 (25th ed. 2009); *Denial of Service Attack*, NEWTON'S TELECOM DICTIONARY, *supra*, at 357.

92. *See* Solis, *supra* note 21, at 36–37 ("[A] small group of individuals located in California, launched a pre-announced distributed-denial-of-service program against a Pentagon website . . . as a virtual sit-in.").

93. *See* David D. Cole, *Assessing the Leakers: Criminals or Heroes?*, 8 J. NAT'L SECURITY L. & POL'Y 107, 107 (2015).

94. *See* Complaint at 1, United States v. Snowden, No. 1:13-CR-265 (E.D. Va. June 14, 2013); Charlie Savage & Emmarie Huetteman, *Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files*, N.Y. TIMES (Aug. 21, 2013), http://www.nytimes.com/2013/08/22/us/manning-sentenced-for-leaking-government-secrets.html.

to label them as hacktivists because of their motive—to release information to the public in order to disclose what they believed to be immoral or illegal activities by the U.S. government.[95]

B. *Information Taken and Its Potential Uses*

The next factor to analyze when developing a response is the information taken and its potential uses, which is necessary to determine the seriousness of the breach and therefore how severe the response should be. A wide range of information could be stolen from the government, from PII[96] to nuclear codes. The uses of the information will also be dependent on the actor who stole the information.[97] As an example, PII stolen from the government by a cybercriminal would likely be used to make money through identity theft,[98] whereas PII stolen by a terrorist could be used to kill government employees.[99]

Additionally, the government must look at not only who stole the information, but also who could acquire the information. For example, Manning and Snowden both released millions of classified documents.[100] However, the danger is not with Manning or Snowden having the documents but with terrorists or other countries gaining information regarding U.S. security practices.[101]

In addition to items taken directly from the government, items stolen from government contractors should also be considered data breaches against the government warranting a response. One prominent example was the hacking of Lockheed Martin, which resulted in the theft of plans and specifications of the new F-35 aircraft.[102] Data breaches against certain political groups should also be considered as a breach against the government if they have the potential to harm U.S. interests. An example of this would be the hack against the Democratic National Committee, where hacktivists and state actors allegedly attempted to influence U.S.

---

95. Cole, *supra* note 93, at 108.

96. *See* News Release, Office of Pers. Mgmt., *supra* note 31 (explaining that employees and contractors for the federal government had their PII stolen in a cybersecurity incident).

97. *See supra* Section II.A.

98. *See supra* note 85 and accompanying text.

99. *See* CBS NEWS, *supra* note 39; Frantz, *supra* note 77.

100. Cole, *supra* note 93, at 107.

101. *See* Jason Leopold, *Official Reports on the Damage Caused by Edward Snowden's Leaks Are Totally Redacted*, VICE: NEWS (Feb. 25, 2015, 12:30 PM), https://news.vice.com/article/official-reports-on-the-damage-caused-by-edward-snowdens-leaks-are-totally-redacted ("Snowden's actions are likely to have lethal consequences for our troops in the field."). The report that Chairman Rogers was basing this statement on was completely redacted for the media except for subheadings. *Id.*

102. *China's Cyber-Theft Jet Fighter*, *supra* note 28.

elections.[103] Thus, the more sensitive the stolen information is, and more harm it could cause, the more severe the response should be. The assessment should be specific to each breach and the circumstances around it. After the fact-specific analysis, the government should rate the severity as insignificant, negligible, moderate, extensive, or extreme.

IV. POTENTIAL RESPONSES

As stated previously, responses range from kinetic warfare to inaction. These options are themselves at the extremes and should only be used in extraordinary circumstances, even though they seem to be the norm under the current policy—or lack thereof.[104] Other possible responses include criminal prosecution,[105] financial sanctions,[106] diplomatic measures,[107] and counter-breaches.[108] Cybersecurity expert Peter Singer believes the best option for the United States is to build a strong defense.[109] Although having a strong cybersecurity posture is important, it is not a solution for how to respond to cyber intrusions.[110] Cyber defenses are similar to home security: you can have an alarm system, a fence, a dog, and a neighborhood watch, but if someone really wants to break into your home they will still find a way. Instead, having a framework for choosing an

---

103. David Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. TIMES (Oct. 7, 2016), http://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html.

104. *See* Sanger, *supra* note 8 (explaining that the U.S. has deemed they need to respond to China's hack of OPM records, but because of a lack of policy they do not know how or when to do so).

105. *See* Indictment, *supra* note 83, at 1–2 (indicting five Chinese People's Liberation Army hackers for stealing trade secrets from U.S. companies).

106. Carol Morello, *U.S. Sanctions North Korea over Sony Hack*, HOUS. CHRON., Jan. 3, 2015, at A4 (discussing a new Executive Order imposing financial sanctions against North Korea in response to their hacking of Sony).

