IF A TREE FALLS IN CYBERSPACE, IS ANYONE HURT BY IT? EVALUATING INTERNATIONAL CYBERSECURITY IN LIGHT OF THE PSYCHOLOGICAL EFFECTS OF CYBER INTRUSIONS

Sam Renshaw

INTRODUCTION

Robert Morris created the first computer worm in the late 1980s and put the world on notice of the need for stronger cybersecurity infrastructure.[1] Since then, cyber intrusions have become extremely advanced.[2] These advancements have resulted in an increased likelihood of cyber intrusions for entities of all sizes.[3] Cyber intrusions have a psychological impact on their victims, and legal regimes are continually evolving to meet these threats.

Within existing legal regimes, the term "cybersecurity" varies greatly in meaning between nations with different views of the internet and different levels of reliance upon it. Within international law, there are important distinctions between cybercrime, cyberespionage, and cyberattacks, which can lead to different legal consequences. Currently, the Convention on Cybercrime is in place to address cybercrime, but not necessarily cyberespionage or cyberattacks.[4]

Types of cyberespionage are distinguished by the purpose of the espionage.[5] Cyberattacks come in many forms but often stand alone, work alongside conventional warfare, or are used alone but result in kinetic

---

[1] JEAN LEHMANN, INTRODUCTION TO CYBERSECURITY 11 (YOUPublish 2016).

[2] *Id.* at 13.

[3] *Id.* "Organisations are constantly at threat, and it is very difficult to be 100% sure of preventing an attack, since new types of attack are being developed and attacks are evolving in sophistication."

[4] *See* Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13174, E. T.S. No. 185 (discussed *infra* in Part II (D)).

[5] Cyberespionage is most often divided based on whether the purpose was for economic or political gain. Sometimes, these motives overlap.

violence.[6] These cyber intrusions have an adverse effect on people and society as a whole.[7] As a result, psychologists within organizations have developed ways for entities and individuals to better prepare for cyber threats.[8] Additionally, existing treaty organizations have adapted to meet cyber threats.[9] Finally, "cyberpsychology" can be used to inform public policy and "nudge" users to adopt more secure behaviors.

I. INTERNATIONAL CYBERSECURITY LAW

The legal issues surrounding cybersecurity are full of asymmetries. These include freedom of information versus cybersecurity and the distinctions between cyberespionage and cyberattacks. There are also important questions concerning whether and when self-defense can be used in response to a cyberattack.[10]

A. *Freedom of Information v. Cybersecurity*

There is no international consensus on how the laws of armed conflict should apply to cyberwarfare.[11] Both definitional and cultural differences

---

[6] Kinetic violence and kinetic effects involve "physical damage or destruction." Stephanie Gosnell Handler, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, 48 STAN. J. INT'L L. 209, 210 (2012). Kinetic violence has long been used to determine if military operations meet the level of an armed attack under the international law of armed conflict. Existing scholarship on cyberwarfare "focuses predominantly on cyberattacks committed in the absence of conventional operations," and scholars pay particular attention to kinetic effects directly caused by cyberattacks. *Id.*

[7] *Id.*

[8] Rachel C. Dreibelbis et al., *The Looming Cybersecurity Crisis and What It Means for the Practice of Industrial and Organizational Psychology*, 11 INDUS. AND ORGANIZATIONAL PSYCH. 346, 348 (2018).

[9] *Increasing International Cooperation in Cybersecurity and Adapating Cyber Norms*, COUNCIL ON FOREIGN RELATIONS (Feb. 23, 2018), https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

[10] Andrew Davies, *An Australian Perspective on ANZUS and Cyberthreats*, *in* 46 SPECIAL REPORT: ANZUS 2.0, CYBERSECURITY AND AUSTRALIA-US RELATIONS, 3, 5 (Australian Strategic Policy Institute) (2012).

[11] Jessica R. Herrera-Flanigan, *Cybersecurity: Legal and Normative Issues*, *in* SPECIAL REPORT: ANZUS 2.0, CYBERSECURITY AND AUSTRALIA-US RELATIONS 17, 18 (Australian Strategic Policy Institute, 2012).

contribute to the challenges of formulating a uniform global solution to cyber threats.[12] The challenges in defining cybersecurity spring from the cultural differences between Western democracies such as the United States and other nations such as Russia and China.[13] Western democracies agree that cybersecurity should focus on creating an "interoperable, secure and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[14] The approach advocated for by Russia and China stands in contrast to that of Western democracies.[15] Russia and China, among others, define cybersecurity "in terms of controlling content, communications and social networking tools in a manner that does not undermine nations' cultural, political, economic and social stability."[16]

---

[12] *Id.* In a 2011 U.S.-Australia AUSMIN Joint Statement on Cyberspace, the statement "appears to treat cyberattacks in the same fashion as a bombing or assault." *Id.* However, Russian proposals mirror actions taken in the area of weapons of mass destruction. *Id.* This "cyberarms control" would commit States "to abstaining from developing offensive cybercapabilities or from engaging in cyberespionage." *Id.*

[13] *Id.* at 17.

[14] *Id.* "Under such an approach, protecting systems against damage and compromise and assuring reliability is coupled with promoting intellectual property protections, human rights and privacy." *Id.*

[15] *Id.*

[16] *Id.* Russia and China, joined by Tajikistan and Uzbekistan, proposed to the United Nations an International Code of Conduct for Information Security. *Id.* The Code of Conduct would require nations to pledge:

> To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment.

Annex to the Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Fed'ns, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, International Code of Conduct for Information Security, ¶ 2(c), U.N. Doc. A/66/359 (Sept. 14, 2011). An updated letter and Code of Conduct have been submitted by these same countries with the addition of Kazakhstan and Kyrgyzstan joining in support. Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Fed'ns, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, U.N. Doc. A/69/723 (Jan. 13, 2015).

These two conflicting views place different weight on internet liberty and internet sovereignty.[17] These differences will continue to persist as long as some governments continue to see freedom of information as a threat to their societal norms or until Western democracies are willing to make compromises that legitimately recognize other nations' concerns. Despite guidelines created by international organizations, finding global consensus on cyber issues is a difficult challenge.[18]

B. *Cyberespionage v. Cyberattacks*

An important distinction within cybersecurity is the difference between cyberattacks and cyberespionage. Cyberespionage is "the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor."[19] A cyberattack is an offensive cyberspace operation that rises to the level of an armed attack.[20] There is a simple test to determine if an action in cyberspace is an attack or espionage: if the cyber intrusion is merely collecting information, then it is cyberespionage.[21] However, this simple test

[17] Herrera-Flanigan, *supra* note 11, at 17. These opposing views create "an inherent conflict between promoting internet liberty and assuring internet sovereignty." *Id.*

[18] *See id.* ("Reaching a consensus on cybersecurity will be one of the most difficult global policy issues facing nations collectively in the coming years."). One example of proposed guidelines is the Organization for Economic Co-operation and Development's *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. *Id.* at 19 (citing OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD Council, 1037th Sess. (July 25, 2002), http://www.oecd.org/sti/ieconomy/15582260.pdf).