107. *See* Aaron Burnstein, *Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionage*, 41 ARIZ. ST. L.J. 933, 986–87 (2009) (advocating for countries to openly share information, thus reducing the incentive for cyber espionage); Eckert & Magnowski, *supra* note 65 (explaining the need for diplomatic resolution to escalating cyber conflict).

108. *See* Sanger, *supra* note 8.

109. Symposium, *Talking Foreign Policy: A Discussion on Cyber Warfare*, 47 CASE W. RES. J. INT'L L. 319, 322–23 (2015).

110. *See* Ellen Nakashima, *Cyber Chief: Efforts to Deter Attacks Against the U.S. Are Not Working*, WASH. POST (Mar. 19, 2015), https://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html (quoting Admiral Michael Rogers, Commander of U.S. Cyber Command and Director of the National Security Agency, in his testimony to Congress that offensive cyber capabilities need to be improved for a stronger deterrent effect because "a purely defensive, reactive strategy will be both late to need and incredibly resource-intense").

appropriate response signals to potential hackers that the United States will respond and take action, creating a deterrent effect.[111]

Certain responses to cyber actions may raise questions regarding their legality under international law as well as their authorization under domestic law.[112] The United Nations Charter Article 2(4) states: "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."[113] The question then becomes what, if anything, in the cyber realm is the use of force?[114] The DOD Law of War Manual explains the difficulties of this question:

> [C]yber operations could be a non-forcible means or method of conducting hostilities (such as information gathering), and would be regulated as such under rules applicable to non-forcible means and methods of warfare. Other cyber operations could be used to create effects that amount to an attack and would be regulated under the rules on conducting attacks. Moreover, another set of challenging issues may arise when considering whether a particular cyber operation might be regarded as a seizure or destruction of enemy property and should be assessed as such.[115]

This description exhibits the difficulty in determining what can be

111. *Compare* Sanger, *supra* note 8 ("One of the conclusions we've reached is that we need to be a bit more public about our responses, and one reason is deterrence . . . . We need to disrupt and deter what our adversaries are doing in cyberspace, and that means you need a full range of tools to tailor a response."), *with* Aaron Brantly, *Ambiguous Deterrence*, CYBER DEF. REV. (Jan. 23, 2015), http://www.cyberdefensereview.org/2015/01/23/ambiguous-deterrence/ (confirming claims by high-level officials "that ambiguity of response facilitates deterrence" as accurate).

112. *See generally* Hathaway et al., *supra* note 16, at 841–57 (explaining how cyberattacks fit into the *jus ad bellum* and *jus in bello* frameworks as well as discussing how cyberattacks are governed under non-law of war frameworks); Tyler K. Lowe, *Mapping the Matrix: Defining the Balance Between Executive Action and Legislative Regulation in the New Battlefield of Cyberspace*, 17 SCHOLAR 63, 73–74 (2015) (explaining that Congress has not explicitly authorized cyberwar, but has implicitly authorized Executive Action authority for offensive cyber operations); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 429 (explaining that how a country defines "force" and "aggression" under the U.N. charter is important in determining the legality of cyberattacks).

113. U.N. Charter art. 2, ¶ 4.

114. Many experts have asked and attempted to answer this question. *See, e.g.*, Hathaway et al., *supra* note 16, at 841–57; Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference* (Sept. 18, 2012), *in* HARV. INT'L L.J. ONLINE, Dec. 2012, at 1, 3–4 ("[C]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force." (emphasis omitted)); Waxman, *supra* note 112, at 429.

115. OFFICE OF GEN. COUNSEL, *supra* note 23, at 997 (footnotes omitted).

classified as the use of force.[116] The easy answer is that cyberattacks that result in death or physical destruction are a clear use of force.[117] However, the difficulty is whether cyber actions that do not rise to the level of physical destruction or death can be classified as a use of force.[118]

Whether a cyber intrusion is classified as a use of force under Article 2(4) is important because it establishes whether a country may respond in self-defense.[119] The U.N. Charter allows any country to defend itself against any armed attack,[120] however there is much debate about what level of force equates to an armed attack.[121] The International Court of Justice has claimed that not all uses of force equate to an armed attack, but instead, "it [is] necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[122] Therefore, classifying a cyber operation as a use of force would not automatically allow a country to respond in self-defense under international law.[123]

Certain responses, excluding kinetic force, would still be available to respond to cyber intrusions that constitute force but do not rise to the level of an armed attack.[124] Therefore, the United States would be able to respond in kind if it were a victim to a cyber intrusion.[125] If the act against the United States was not considered a use of force, then the response in kind would also not be considered a use of force.[126] If the original intrusion was a use of force, then the United States would likely be justified in responding with a similar use of force in the cyber realm.[127]

---

116. *See* Waxman, *supra* note 112, at 421–22 (providing several hypothetical cyberattack situations that demonstrate the difficulty in determining which could be classified as a use of force under international law).

117. Antonia Chayes, *Rethinking Warfare: The Ambiguity of Cyber Attacks*, 6 HARV. NAT'L SECURITY J. 474, 507 (2015); *see also* Koh, *supra* note 114, at 3–4.

118. *See* Hathaway et al., *supra* note 16, at 841–57 ("[T]here may be acts that violate Article 2(4)'s prohibition on the use or threat of force that do not rise to the level of an armed attack, and hence do not trigger the right of self-defense under Article 51.").

119. *See* U.N. Charter art. 2, ¶ 4; U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations . . . ."). *But see* Hathaway et al., *supra* note 16, at 841–57.

120. U.N. Charter art. 51.

121. Hathaway et al., *supra* note 16, at 841–57.

122. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 191 (June 27).

123. *See* U.N. Charter art. 2, ¶ 4; U.N. Charter art. 51; Nicar. v. U.S., 1986 I.C.J. at 191.

124. Hathaway et al., *supra* note 16, at 845 & n.109 ("Where they may not resort to defensive force under Article 51 . . . states may be permitted to respond with retorsions or nonforceful countermeasures within carefully proscribed legal limits.").

125. *Id.*

126. *See* U.N. Charter art. 2, ¶ 4

127. *See* Waxman, *supra* note 112, at 434–35.

From a policy perspective, the U.S. government is likely satisfied with a vague international definition of "force" in the cyber context because it allows them to conduct cyber operations of their own.[128]

Essentially, cyber operations under international law can be broken down into three categories: those that do not classify as the use of force, those that are the use of force but not an armed attack, and those actions that constitute an armed attack.[129] Although there are difficulties in determining whether a certain cyber intrusion should be classified as a use of force or an armed attack, the most effective way to classify such actions is to analogize the results to those of conventional actions.[130] To state it differently:

> In order for a [cyber operation] to be considered an armed attack it has to look like one; and the way to tell is by the results of the attack. If the consequences of a [cyber operation] are similar to those that result from an armed attack in its traditional meaning—loss of life or destruction of property, then it is in point of fact an armed attack . . . .[131]

Using this approach to define when a cyber operation can be considered a use of force continues our theme of using effects- and end-state based definitions.[132]

Even if the United States is authorized under international law to conduct retaliatory cyber operations, there is still the debate about whether Congressional approval is needed.[133] A full discussion on which branch of government has the authority to authorize the use of force is beyond the scope of this Note.[134] Although Congress has not expressly provided any authorization for a cyber use of force, Congress did "recognize[] the ability of the Executive Branch to conduct offensive

---

128. *Id.* at 435 ("[W]hile very concerned about U.S. vulnerabilities to [] [cyber] activities and eager to prevent them, U.S. planners may be reluctant to draw boundaries too tight, lest those boundaries impede their own ability to infiltrate and extract information from others' systems . . . ."); *see also* OFFICE OF GEN. COUNSEL, *supra* note 23, at 999; Nakashima, *supra* note 110.

129. Osnat Davidson, *A Legal Analysis of Computer Network Attacks Under International Law*, 3 ISR. DEF. FORCES L. REV. 70, 75 (2008).

130. *Id.* at 81.

131. *Id.* at 79–81.

132. *See supra* notes 19–20 and accompanying text.

133. For a more in-depth look at which branch of government has the power to authorize offensive cyber operations, see Eric Lorber, Comment, *Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?*, 15 U. PA. J. CONST. L. 961, 962–63 (2013).

134. *See generally* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICY 284–86, 373–76 (3d ed. 2006) (explaining the scope of Congressional and Executive power in the War Powers context).

cyber warfare . . . ."[135] Therefore, the Executive Branch likely has the power to retaliate to any cyber intrusion taken against it, even if the original act is not classified as a use of force.[136] We will now look at the different options the government could take: criminal prosecutions, financial sanctions, diplomatic measures, retaliatory countermeasures, or kinetic actions.[137]

A. *Criminal Prosecutions*

Criminal prosecution would only work in limited situations where individual attribution is available and a trial would not implicate U.S. countermeasures.[138] The United States has two primary laws under which it could charge individuals for cyber espionage: the Espionage Act of 1917[139] and the Computer Fraud and Abuse Act (CFAA).[140] The United States has the ability to charge citizens and noncitizens under the Espionage Act of 1917 even if the espionage is committed outside of the United States.[141] Although cyber espionage is not directly referenced in the act, the law's applicability can be inferred through the broad definition of espionage.[142]

The CFAA is even more applicable to these types of actions, as "cyberexploitation was a focus of the act."[143] The CFAA, although originally designed to protect government computers from unauthorized access,[144] makes it a felony to access a computer without authorization, or in excess of authorization, to obtain government information.[145] Although, there has never been any ruling on whether the CFAA could

---

135. Lowe, *supra* note 112, at 73 (quoting the National Defense Authorization Act for Fiscal Year 2012: "Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests . . . .").

136. Lowe, *supra* note 112, at 74.

137. The sixth option the government could take, and often does take, is to do nothing. However, this option requires no explanation.