[19] David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 370-71 (2013) (quoting Kevin G Coleman, *Cyber Espionage Targets Sensitive Data*, SIP TRUNKING (Dec. 29, 2008), http://sip-trunking.tmcnet.com/topics/security/articles/47927-cyber-espionage-targets-sensitive-data.htm).

[20] Handler, *supra* note 6, at 212. The term "cyberattack" is also used as "an umbrella term to describe offensive cyberspace operations that include both criminal activities and attacks that fall under the law of war." *Id.*

[21] Weissbrodt, *supra* note 19, at 372.

grows complex in application because computer codes for information-collecting programs can be similar to more malicious programs.[22]

Traditional espionage does not rise to the level of a use of force under the U.N. Charter.[23] By analogy, cyberespionage is also not a use of force under international law.[24] While every cyber intrusion cannot be labeled an attack, it is important to assess whether an intrusion exploited a network vulnerability that could be used in future, more malicious intrusions.[25]

In addition to the necessary distinctions drawn between cyberattacks and cyberespionage, there is a question of aggregation: "whether at some point the level of crime and espionage in cyberspace or the cumulative effect becomes a threat to national security."[26] The aggregation question is complicated because many points of access used in cyberespionage are also places from which an attack could be launched.[27] Further, non-state actors—who may or may not be encouraged by a state—can act as proxy forces and "blur" threats from other nations.[28] These factors cause some to assert that cyberespionage deserves more severe treatment than traditional espionage.[29]

---

[22] *See id.* ("[I]t is often difficult to determine from the computer code alone whether . . . [the] objective is merely the collection of information, or something more malicious, since both can use similar technology.").

[23] *Id.* at 371.

[24] *See* Lydia Khalil, *Conclusion*, *in* SPECIAL REPORT: ANZUS 2.0, CYBERSECURITY AND AUSTRALIA-US RELATIONS 28, 29 (Australian Strategic Policy Institute) (2012) ("To label an act of [cyber]espionage as an attack and therefore a potential precursor for an armed response is a major departure from accepted international practices.").

[25] *See id.* ("The same . . . method that's used to extract information from a network can also be exploited to conduct an attack to disrupt that network. This is a critically important distinction that policymakers must be aware of and account for.").

[26] James Lewis, *US Perceptions of Cyberthreats*, *in* SPECIAL REPORT: ANZUS 2.0, CYBERSECURITY AND AUSTRALIA-US RELATIONS 10, 11 (Australian Strategic Policy Institute) (2012).

[27] *Id.*

[28] *Id.*

[29] Weissbrodt, *supra* note 19, at 371. However, this is a minority opinion. *Id.* at 372.

The Flame virus is an example of malicious software that effectuated cyberespionage.[30] In May 2012, the Kaspersky Lab in Moscow, Russia, disclosed the discovery of the Flame virus.[31] Analysts of the Flame virus determined that its primary objective was information collection.[32] Further, the virus's complexity implied that it was created by a state government.[33] Because the program collects only information, it is cyberespionage.[34] "If the cyber-spies responsible . . . were ever apprehended they could be prosecuted for espionage in any of the [S]tates where Flame collected information," but the program would not constitute a cyberattack.[35]

C. *Self-Defense and Cyberattacks*

There is debate on whether a State's aggressive use of cyberspace against another State could justify self-defense under the U.N. Charter.[36] Article 2(4) states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[37] However, States retain the right to self-defense under Article 51.[38] Further, the International Court of Justice stated, in an advisory opinion, that these provisions of the U.N. Charter "do

---

[30] A virus is "a computer program that has the ability to self-replicate, without the user of the system that it is operating in having given permission." LEHMANN, *supra* note 1, at 5.

[31] Weissbrodt, *supra* note 19, at 352.

[32] *See id.* at 352-53, 380 (providing a non-exhaustive list of information the software collects ranges from "computer display contents, documents, stored files, password information, contact data, audio conversations, and monitoring of Skype.").

[33] *See id.* at 383 (concluding that the virus was "nearly sixty times the average size of other known malicious programs" and "most of the infected computers were in the Middle East.").

[34] *Id.* at 380.

[35] *Id.*

[36] In May 2011, the United States' discussion of cybersecurity "include[d] the statement that 'certain aggressive acts in cyberspace' coming from another country might justify the invocation of the right of self-defense under the U.N. Charter." Davies, *supra* note 10, at 5.

[37] U.N. Charter art. 2, ¶ 4.

[38] *See* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.").

not refer to specific weapons. They apply to *any* use of force, regardless of the weapons employed."[39]

The interpretation of "armed attack" when applied to cyberspace is key to determining whether Article 51 will allow a State to exercise self-defense. Conventional weapons and attacks causing damage to "physical or real property or injury or death to humans" are considered to be a use of force under the U.N. Charter.[40] However, not every use of force rises to the level of an armed attack.[41] On the other end of the spectrum, economic and political coercion cannot be a use of force.[42] If a cyberattack occurs, but the action does not rise to the level of an armed attack, the victim state may only take non-forceful actions in response.[43] If the victim state suffers a cyberattack that *does* meet the level of an armed attack, then the state can respond with a use of force so long as it meets the requirements of necessity, proportionality, and immediacy.[44]

A strict reading of "armed attack" prohibits use of force in self-defense reactions to cyberespionage, but actions such as economic sanctions would be appropriate.[45] Article 51 also likely precludes self-defense in response to denial-of-service attacks.[46] A strict textual view would read

---

[39] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8) (emphasis added).

[40] Weissbrodt, *supra* note 19, at 358.

[41] An example of this can be found in the case of *Nicaragua v. United States of America*, in which the ICJ found that the laying of mines by the United States in the territorial waters of Nicaragua constituted a use of force, but that use of force did not rise to the level of an armed attack. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

[42] Weissbrodt, *supra* note 19, at 358. ("[I]nternational law has established that economic and political coercion are expressly excluded from the definition of the use of force . . .").

[43] *Id.* at 362.

[44] *Id.* at 364.

[45] *Id.* at 382.