138. Sanger, *supra* note 8 ("Intelligence officials say that any legal case could result in exposing American intelligence operations inside China . . . ."); *see also* SINGER & FRIEDMAN, *supra* note 14, at 72–80 (explaining the problem of attribution in the cyber context).

139. Pub. L. No. 65-24, 40 Stat. 217 (codified as amended at 18 U.S.C. §§ 792–99 (2012)).

140. Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030); *see also* Pelican, *supra* note 25, at 374–76. For a more detailed background on the CFAA, see Trace Jackson, Note, *Can Jailbreaking Put You in Jail, Broke?*, 68 FLA. L. REV. 631 (2016).

141. *See* United States v. Zehe, 601 F. Supp. 196, 198 (D. Mass. 1985).

142. *See* 18 U.S.C. § 794 (inferring cyber espionage to fall under the act of "communicates, delivers, or transmits").

143. Pelican, *supra* note 25, at 376 (citing 18 U.S.C. § 1030(a)(1), (d)(2)).

144. Jackson, *supra* note 140, at 635.

145. 18 U.S.C. § 1030.

be applied to actions committed abroad,[146] the USA PATRIOT Act of 2001[147] amended several criminal statutes to allow for extraterritorial applicability to cyber actions against the United States from abroad.[148]

Although criminal charges are available to known hackers, there are many issues that complicate this response.[149] First, there is the issue of extraditing the alleged hackers to the United States for trial.[150] Since it is likely the individuals the United States would want to prosecute for data breaches are from countries who are not friendly to us, it is unlikely that those countries would be willing to extradite their citizens.[151] Even countries that have extradition treaties may be unlikely to extradite individuals, just as Hong Kong refused to extradite Edward Snowden before he left there for Russia.[152]

Second, a trial could potentially involve the United States having to prove how the foreign adversary bypassed security and stole the information.[153] This could result in the publication of the United States' security protocols as well as tactics that worked for the defendant—both are items that should not be made public.[154]

Although criminal prosecutions for corporate espionage have been successful, criminal prosecutions for cyber espionage against the U.S. government are more difficult to establish.[155] In May 2014, the

146. Pelican, *supra* note 25, at 376 (citing 18 U.S.C. § 1030(a)(1), (d)(2)).

147. Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

148. 18 U.S.C. § 1030; Hathaway et al., *supra* note 16, at 875 ("The statute banning computer fraud was likewise amended as part of the USA PATRIOT Act to provide for extraterritorial applicability.").

149. *See supra* notes 138–45 and accompanying text.

150. *See* Paul Mozur, *China Questions Evidence Used in U.S. Cybercrimes Indictment*, WALL ST. J. (May 29, 2014, 12:03 PM), http://www.wsj.com/articles/chinas-defense-ministry-questions-evidence-used-by-u-s-to-indict-five-peoples-liberation-army-officers-for-cybercrimes-1401359575 (explaining how the Chinese government refuses to accept responsibility for the alleged hacking and that the United States commits the same acts).

151. *See* 31A AM. JUR. 2D *Extradition* § 14, Westlaw (database updated Aug. 2015) (explaining that an extradition treaty is required between two countries in order for either country to be able to extradite potential defendants).

152. Eleni Himaras et al., *Snowden Lands in Moscow as Hong Kong Rejects U.S. Warrant*, BLOOMBERG (June 23, 2013, 11:26 AM), http://www.bloomberg.com/news/articles/2013-06-23/snowden-leaves-hong-kong-as-u-s-seeks-his-extradition.

153. *See* Sanger, *supra* note 8.

154. In almost every section, the CFAA has the element of "access[ing] a protected computer without authorization." 18 U.S.C. § 1030 (2012). Unless the defendant were to stipulate this element of the crime, the prosecution would have to prove that they knew the particular defendant accessed the protected computer. *Id.* This would likely result in the U.S. disclosing how they were hacked, potentially creating a blueprint for others to emulate.

155. *See* Sanger, *supra* note 8 ("Intelligence officials say that any legal case could result in exposing American intelligence operations inside China . . . .").

Department of Justice indicted five Chinese People's Liberation Army hackers for stealing trade secrets from various U.S. companies.[156] This was the first time the U.S. government had indicted known state hackers for trade secret theft.[157] However, if the actor is acting on behalf of a foreign government and is stealing government information, then it is no longer trade secret theft but is instead a form of government espionage.[158] Espionage is generally held not to be a violation of international law, but rather is a violation of the target country's laws.[159] Criminal prosecution against state actors is a risk because it is likely the United States is conducting similar actions against that nation, and therefore the other nation could reciprocate the charges.[160]

Hacktivism, on the other hand, is a type of data breach that can be deterred through criminal prosecution. The United States has sought to bring criminal charges against individuals who released classified government information—most notably Chelsea Manning and Edward Snowden.[161] Although these two cases were situations where the perpetrator already had access to the information and did not illegally obtain access,[162] the penalties would have been more severe for someone who, in addition to illegally releasing classified documents, did so by illegally obtaining access to them.[163] Cyber criminals could also be deterred through criminal prosecution. The CFAA and domestic theft laws could be used to prosecute cyber criminals who breach government systems.[164]

Criminal prosecutions could be used against terrorists. However, this approach would likely only work for those who support terrorists groups from within the United States.[165] Therefore, criminal prosecutions seem to work best only if the actor is a hacktivist or cyber-criminal, based in the United States or a country that has an extradition treaty with the

156. Indictment, *supra* note 83, at 1–2.

157. Press Release, U.S. Dep't of Justice, *supra* note 83.

158. *See* 70 AM. JUR. 2D *Sedition, Etc.* § 13, Westlaw (database updated Aug. 2015).

159. *See* Pelican, *supra* note 25, at 369–70 (concluding after analysis of various legal scholars' views, that peacetime espionage is not a violation of international law).

160. Sanger, *supra* note 8.

161. *See* Complaint, *supra* note 94, at 1; Savage & Huetteman, *supra* note 94.

162. *See* Cole, *supra* note 93, at 108 (describing the leaks by Manning and Snowden as "unauthorized disclosure[s] of classified information").

163. Manning was sentenced to 35 years for charges of violating the Espionage Act. Savage & Huetteman, *supra* note 94. Her sentence could have been even greater if she had additionally been charged with violations of the Computer Fraud and Abuse Act. 18 U.S.C. § 1030 (2012).

164. *See supra* notes 138–45 and accompanying text.

165. The United States has a robust counterterrorism task force, but often lacks the ability to capture or extradite terrorists who commonly operate from the Middle East and Africa.

United States, and the trial would not involve the further disclosure of sensitive information.[166]

B. *Financial Sanctions*

A second option for the United States would be the use of economic and financial sanctions against the perpetrators. Economic sanctions have the objectives of behavior modification, retribution, or deterrence.[167] The purposes behind sanctions as a response to data breaches would primarily be behavior modification and deterrence.[168] Specifically, sanctions would be used to modify the behavior of the target of the sanctions and to deter other actors from acting similarly.[169] Although behavior modification and retribution are commonly overlapping results of economic sanctions, it is important to state the objective as behavior modification because the United Nations has "denounced the use of economic sanctions for retributive purposes."[170] Several studies on the effectiveness of economic sanctions have concluded that they do not achieve their desired goal.[171] However, many of these studies have only looked at the stated objective of the sanctions and did not look at other effects the sanctions had, which are commonly effective in producing a desirable outcome for the imposing country.[172]

The United States draws its international authority for economic sanctions from the powers vested in the U.N. Security Council.[173] Domestically, the Commerce Clause of the Constitution grants Congress the power to "regulate Commerce with foreign Nations."[174] The primary

166. An example of where criminal prosecution worked was with Manning, who was a U.S. citizen and soldier in Iraq when arrested. Savage & Huetteman, *supra* note 94. However, the deterrent effect of Manning's prosecution was short lived when, during his last week in office, President Obama commuted Manning's sentence. Charlie Savage, *Chelsea Manning to Be Released Early as Obama Commutes Sentence*, N.Y. TIMES (Jan. 17, 2017), https://www.nytimes.com/2017/01/17/us/politics/obama-commutes-bulk-of-chelsea-mannings-sentence.html.

167. KERN ALEXANDER, ECONOMIC SANCTIONS: LAW AND PUBLIC POLICY 10 (2009).

168. *See id.*

169. Nicholas Wolfe, *Nuclear Chain Reaction: Why Economic Sanctions Are Not Worth the Public Costs*, 27 FLA. J. INT'L L. 1, 4–5 (2015).

170. *Id.* (citing G.A. Res. 51/242, annex II, Supplement to an Agenda for Peace, ¶ 4 (Sept. 26, 1997)).

171. ALEXANDER, *supra* note 167, at 34–35.

172. *Id.* at 34–36 ("The measure of the effectiveness of economic sanctions therefore should not necessarily be assessed in terms of whether they achieve their stated objectives, which may be only aspirational, but rather should be assessed in terms of whether they perform other functions, such as communicating to other states and to supportive and opposing groups, or merely imposing economic costs on the targets in retribution for particular acts or policies.").