[46] Matthew C. Waxman, *Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INT'L L. STUD. 109, 111 (2013). A denial of service attack floods a server or website with internet traffic "in order to overload digital systems and take them offline." LEHMANN, *supra* note 1, at 14. These attacks "often serve as a camouflage for a targeted attack" aimed at specific data. *Id.*

"armed attack" as equivalent to "kinetic violence."[47] However, a cyberattack resulting in kinetic violence could trigger the victim State's right to self-defense.[48]

Some legal experts hold the position that the effects of a cyberattack must be violent,[49] including only physical damage to people or property.[50] However, other legal experts advocate for a broader view concerning what effects constitute an armed attack.[51] These experts argue that focusing on physical damage or death "fails to account for modern society's critical reliance on information infrastructure and connectivity."[52] In light of modern society's reliance on digital technologies, an effect's magnitude and immediacy should be more important than the type of effect when determining whether self-defense is triggered.[53]

An effects-based assessment is most commonly used to determine whether a cyberattack rises to the level of an armed attack.[54] Determining when the right to self-defense is available is simplest when cyberspace operations support traditional military operations because the traditional military attack alone will satisfy the armed attack requirement, and it is unnecessary to determine whether the cyberattack would separately be considered an armed attack.[55] A lone cyberattack can also constitute an armed attack when it results in destruction of property, injury, or death.[56] When a cyberattack targets non-tangible infrastructure or information, the

---

[47] Waxman, *supra* note 46, at 111.
[48] *Id.* "The position is therefore rarely advanced that a cyber attack could never constitute an armed attack." *Id.*
[49] *Id.* at 112.
[50] *See id.* ("[F]or example, a cyber attack that caused a power station to explode or one that caused airplanes to crash could legally constitute an armed attack, but cyber attacks that cause economic or social damage—like taking down the stock market or bringing transportation systems to a halt—could not.").
[51] *Id.*
[52] *Id.*
[53] *See id.* (Some experts look beyond "the type of effect to its magnitude, immediacy and other factors in assessing whether a cyber attack crosses the self-defense threshold.").
[54] Weissbrodt, *supra* note 19, at 363.
[55] *Id.* at 364.
[56] *Id.*

"scale and effects" of the attack must be assessed to determine whether it rises to the level of an armed attack.[57]

D. *Convention on Cybercrime*

In 2004, the Convention on Cybercrime entered into force.[58] The Convention pursues "a common criminal policy aimed at the protection of society against cybercrime . . . by adopting appropriate legislation and fostering international co-operation."[59] The drafters of the Convention sought to promote cooperation while addressing the massive impact that cybercrime has on individuals and companies worldwide.[60] The Convention aimed to address two concerns: (1) ensure that cybercrime definitions "were flexible enough to adapt to new crimes and methods of committing existing crimes as they evolve" and (2) "remain sensitive to the legal regimes of domestic states."[61] Flexibility in criminal definitions is essential because "perpetrators of cyber crimes find new technology to bypass an essential element of the crime or impede investigations" as new statutes are created.[62] Also essential is sensitivity to domestic legal regimes—and the "moral and cultural values" they reflect—to ensure that states ratify the treaty.[63] Despite cultural and political differences, most nations agree that cybercrime must be addressed.[64]

---

[57] *Id.* at 362.

[58] *Details of Treaty No. 185*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (last visited Nov. 29, 2020) [hereinafter *Details of Treaty*].

[59] Convention on Cybercrime, *supra* note 4, ¶ 3. The Convention deals "particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security." *Details of Treaty*, *supra* note 58.

[60] Shannon L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, 2 J. HIGH TECH. L. 101, 105 (2003).

[61] *Id.*

[62] *Id.* at 103.

[63] *Id.* at 105 ("For example, European nations have a much higher degree of privacy protection than the United States. The United States, on the other hand, has stronger speech protection than other nations.").

[64] *Id.* at 107. "Globally, cyber crimes constitute more than $15 billion in damages every year. Most organizations do not report cyber crimes because they fear exposure would make

The Convention requires that Member States enact domestic criminal law governing cybercrimes, including both substantive and procedural laws.[65] Under the Convention, Member States must also:

> [A]dopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in . . . this Convention, when the offence is committed:
>
> a) in its territory; or
>
> b) on board a ship flying the flag of that Party; or
>
> c) on board an aircraft registered under the laws of that Party; or
>
> d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.[66]

Finally, the Convention includes principles and provisions governing cooperation between Member States in prosecuting cybercrimes.[67]

II. DISTINCTIONS IN CYBERESPIONAGE

Cyberespionage occurs in more than one form. Economic espionage focuses on the use of espionage for the purpose of gaining economic

---

them vulnerable to future attacks by copycats or cause a loss of public confidence." *Id.* at 108.

[65] *See* Convention on Cybercrime, *supra* note 4, arts. 2-13 (requiring substantive laws); *see also id.*, arts. 14-21 (requiring procedural laws).

[66] *Id.*, art. 22, ¶ 1.

[67] *See id.*, arts. 23-35.

advantage.[68] Traditional forms of espionage, on the other hand, gather intelligence about foreign states for political advantage.[69] Both of these types of espionage occur in the cyber context.

A. *Economic Cyberespionage*

Economic cyberespionage poses a risk to companies in developed countries, particularly the United States. The issue of economic cyberespionage is an old one; beginning in the 1990s and early 2000s, non-governmental hackers in China conducted activity against the United States.[70] The United States National Security Agency (NSA) has documented increased instances of economic espionage against U.S. companies since 2009.[71] Further, evidence indicates prevalent state-sponsored cyberespionage aimed at stealing trade secrets from private entities.[72]

Economic cyberespionage is difficult to attribute to a specific actor or group of actors.[73] This is because most tools used to facilitate cyberespionage allow users to remain anonymous.[74] In 2015, a delegation

---

[68] JEFFREY L. DUNOFF ET AL., INTERNATIONAL LAW NORMS, ACTORS, PROCESS: A PROBLEM-ORIENTED APPROACH 120 (5th ed., 2020).

[69] *Id.*

[70] *Id.* at 119. Economic cyberespionage has also occurred in other developed countries. *See, e.g., id.* at 120 ("Chinese hackers have reportedly also attacked companies in Europe, Australia, and Japan.").

[71] *Id.* at 119. The NSA claimed "to have documented over 600 instances between 2009 and 2013 in which Chinese hackers stole confidential information from U.S. companies, for the apparent economic benefit of their Chinese competitors." *Id.*

[72] David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230 (2015). Evidence "suggests that some governments are specifically initiating and supporting theft of U.S. trade secrets from private companies via unauthorized intrusions into computer networks as a means to further their own economic development." *Id.* at 233.

[73] DUNOFF ET AL., *supra* note 68, at 119. Attribution of cyberespionage and cyberattacks is directly linked to the law of state responsibility. *Id.* at 127. A state is responsible for its actions or inactions with respect to the conduct of non-state actors. *Id.*

[74] *Id.* at 119. Cyber-based tools typically "involve a degree of anonymity that complicates efforts to identify who is acting, toward what ends, or with what effect." *Id.*

from China met with U.S. officials for four days to discuss cybersecurity.[75] While the talks did not address the issue of attribution, the agreement between the two countries addressed state responsibility.[76] The agreement reached by the presidents of China and the United States "[stated] that neither country's government will conduct or knowingly 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."[77]

B. *Cyberespionage Against States*

Cyberespionage also occurs against states.[78] This is typically done to gain a political advantage.[79] While theft of trade secrets and other economic espionage is more common today, economic espionage can serve a dual purpose when also conducted for political reasons.[80] In 2019, the United States experienced 1,473 data breaches that exposed over 164 million sensitive records.[81] The majority of cyber intrusions begin with baited emails that contain either phishing attempts or malicious attachments.[82]

Cyberespionage against states can have detrimental ramifications. For example, in 2013 the United States disclosed that Chinese agents accessed thirty-seven Pentagon weapons programs and twenty-nine defense

---

[75] WAYNE M. MORRISON, CONG. RSCH. SERV. RL 33536 CHINA-U.S. TRADE ISSUES 1 (2015).

[76] *Id.*

[77] *Id.* at 42. Critics of the agreement have noted that "it is often extremely difficult to identify hackers, let alone trace it back to a government entity." *Id.* However, some analysts "have called [the agreement] a good first start to developing rules governing cyber theft. . . ." *Id.*

[78] DUNOFF ET AL., *supra* note 68, at 120.

[79] *Id.*

[80] *How Nations Use Digital Espionage Against Each Other*, NORWICH UNIVERSITY ONLINE, https://online.norwich.edu/academic-programs/resources/how-nations-use-digital-espionage-against-each-other (last visited Nov. 29, 2020).

[81] Joseph Johnson, *Cyber Crime: Number of Breaches and Records Exposed*, STATISTA (Oct. 1, 2020), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[82] *How Nations Use Digital Espionage Against Each Other*, *supra* note 80. Phishing messages account for 23% of cyberespionage attempts, while malicious attachments account for 11%. *Id.*

technologies.[83] Other examples of recent cyberespionage include Russia's "weaponization of social media" to interfere in the 2016 U.S. election[84] and allegations of hacking "the world's most prominent coronavirus vaccine researchers" leveled against North Korea and Russia.[85]

III. DISTINCTIONS BETWEEN CYBERATTACKS

A cyberattack can occur in more than one manner.[86] Three types of cyberattacks with different legal consequences are (1) denial of service attacks, (2) cyberattacks alongside conventional warfare, and (3) cyberattacks with kinetic violence as an effect.[87] In 2007, Estonia experienced a denial of service attack.[88] The government's response to the attack provides an example of appropriate reactions to a denial of service attack. In 2008, Georgia suffered a cyberattack alongside conventional warfare.[89] This type of attack naturally has different legal consequences because of the presence of conventional warfare.[90] Lastly, in 2010, the Stuxnet worm infiltrated Iran's nuclear program.[91] This computer worm

---

[83] *See id.* ("A year later, there were two major breaches of U.S. government databases–the security clearance files of 22.1 million people and personnel records.").

[84] *See* S. SELECT COMM. ON INTELLIGENCE, 116TH CONG., REP. ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS, at 14, (1st Sess. 2018), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[85] Kevin Collier, *North Korea and Russia Are Still Trying to Hack Coronavirus Vaccine Researchers*, NBC NEWS (Nov. 13, 2020, 9:19 AM), https://www.nbcnews.com/tech/security/north-korea-russia-are-still-trying-hack-coronavirus-vaccine-researchers-n1247692. *See also* Chris Fox & Leo Kelion, *Coronavirus: Russian Spies Target Covid-19 Vaccine Research*, BBC NEWS (July, 16, 2020), https://www.bbc.com/news/technology-53429506.

[86] *See* JULIE E. MEHAN, CYBERWAR, CYBERTERROR, CYBERCRIME AND CYBERACTIVISM 118-33 (2d ed. 2014) (summarizing various types of cyberattacks).

[87] *Id.* at 42-43, 110, 123.

[88] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007, 12:00 PM), https://www.wired.com/2007/08/ff-estonia/.

[89] John Markoff, *Before the Gunfire, Cyberattacks,* N.Y. TIMES (Aug. 12, 2008), https://nytimes.com/2008/08/13/techinology/13cyber.html.

[90] This is because this type of cyberattack is done "in an effort to obtain a battlefield advantage or a force multiplier." MEHAN, *supra* note 86, at 39.

[91] Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-

caused kinetic effects, which may allow different retaliation options than less malicious attacks.[92]

A. *Denial of Service: Estonia*

In 2007, Estonia experienced a wave of cyberattacks.[93] The attacks came in the midst of Estonian political tensions; the government removed a controversial statue from downtown Tallinn, Estonia's capital, and installed it in a military cemetery.[94] On April 28, the day after the statue's removal, the country experienced a disruption of its networks.[95]

Estonia suffered a denial of service attack, which "occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor."[96] A flood of network server traffic is the most common method of denial of service attacks.[97] In Estonia, multiple machines operated together in a distributed denial of service attack.[98] These more complicated attacks used botnets to have a larger effect.[99]

The attacks continued into May 2007.[100] Using chat rooms, hackers recruited individuals to spam Estonian servers.[101] Additionally, botnets were used for a distributed denial of service attack across a variety of government and business websites while some hackers changed the language or postings

---

security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[92] *Id.*

[93] Davis, *supra* note 88.

[94] *Id.*

[95] *Id.* The attack affected "[a]ll major commercial banks, telcos, media outlets, and name servers . . . and this affected the majority of the Estonian population." *Id.*

[96] *Security Tip (ST04-015)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (last updated Nov. 20, 2019), https://us-cert.cisa.gov/ncas/tips/ST04-015.

[97] *Id.*

[98] Davis, *supra* note 88.

[99] "A botnet" is a group of "hijacked internet-connected devices." The devices forming the botnet are also victims in this type of attack. *Security Tip (ST04-015)*, *supra* note 96.

[100] *Id.*

[101] *Id.*

on these sites to spread their political message.[102] The botnets overloaded servers with waves of spam and automated online requests.[103] On May 8, 2007 at 11:00 PM in Tallinn, the nation's networks experienced a 200-fold surge compared to normal traffic.[104] Throughout the following day, the country experienced fifty-eight separate botnet attacks.[105]

The attack on Estonia was the first instance of a cyberattack taking down a state's entire digital infrastructure.[106] Estonia as a nation fought back against the cyberattacks with the help of the Vetted, a "select few who are trusted by the world's largest [internet service providers] and can ask [the service providers] to kick rogue computers off the network."[107] On May 8, the night of the worst attack, three members of the Vetted identified Internet Protocol (IP) addresses for the botnets and requested service providers to cut off access for the addresses.[108] In mid-May, the attacks ceased.[109]

Estonia's actions to mitigate the damage of the denial of service attacks were coupled with appeals to Russia, but these were ignored.[110] While many suspected that Russia was responsible for the attacks, investigations indicated that the Russian government was not affiliated.[111] Instead, the

---

[102] The distributed denial of service attack impacted Estonian banks, media outlets, and government bodies' websites due to the unprecedented levels of internet traffic. *Id.*; *see also* Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2017), https://www.bbc.com/news/39655415 ("The result for Estonian citizens was that cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news.").

[103] McGuinness, *supra* note 102.