173. G.A. Res. 51/242, *supra* note 170, ¶ 1.

174. U.S. CONST. art. I, § 8, cl. 3.

laws authorizing economic sanctions against countries are the Trading With the Enemy Act of 1917, the International Emergency Economic Powers Act of 1977, and the Export Administration Act.[175] Following September 11, 2001, the United States implemented several laws and programs that place financial sanctions on terrorist groups and their backers.[176] This operation is now carried out by the Treasury Department's Office of Foreign Assets Control (OFAC), whose mission is to "administer[] and enforce[] economic and trade sanctions based on U.S. foreign policy and national security goals."[177]

Economic sanctions as a response would primarily be limited to state actors and terrorists. If used as a response against nations, this option would likely be more symbolic for larger countries but a beneficial deterrent for smaller countries.[178] Additionally, this option would not be beneficial against countries who are larger trade partners with the United States, because the sanctions could create economic losses for the United States.[179] Additionally, several scholars have criticized economic sanctions because they do more harm to the civilians of the target country than they benefit the sanctioning country.[180] However, as stated previously, economic sanctions have been successful in achieving beneficial objectives.[181]

Economic sanctions can also be used as a response to data breaches by terrorist organizations. Since 2001, OFAC has seized assets and frozen accounts globally as a method of combatting terrorist financing.[182] Although the United States and its allies have sought to freeze financial accounts for suspected financiers of terrorism, these tactics have been criticized[183] and have become less effective as terrorist organizations diversify their revenue streams.[184] Additionally, as terrorist organizations

175. ALEXANDER, *supra* note 167, at 92.

176. *See id.* at 278.

177. *About: Office of Foreign Assets Control (OFAC)*, U.S. DEP'T TREASURY, https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx (last updated Oct. 14, 2016).

178. *See* NAT'L SEC. & INT'L AFFAIRS DIV., U.S. GEN. ACCOUNTING OFFICE, GAO/NSAID-92-106, ECONOMIC SANCTIONS: EFFECTIVENESS AS TOOLS OF FOREIGN POLICY 9 (1992).

179. *Id.* at 14 (explaining that sanctions raise the cost of commerce for both the target of the sanctions and the sanctioning nation).

180. Wolfe, *supra* note 169, at 12–13.

181. ALEXANDER, *supra* note 167, at 10.

182. *Id.* at 283–84.

183. *See* NICHOLAS RYDER, THE FINANCIAL WAR ON TERRORISM: A REVIEW OF COUNTER-TERRORIST FINANCING STRATEGIES SINCE 2001, at 84 (2015) (claiming that the ability to freeze the assets of terrorist supporters "is an ineffective response" and is politically motivated to make it appear as though the government is doing something to combat terrorism).

184. *See* Ana Swanson, *How the Islamic State Makes Its Money*, WASH. POST: WORKBLOG (Nov. 18, 2015), https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-

become more technologically advanced, stopping their funding has become more difficult.[185] Regardless of the difficulties, this option should still be used to combat terrorist hacking. Overall, this option is best suited as a deterrent for small countries and to limit the effectiveness of terrorist organizations.

C. *Diplomacy*

The third option available to the United States against hackers who steal government information is diplomatic measures. This response encompasses a wide variety of options: open sharing to reduce the incentive for cyber intrusions,[186] agreements with countries that define the acceptable scope and limits for cyber espionage,[187] and treaties and international cooperation that dictate acceptable actions in the cyber realm.[188] The issue with most of the diplomatic measures is that they do nothing to punish past offenders. Certain activities, such as direct agreements with other countries, are beneficial if the country has an incentive to cooperate with the United States, as many smaller and developing countries do. However, if the country denies conducting any type of cyber breach and does not need financial incentives from the United States, i.e., China and Russia, then these agreements will not work.[189]

The current trend is for international cooperation to develop baseline security measures for groups of nations where there is a mutual need for

---

its-money/ (explaining how Daesh has avoided having its funding shut down through international financial freezes by diversifying its revenue stream through the sale of oil, taxation and extortion in the areas it controls, ransom from kidnapping, sales of antiquities, seizures of Iraqi banks, sales of looted property, sales and rentals of real estate previously owned by people it has killed, agriculture, and sale of minerals).

185. *See* Aaron Brantly, *Financing Terror Bit by Bit*, COMBATING TERRORISM CTR. SENTINEL, Oct. 2014, at 1, 1–4; *Hacktivists Claim ISIS Terrorists Linked to Paris Attacks Had Bitcoin Funding*, NETWORKWORLD (Nov. 15, 2015, 9:37 AM), http://www.networkworld.com/article/3005308/security/hacktivists-claim-isis-terrorists-linked-to-paris-attacks-had-bitcoin-funding.html.

186. *See* Burnstein, *supra* note 107, at 986–87 (advocating for countries to openly share information, thus reducing the incentive for cyber espionage).

187. Eckert & Magnowski, *supra* note 65 (explaining the need for diplomatic resolution to escalating cyber conflict).

188. *See* Chayes, *supra* note 117, at 510 & n.130; *see also* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 92 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

189. *See* Simon Denyer, *China Calls U.S. Hacking Accusations 'Irresponsible and Unscientific*,*'* WASH. POST (June 15, 2015), https://www.washingtonpost.com/world/asia _pacific /china-calls-us-hacking-accusations-irresponsible-and-unscientific/2015/06/05/7989cad3-583f-417e-a0b7-34be46eb16ff_story.html.

protection.[190] These measures are beneficial in improving security across cooperating countries, but like in the last proposal, they do little to deter larger perpetrators in the absence of mutual gain.[191] The North American Trade Organization (NATO) has taken steps in the right direction by creating the Tallinn Manual.[192] Although it is not completely binding on member states, the Tallinn Manual sets forth rules governing cyber operations in the international context.[193] Additionally, international agreements would do little if there were no enforcement mechanisms built in.[194] Although baseline security measures would be beneficial for organizations like NATO and the European Union, they are methods to prevent breaches, not respond to them.