[104] Davis, *supra* note 88.

[105] *Id.*

[106] *See id.* ("This was not the first botnet strike ever, nor was it the largest. But never before had an entire country been targeted on almost every digital front all at once, and never before had a government itself fought back.").

[107] *Id.*

[108] *Id.*

[109] *Id.* (The Speaker of the Estonian Parliament stated: "When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing . . . [L]ike nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything.").

[110] McGuinness, *supra* note 102.

[111] Weissbrodt, *supra* note 19, at 350.

attacks were "the product of 'spontaneous anger from a loose federation of separate attackers.'"[112]

Cyber actions such as denial of service attacks, website defacements, and harmful information spreading are political coercion tools, but these actions do not involve a use of force.[113] Due to heavy reliance on information infrastructure, information networks are a "logical target."[114] By targeting websites that Estonian citizens, businesses, and government bodies used on a daily basis, the attackers created a sizeable impact.[115] Despite this, these cyberattacks did not give Estonia the right to use force in self-defense under Article 51 of the U.N. Charter. The assault on Estonian systems was economic and political coercion and fell short of an armed attack.[116] Even if Estonia could have legally responded with force, the State's ability to do so would have been impaired by its inability to determine the source of the attacks.[117]

B. *Supplementing Conventional Warfare: Georgia*

In 2008, the South Ossetia conflict in Georgia involved conventional warfare supplemented by a cyber offensive.[118] On August 8, 2008, Georgian President Mikheil Saakashvili sent troops to the province of South Ossetia to quell a separatist movement.[119] President Sakaashvili ordered the Georgian military to capture the South Ossetian capital.[120] Russia quickly reacted by relocating troops to the Georgian border and conducting air strikes against

---

[112] *Id.* (quoting CLAY WILSON, CONG. RESEARCH SERVS., RL 32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 8 (2009)).

[113] *See* Davies, *supra* note 10, at 12 ("[U]sing international law as a guide, these should not be considered attacks, as they don't involve the use of force.").

[114] *Id.* at 13.

[115] Davis, *supra* note 88.

[116] Davies, *supra* note 10, at 8.

[117] *Id.*

[118] *Id.* at 7. This conflict was "among the first cases in which an international political and military conflict was accompanied, or even preceded, by a coordinated cyber offensive." *Id.*

[119] Sarah Pruitt, *How a Five-Day War with Georgia Allowed Russia to Reassert Its Military Might*, HISTORY (last updated Sept. 4, 2018), https://www.history.com/news/russia-georgia-war-military-nato.

[120] *Id.*

Georgian military positions.[121] This swift reaction resulted in Russia rapidly gaining control of South Ossetia's capital and set the stage for Russian forces to push further into Georgia.[122] The conflict lasted five days.[123] However, in the weeks before the conflict, a cyberattack was mounted against Georgia.[124]

Experts in the United States claimed that the cyberattacks on Georgia's internet infrastructure began with distributed denial of service attacks by Russia.[125] The experts then claimed that Russian operatives initiated cyberattacks on government websites, media, communications, and transportation companies.[126] Because of these cyberattacks, the Georgian government lost access to its infrastructure as the Georgian military fought off a conventional attack.[127] As proof of their claims, experts in the United States pointed to previously staged botnets which were activated just before air strikes began similar to those used by a Russian criminal gang called the Russian Business Network.[128]

While the cyberattacks alone were not armed attacks as required by Article 51 to trigger the right of self-defense, the conventional warfare that took place was sufficient. Just before the conflict, Georgia attempted to join the North Atlantic Treaty Organization (NATO).[129] If the nation had been subject to the organization's collective defense agreement, Georgia could

---

[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), https://www.nytimes.com/2008/08/13/technology/13cyber.html.
[125] *Id.* These attacks began as early as July and "effectively shut down Georgian servers." *Id.*
[126] *Id.*
[127] *Id.* Researchers witnessed "the attack against Georgia spread to computers throughout the government after Russian troops entered the Georgian province of South Ossetia." *Id.*
[128] *Id.* "[I]n the run-up to the start of the war . . . computer researchers had watched as botnets were 'staged' in preparation for the attack, and then activated shortly before Russian air strikes began." *Id.*
[129] Pruitt, *supra* note 119.

have called upon NATO forces to assist in its defense against both the cyber and conventional warfare.[130]

C. *Initiating Kinetic Violence: Iran*

In 2008, the Stuxnet computer worm entered the Iranian computer system at an underground uranium enrichment plant.[131] The creators of Stuxnet designed the worm to cripple industrial infrastructure.[132] After Stuxnet infiltrated Iran's nuclear program, the Natanz facility experienced software and hardware malfunctions.[133] Stuxnet would "suddenly speed up or slow down the spinning of centrifuges used to enrich uranium, causing their parts to break and thereby crippling the entire uranium enrichment operation."[134] Stuxnet also caused computers monitoring the centrifuges to report normal functioning while the changes in speed took place.[135] The Stuxnet operation worked successfully until the worm infected an engineer's computer.[136] The worm spread after the engineer took the computer home and connected to the internet.[137] The spread of Stuxnet exposed the computer worm to the public and infected over 100,000 computers worldwide.[138]

Stuxnet infected several industrial sites in Iran.[139] This occurred because computer worms spread on their own following the initial installation into a computer system.[140] The Stuxnet worm operated in three phases: (1) it targeted specific operating systems and networks, (2) sought

---

[130] Elias Chachak & Emilio Iasiello, *NATO's Cyber Operations Center - Will Russia Feel Threatened?*, CYBER RES. DATABANK, https://www.cyberdb.co/natos-cyber-operations-center-will-russia-feel-threatened/ (last visited Nov. 29, 2020) (clarification).

[131] Weissbrodt, *supra* note 19, at 351.

[132] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 447-48 (2012).

[133] Weissbrodt, *supra* note 19, at 351.

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.* at 351-52.

[138] *Id.* at 352.

[139] David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013, 2:00 PM), https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[140] *Id.*

specific software, and (3) compromised the software.[141] On June 1, 2012, the United States admitted that Stuxnet was a joint project between itself and Israel.[142] Iran did not confirm reports that the virus destroyed some of its centrifuges.[143]

The computer worm, "at minimum," was a use of force because the virus was reported to have caused physical property damage.[144]

> The breaking of the centrifuges constitutes a physical destruction of property that rises above the level of a "minor inconvenience or irritation." . . . The consequences were immediate. . . . [T]he breaking of the centrifuges was the direct result of the Stuxnet worm. The attack is considered invasive because the Natanz facility was supposed to be a secure, secret facility. Furthermore, because the United States has claimed responsibility for the cyber-attack, Stuxnet certainly constitutes a use of force. . . .[145]

However, whether the attack rises to the level of an armed attack depends on the interpretation of armed attack.[146] Because the attack did not result in injury or death, Stuxnet could be classified as an unarmed attack.[147]

---

[141] *Id.* "[Stuxnet] targeted Microsoft Windows machines and networks, repeatedly replicating itself." The virus specifically sought out Siemens Setp7 software, which is "used to program industrial control systems that operate equipment, such as centrifuges." The virus finally compromised the software and the programmable logic controllers. "The worm's authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant." *Id.*

[142] Weissbrodt, *supra* note 19, at 351.

[143] Kushner, *supra* note 139. "The overall effectiveness of Stuxnet is unclear, with the United States government arguing that it delayed Iran's nuclear development by one-and-a-half to two years, while others report that Iran was able to successfully contain much of the damage caused by Stuxnet." Weissbrodt, *supra* note 19, at 352.

[144] Weissbrodt, *supra* note 19, at 376.

[145] *Id.* at 376-77 (footnote omitted) (quoting Michael N. Schmitt, *Cyber Operations and the Sus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 576 (2011)).

[146] *See id.* at 377-78.

[147] *Id.* at 377.

Alternatively, Stuxnet caused damage that would have otherwise required a conventional military operation.[148]

Even though Iran suffered an armed attack, it is unlikely an Iranian armed response would satisfy the requirements of necessity, proportionality, and immediacy and would not be lawful.[149] Actions such as eradicating Stuxnet from Iranian systems and legal action—which Iran took in 2012—would eliminate the necessity of an armed response.[150] Proportionality raises several questions and it is unclear whether only cyber actions would be proportional, or if a traditional military response would meet this requirement.[151] Lastly, any response would have come after the United States admitted responsibility for the cyberattack. This admission came two years after the discovery of Stuxnet and would likely not have met the immediacy requirement.[152]

IV. PSYCHOLOGICAL IMPACTS OF CYBER INTRUSIONS

Cyber intrusions—whether acts of espionage or armed attacks—have psychological impacts.[153] The psychological effects of cyber intrusions "can be informed by social impact, and can include more personal aspects such as an individual's anxiety, worry, anger, outrage, depression and so on."[154]

An individual's or user's beliefs about cybersecurity are crucial to understanding their reaction to cyber intrusions.[155] A user's beliefs about the perceived severity of a cyber event, the susceptibility of the threat, the perceived self-efficacy, and the cost and efficacy of preventative or mitigating behaviors influence reactions to cybersecurity and security mechanisms.[156] These factors increase the difficulty of motivating protective

---

[148] *Id.* at 378.
[149] *Id.*
[150] Weissbrodt, *supra* note 19, at 376.
[151] *Id.* at 379.
[152] *Id.*
[153] *See generally* MARIA BADA & JASON R. C. NURSE, EMERGING CYBER THREATS AND COGNITIVE VULNERABILITIES (Academic Press, 1st ed. 2020).
[154] *Id.* at 74.
[155] *Id.* at 75.
[156] *See id.* ("[T]he general culture of fear related to crime and cyber-events" is an additional element to be considered.).

cybersecurity practices and predicting social and psychological responses to cyberattacks.[157]

Cyberattacks are often acts of terrorism and attempts to instill fear in the civilian population to extract political concessions.[158] In the "war on cyber terrorism," security measures are rightly focused on defending transportation networks, hospitals, banks, military installations, and government offices from cyberattacks.[159] However, concerns over the human dimension of cyberwarfare are equally important.[160]

"[F]or a vibrant civil society," citizens "must be able to live free of undue fear, anxiety, and trepidation."[161] This is known as "human security."[162] "[C]onventional terrorism undermines human security even more than national security" and "exacerbates feelings of insecurity and perceptions of threat that prompt public cries for protective and militant government policies."[163]

In field surveys, researchers studied the effects of cyberterrorism on "psychological well-being and political attitudes that impinge upon human security by causing stress, anxiety, and fear—all of which radicalize political attitudes and push people to exchange privacy for security to prevent cyber terror in the future."[164] In the first field survey experiment, researchers interviewed 522 individuals following an act of cyberterrorism by the

---

[157] *Id.*

[158] *See* Michael L. Gross et al., *The Psychological Effects of Cyber Terrorism*, 72 BULL. ATOMIC SCI. 284, 285 (2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5370589/ ("In this way, cyber terrorism is no different from conventional terrorism. Yet cyber terrorism is far more subtle.").

[159] *Id.* Cybersecurity measures focus on key infrastructure just as traditional security measures "worry about defending the same facilities from terrorist bombs or ballistic missiles. . . . But as the war on cyber terrorism continues, it is increasingly clear that protecting vital national interests is only half the battle." *Id.*

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] Gross et al., *supra* note 158.

"hacktivist" group known as Anonymous.[165] In the second experiment, 907 subjects viewed various film clips depicting hypothetical Hamas attacks on Israel's national water company.[166] Following the screenings, researchers surveyed the subjects to measure the effect on human security.[167]

The results demonstrated that exposure to cyber terrorism increases stress.[168] Additionally, feelings of stress and anxiety grow as cyberattacks become more deadly.[169] Stress scores for lethal and non-lethal cyber terrorism were not far behind the scores for conventional terrorism.[170] Additionally, "[i]ndividuals were equally disturbed by lethal and non-lethal cyber terrorism, meaning there is no significant difference between the two when it comes to stress."[171] Similar to stress, more severe attacks increased threat perception.[172] While both lethal and non-lethal cyberattacks evoked feelings of stress in the study, "only terrorism accompanied by injury and loss of life nurtures a serious preoccupation about the next attack."[173]

---

[165] *See id.* (stating that Anonymous threatened to "take down servers and 'erase Israel from cyber space'" in an "electronic Holocaust" in April 2015).

[166] *Id.* In the first scenario, the clip depicted a cyber terrorism incident where the country's water supply's chlorine content reached a fatal level. A second scenario showed a nonlethal act of cyber terrorism when hackers appropriated bank account numbers and transferred money to Hamas. *Id.* at 286. A final scenario depicted a fatal but conventional mass-casualty terrorist attack. A control group watched a neutral film showing the dedication of a water treatment plant. *Id.*

[167] *See id.* at 286 ("These included stress, anxiety, insecurity and threat perception, political militancy, and a willingness to relinquish privacy and civil liberties in favor of security.").