Some scholars have also called for the regulation of offensive cyber weapons.[195] However, these measures do not seem realistic in light of the current buildup of cyber arms by most of the world's more powerful countries.[196] The buildup of offensive cyber weapons has been compared to the buildup of nuclear weapons in the Cold War era.[197] This has led scholars to conclude that similar arms reduction agreements are necessary.[198] Although such agreements would be beneficial to demonstrate internationally the acceptable use of offensive cyber weapons, an important aspect of effective nuclear arsenal reduction agreements was the ability to inspect a nation's compliance—a vital element that would be completely lacking in the cyber realm.[199] Overall, treaties and international cooperation could be beneficial to help develop custom among nations as to what is acceptable, however they are not an effective response to cyber breaches that have already occurred.

A diplomatic measure that should be taken in response to cyber intrusions is public reprimand. This would include actions such as

190. Chayes, *supra* note 117, at 510–12.

191. *Id.* at 517.

192. *See* TALLINN MANUAL, *supra* note 188, at 1.

193. *Id.* at 6. The Tallinn Manual sets forth rules governing cyber warfare based on its interpretation of existing international law. *Id.* at 1–4. Therefore, the Independent Group of Experts, the authors of the rules, state that "[t]o the extent that the Rules accurately articulate customary international law, they are binding on all States." *Id.* at 6. Although this is correct in the sense that any international treaty ratified by a state is binding on that state, these rules are based on interpretations of treaties as they apply to the cyber realm and have not been ratified by the U.S. Senate. Thus, they are not binding law on the United States.

194. Chayes, *supra* note 117, at 513–15.

195. *Id.* at 517–19.

196. *See id.* at 515 & n.158.

197. Symposium, *supra* note 109, at 328.

198. Chayes, *supra* note 117, at 517–19.

199. *Id.* (stating that a Code of Conduct for states in the cyber realm would be beneficial in developing acceptable social customs as nuclear reduction treaties did, but also stating that those agreements relied on verification for effectiveness).

summoning the ambassador of a foreign country, or even outing diplomats. These actions would primarily be symbolic, but could have some deterrent effect. These actions would only be effective against state actors.

D. *Retaliatory Countermeasures*

Another approach that the United States could take in response to cyber intrusions is retaliatory countermeasures. These measures include a range of activities from stealing similar information from the perpetrator to destroying or degrading networks. [200] This approach is likely the most nuanced. It requires the United States to commit acts that it does not want committed against itself.[201]

Positives of this approach are its deterrent factors. If other countries know that stealing data from government is going to result in similar actions against them, they may refrain from doing so.[202] Additionally, if terrorists, criminals, or hacktivists know that the United States is going to respond to their data breaches with cyber actions, they may be less likely to take the action in the first place.[203] However, the deterrent only works against state actors if the other country believes that the United States is not already conducting such activities, and that the United States would not conduct breaches unless it was first breached.[204] Additionally, the deterrent only works if the other country knows that the United States has taken retaliatory action,[205] which the United States may not want to announce for fear of bad publicity or disclosing vulnerabilities in the other nation's cyber defenses.

Nonetheless, countermeasures can be an effective response against nations when the information stolen is damaging but not catastrophic. An example would be the PII stolen in the OPM hack.[206] The United States could steal similar data from the Chinese government and use that information to deter the Chinese from stealing more personal data or from using the data they already stole. This type of action would be acceptable

200. *See* Sanger, *supra* note 8.

201. *See* OFFICE OF GEN. COUNSEL, *supra* note 23, at 999.

202. *See* Nakashima, *supra* note 110.

203. For an example of the United States responding to hacktivists with a cyberattack, see Solis, *supra* note 21, at 36–37.

204. Denyer, *supra* note 189 (citing Chinese state news agency Xinhua, which pointed to the Edward Snowden leaks as proof that the U.S. government "appl[ied] double standards and ma[de] unfounded accusations against China").

205. *See* Nakashima, *supra* note 110 (quoting Maine Senator Angus King as stating that the United States needs an offensive cyber capability and that the capability needs to be publicized for it to be an effective deterrent).