[168] *Id.*

[169] *Id.* Results were measured using a State-Trait Anxiety Inventory (STAI). *Id.*

[170] Gross et al., *supra* note 158, at 286 "[C]onventional mass-casualty terrorism (e.g. suicide bombings) evokes a level of anxiety at the top of the scale. The stress scores for lethal and non-lethal cyber terrorism are not far behind, and all the scores significantly surpass the control group." *Id.*

[171] *Id.* Both lethal and nonlethal cyberattacks "cause significant panic and anxiety and both, it seems, are equally capable of cracking the foundations of personal wellbeing and human security." *Id.*

[172] *Id.* at 287. Threat perception did not increase with non-lethal cyber terrorism. However, lethal terrorism triggered a significant jump regardless of conventional or cyber based attacks. The authors concluded that "[t]hese findings show how stress and threat perception are two different phenomena. Stress is emotional while threat perception is cognitive." *Id.*

[173] *Id.* Additionally, the participants' reactions changed between the two studies with the identity of the group. *Id.*

The study results also revealed that political attitudes harden in response to terrorism.[174] Researchers asked participants about their level of "support for internet surveillance, government regulation, and military retaliation in the context of an unspecified cyber terror attack."[175]

> From a psychological perspective, the data offer a curious finding. [The researchers] expected to find a clear connection between exposure to cyber terrorism and militant hardline attitudes. The harsher the terrorist attack [the] subjects experienced, the greater their militancy. But this is not what [the researchers] discovered. Instead, [they] found that the greater one's *perception of threat*, the greater one's militancy. The odds were more than twice as high that individuals with high levels of threat perception will support surveillance, government regulation, and military retaliation compared to those whose threat perception is lower.[176]

In addition to increasing "hardline attitudes" and "political militancy,"[177] "[c]yber terrorism is a force multiplier that can magnify the effects of limited, sporadic, and even failed kinetic terrorist attacks."[178]

---

[174] *Id.* at 288.

[175] *Id.*

[176] Gross et al., *supra* note 158 at 290 (emphasis in original). The researchers could not explain why some subjects exhibited more fear than others.

> Past exposure to cyber attacks explains only a small part of the variance. Other personality factors, beyond the scope of [the] study to examine, are also probably at work. Nevertheless, it is clear that the threat of terrorism and how one perceives it are better determinants of militancy and hardline attitudes than the experience of an actual attack.

Id.

[177] *Id.* The study also demonstrated that cyber terrorism increases stress, fear, and anxiety. *Id.* "These results offer tantalizing evidence that cyber terrorism mirrors conventional terrorism even when its victims do not suffer injury or loss of life." *Id.* "Individuals who misunderstand the nature of cyber terrorism and the threat it poses are most likely inclined to greater fear, insecurity, and militancy than those whose assessment is sober." *Id.* at 291.

[178] *Id.* at 290. "In tandem, conventional and cyber terrorism can undermine human security in a most fundamental way. . . . One need not suffer direct harm to be terrorized; it is enough

Overall, the "experiments show a cyber terrorism effect . . . enables terrorists to foster fears akin to kinetic terrorism and pursue similarly ideological goals."[179]

Victims of cybercrime and cyberattacks can experience emotional trauma resulting from the incident.[180] Some victims experience limited symptoms of Acute Stress Disorder while others experience feelings of betrayal, vulnerability, and anger.[181]

> Often, victimization can lead victims to feelings of outrage, anxiety, a preference for security over liberty, and little interest of adopting new technology due to loss of confidence in cyber. The victim can go into stages of grief, suffer from anger or rage. In some cases, victims may even blame themselves and develop a sense of shame . . .[182]

As a result of cyber intrusions, "victims react with not only fear, as do victims of crime, but with demands for protection from the government, via surveillance and stronger regulations."[183] These psychological reactions are often magnified when the cyber intrusion is an act of cyberterrorism.[184]

V. DEVELOPMENTS IN CYBERSECURITY

As technology develops, new threats develop that must be addressed. The use of psychology addresses some cyber threats by informing user behavior and developing well-rounded action plans. On an international scale, existing treaty organizations are evolving to address new cyber threats.

---

that one *fear* direct harm to suffer the ravages of contemporary terrorism, whether cyber terrorism or conventional terrorism." *Id.* (emphasis in original).

[179] *Id.* at 291 (internal quotations omitted). "In this way, cyber terrorism pushes well beyond cyber crime even when its methods . . . are sometimes similar." *Id.* at 292. Victims under attack "react with not only fear and trepidation, as do victims of crime, but with demands for protection from the enemies of the state via harsh military retaliation, surveillance, and strong government." *Id.*

[180] BADA & NURSE, *supra* note 153, at 82.

[181] *Id.*

[182] *Id.* at 83.

[183] *Id.*

[184] *Id.*

Lastly, cyberpsychology can influence user behavior to strengthen cybersecurity mechanisms.

A. *Use of Psychology in Organizations*

"Cyberpsychology" expands as experts use psychology to understand how users behave in a cyber context.[185] Cyberpsychology considers how humans interact with digital tools in digital space.[186] Particularly, industrial-organizational (I-O) psychologists use cyberpsychology to influence the security of cyberspace.[187] I-O psychologists use job analysis "to identify essential functions and KSAOs (knowledge, skills, abilities, and other characteristics) . . . to develop performance criteria."[188] Within organizations, I-O psychologists should apply this process to the cybersecurity domain.[189]

A strategic job analysis, conducted by an I-O psychologist, describes the current state of the job and also anticipates performance requirements of jobs that will exist in the future.[190] This anticipation can be especially important in cybersecurity where evolving technology dictates what positions are needed and the necessary skills for the people who fill those positions.[191] Additionally, "due to the inherently cognitive and human-computer mediated nature of cybersecurity work, nontraditional job analytic techniques may be particularly useful."[192]

Several factors will need to go into selecting personnel who are the best fits for cybersecurity positions within organizations to reduce the risk

---

[185] Rachel C. Dreibelbis et al., *The Looming Cybersecurity Crisis and What It Means for the Practice of Industrial and Organizational Psychology*, 11 INDUS. & ORGANIZATIONAL PSYCHOLOG. 346, 348 (2018).
[186] *Id.*
[187] *Id.*
[188] *Id.* at 349.
[189] *Id.*
[190] *Id.* at 351.
[191] Dreibelbis et al., *supra* note 185, at 351.
[192] *Id.*

of "insider threats."[193] Insider threats to cybersecurity in organizations come from employees who are either purposefully compromising security or behaving with laziness; both can result in noncompliance with cybersecurity procedures.[194] By predicting which individuals are likely to violate cybersecurity procedures, organizations can focus training efforts on the identified individuals.[195]

Stronger security policies in reaction to security breaches or threats do not guarantee "cybersafe" employee behavior.[196] However, establishing a security culture within an organization develops norms that improve information security.[197] A security culture affects overall behaviors toward information security and can be reenforced through less abstract trainings such as simulations.[198] I-O psychology suggests that organizations should move away from "parameter defense" as a cybersecurity posture toward "cyber resilience."[199] In doing so, organizations should focus on building teams capable of rapid detection, response, and adaptation in the face of the rapidly evolving security context.[200] However, organizations facing cybersecurity threats are not the only actors in cybersecurity.

---

[193] *Id.* at 352. "[I]t is critical to consider the motivations of cyber operators during the selection process in order to reduce the risk of insider threat." *Id.* at 353.

[194] *Id.* at 356.