206. Davidson, *supra* note 27.

under international law as either a form of espionage[207] or as a proportionate countermeasure.[208] Retaliatory countermeasures would work best when the perpetrator is a state actor who stole information that is not directly related to vital national security. When conducting countermeasures against state actors, the United States should strive to ensure that the countermeasures are proportionate and not escalatory.[209]

These measures can also be effective against other types of actors such as terrorists, criminals, and hacktivists.[210] However, with respect to criminals and hacktivists, criminal prosecution is a better response because the U.S. government should not be conducting cyber intrusions or attacks against individuals—the criminal justice system is in place to deal with law breakers. Terrorists, on the other hand, should face continuing cyber action by the United States because they pose a threat to U.S. security, and offensive cyber operations, should not be left unused in defending against terrorism.[211]

E. *Kinetic Responses*

The last, and most severe, action the United States could take in response to a cyber intrusion would be to use kinetic force. This response should be seen as a last resort and should be limited to use against terrorists, or states that have stolen information damaging to national security. The use of force should follow the principles of distinction, necessity, and proportionality.[212] Distinction refers to the ability to direct the effects of an attack against combatants and not civilians.[213] Proportionality is the concept that a country should respond to hostilities in a manner that is proportional. This does not necessarily refer to the quantity or type of acts taken, but instead refers to the effects of the act

207. Espionage is generally not held as a violation of international law since most countries actively conduct espionage against other nations. OFFICE OF GEN. COUNSEL, *supra* note 23, at 999. Instead acts of espionage are punishable under domestic laws of the victim country, meaning it would be unlikely for anyone to actually face criminal detention for such acts. *See* Indictment, *supra* note 83, at 1–2 (indicting members of the Chinese People's Liberation Army for violating the United State's Computer Fraud and Abuse Act). Note, however, that this indictment was only pursued because the hackers stole trade secrets and were not charged with espionage.

208. TALLINN MANUAL, *supra* note 188, at 36–41 (explaining the different sources of international law that govern countermeasures).

209. *See id.*

210. *See* Solis, *supra* note 21, at 36–37.

211. U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member . . . .").

212. Davidson, *supra* note 129, at 91; *see* TALLINN MANUAL, *supra* note 188, at 36–41.

213. Davidson, *supra* note 129, at 91.

taken.[214] Necessity refers to the concept that any amount of force in excess of what is needed to accomplish the mission is unlawful.[215]

If the principles of distinction, necessity, and proportionality were followed, there would be very few situations where a cyber intrusion by a state actor would warrant a kinetic response. Additionally, kinetic responses should not be used against criminals or hacktivists, as doing so would violate the Fifth and Fourteenth Amendments of the U.S. Constitution.[216] However, kinetic force is acceptable as a response to terrorist data breaches if such breaches create a threat to national security or U.S. citizens.[217] The example used previously in this Note of Junaid Hussain is a situation where kinetic force was an acceptable response to a breach by a terrorist.[218] In that instance Hussain, a known terrorist, stole and published personal information of military personnel.[219] Publishing personal information online on its own was not enough to justify kinetic force. However, Hussain called for lone wolves to kill the service members whose information he had just released, escalating the breach to a level warranting kinetic force, as it posed a threat to American lives.[220] Therefore, kinetic force should be reserved as a response to data breaches for situations where national security is threatened or American lives are jeopardized.

CONCLUSION

In order to limit future data breaches against government systems, the government must have a policy in place to respond to such actions. The types of responses analyzed in this Note create a continuum for the government, ranging from doing nothing to using violence. The decision-making process is to first identify the actor, then determine what was stolen, next analyze the potential uses of the information stolen, and lastly initiate a response. Figure 1, above, depicts the decisional matrix for determining the appropriate actions to take. The decision matrix assists in choosing an appropriate response to data breaches by analyzing the severity of the information taken and the type of actor that stole the information. Based on this information, a range of appropriate responses is presented.

---

214. TALLINN MANUAL, *supra* note 188, at 36–41.

215. OFFICE OF GEN. COUNSEL, *supra* note 23, at 54–58.

216. U.S. CONST. amends. V, XIV.

217. *But see* John Reed, *Questions the Media Should Be Asking About DOD's Latest Targeted Killing*, JUST SECURITY (Sept. 1, 2015, 10:40 AM), https://www.justsecurity.org/25729/questions-media-dods-latest-targeted-killing/ (questioning what information is required to "land" someone on the targeted kill list).

218. *See supra* Section I.B.

219. CBS NEWS, *supra* note 39.

220. De Freytas-Tamura, *supra* note 1.

Although this decisional framework does not give the exact action to take for every type of data intrusion against the government, it does create the basis for a policy that government decision makers can act upon. Therefore, this decision-making process would not only make government responses easier, but would also send a message to potential hackers that something will be done if they hack the United States. This matrix is merely a tool for the government to use. The consequences of each action, as outlined above, make picking the "correct" response difficult. The lack of perfect information to aid decision makers is only compounded in the cyber realm, where it is easy for anyone to mask who they are, where they come from, when they committed the breach, and their intentions for doing so. Gathering the information needed to determine the inputs for the decision matrix may well be the most difficult aspect of implementation. However, difficulty in this determination should not result in a lack of policy—something must be done and this is a start.