[195] *Id.* at 356-57. Most employees will pose a non-malicious threat to an organization's cybersecurity. *Id.* at 356. For these employees, "cybersecurity tasks (even small things like looking out for phishing emails) might have been part of their onboarding training, though it is likely not part of an official job description." *Id.* In light of this, "cybersecurity behaviors should be considered an emerging class of extra-role or organizational citizenship behaviors (OCBs), signaling the importance of citizenship-related predictors." *Id.* at 356-57.

[196] *Id.* at 357-58.

[197] Dreibelbis et al., *supra* note 185, at 358.

[198] *Id.* at 357.

[199] *Id.* at 358.

[200] *Id.* So far, "research on effective cybersecurity teams has been confined to military and government settings" and has "found that encouraging analysts to work as a team and providing team rewards led to increased performance, but team structure, a lack of team communication, and information overload all contributed to the degradation of cybersecurity team performance in a cybersecurity defense task." *Id.* at 358-59. Implementing I-O psychology in a corporate setting could improve protection against economic espionage resulting from phishing attempts and malicious attachments. Further, the use of cyberpsychology could help policy makers determine what protections can be

B. *Treaties and Cybersecurity*

Lawmakers also engage in efforts to protect cyberspace. To date, a number of bilateral agreements address the allied response to cyber threats.[201] While there is currently no multilateral treaty specifically tailored to address cybersecurity, a few existing international agreements and their organizations are addressing cybersecurity concerns.

1. *ANZUS*

On September 15, 2011, the United States and Australia announced that their alliance would "extend into cyberspace."[202] The joint statement echoed Article III of the Australia, New Zealand, United States Security Treaty (ANZUS) which addresses threats to security, rather than Articles IV and V which address armed attack.[203] The joint statement focused on "attacks on military systems designed to degrade or disable them" rather than acts of cyberespionage.[204]

2. *NATO*

The 2007 attack on Estonia prompted NATO to change its "cyber-war capabilities."[205] In 2014, NATO updated its cyber defense policy and now treats "digital attacks as the equivalent of kinetic attacks under its

---

independently implemented by organizations and where the law should evolve to fill the gaps.

[201] Herrera-Flanigan, *supra* note 11, at 18.

[202] Lydia Khalil, *Introduction*, *in* SPECIAL REPORT: ANZUS 2.0, CYBERSECURITY AND AUSTRALIA-US RELATIONS 1, 1 (Australian Strategic Policy Institute) (2012).

[203] Davies, *supra* note 10, at 4.

[204] *Id.*

[205] Associated Press, *A Look at Estonia's Cyber Attack in 2007*, NBCNEWS.COM (July 8, 2009), http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.XxmZd_hKii5.

collective security arrangement under Article 5 of the [North Atlantic Treaty]."[206]

C. *Applying Cyberpsychology*

Cyberpsychology can be used to influence user behavior. Individuals using information systems and technology are the weakest links in cybersecurity measures.[207] People engage in the development and implementation of security tools, use information infrastructure, and use applications to manage their tasks.[208] People also make mistakes.[209] In light of this fact, developments in the security community acknowledge user behavior and its effect on cybersecurity.[210] While an individual may be the "weak link," the human element in information systems is often the best route to building an effective cybersecurity program.[211] One of the primary ways organizations can achieve better levels of cybersecurity is by educating users.[212] Further, as companies have modified their practices, they "have become more risk aware, have integrated security into software development, and have started to use artificial intelligence to assist in analyzing user behavior."[213]

Cybersecurity and user behavior can be improved through "nudge interventions."[214] The nudge approach has gained attention in England where

---

[206] Chachak & Iasiello, *supra* note 130. However, classifying cyberattacks under Article 5 does not "provide a path forward to how NATO can and should engage and respond to cyber attacks." *Id.*

[207] MEHAN, *supra* note 86, at 112.

[208] *Id.*

[209] *Id.* Because of this, "people, a major element of any information system, are always going to be the weak point in that same system." *Id.* at 101. "Another component of the problem is that organizations remain focused on external threats, such as hackers and viruses, at the same time consistently *underemphasizing* internal threats." *Id.* at 102 (emphasis added).

[210] *Id.*

[211] *Id.* at 134.

[212] *See id.* at 135.

[213] Michael Speas, *Foreword* to TARI SCHREIDER, BUILDING AN EFFECTIVE CYBERSECURITY PROGRAM: A SECURITY MANAGER'S HANDBOOK 28 (Kristen Noakes-Fry ed., Rothstein Publishing 2018).

[214] P. Briggs et al., *Behavior Change Interventions for Cybersecurity*, *in* BEHAVIOR CHANGE RESEARCH & THEORY 242, 247 (Linda Little, Elizabeth Sillence & Adam Joinson eds., Academic Press 2017).

a behavioral insights team (also known as the "Nudge Unit") forms public policy using insights from the behavioral sciences.[215] Behavioral nudges can be employed in a "choice architecture" by deliberately privileging some choices over others.[216] Choice architectures work most effectively in circumstances where users make swift decisions.[217] The cybersecurity context utilizes nudge interventions within the context of human-computer interaction.[218]

By applying psychology and knowledge of user behaviors, governments and companies could better strengthen the weakest links in cybersecurity measures. Additionally, the understanding of user behavior could be applied in the legal context to better analyze legal regimes' strengths and weaknesses. Finally, the use of cyberpsychology has the potential to improve and modify existing legal regimes to strengthen security in cyberspace worldwide.[219]

CONCLUSION

Cyber intrusions exist in a complicated place in international law. They also pose a threat to individuals' mental wellbeing in addition to data and security systems. The development of cyberpsychology and further understanding of how humans interact with cyber networks is currently

---

[215] *Id.*

[216] *See, e.g., id.* (Examples of nudges in action include "the use of default settings, simplified notices that make certain choices more 'salient,' social nudges that induce people to conform to type and a range of other message manipulations that simply make some choices seem easier or more desirable than others.").

[217] *Id.*

[218] *Id.* at 250. Further examples of nudges include messages based on "morality, deterrence, and incentives to nudge users to lock smartphones" and conveying information "about risks and about safer online behaviors" in a way that improves users' understanding of the consequences of their actions. *Id.*

[219] *See* BADA & NURSE, *supra* note 153, at 77 ("[P]olicy makers need to understand how people think about and respond to risk and materialized attacks, given that without such insight policies or awareness efforts might be unsuccessful."); Asmeret Bier Naugle et al., *Simulating Political and Attack Dynamics of the 2007 Estonian Cyber Attacks*, 1-2, SANDIA NATIONAL LABORATORIES, 2016 Winter Simulation Conference (Doc. SAND2016-3036C) (describing the simulation of the 2007 Estonian cyber events and possible use of the model focusing on "short term dynamics of the cyber attacks and rioting").

being used in organizations to improve responses to cyber intrusions. Further, international organizations are actively working to address the issue of cyber threats. The use of cyberpsychology in developing public policy can improve existing legal regimes and lead to a more secure world.