


# Peeling Back the Onion of Cyber Espionage after Tallinn 2.0

David A. Wallace

Amy H. McCarthy

Mark Visger

Follow this and additional works at: <https://digitalcommons.law.umaryland.edu/mlr>

 Part of the [Computer Law Commons](#), [International Law Commons](#), and the [National Security Law Commons](#)

---

### Recommended Citation

78 Md. L. Rev. 2015 (2019)

This Article is brought to you for free and open access by the Academic Journals at DigitalCommons@UM Carey Law. It has been accepted for inclusion in Maryland Law Review by an authorized editor of DigitalCommons@UM Carey Law. For more information, please contact [smccarty@law.umaryland.edu](mailto:smccarty@law.umaryland.edu).

---

---

**PEELING BACK THE ONION OF CYBER ESPIONAGE  
AFTER TALLINN 2.0**

COLONEL DAVID A. WALLACE,\* AMY H. MCCARTHY,\*\*  
LIEUTENANT COLONEL MARK VISGER\*\*\*

ABSTRACT

*Tallinn 2.0 represents an important advancement in the understanding of international law's application to cyber operations below the threshold of force. Its provisions on cyber espionage will be instrumental to states in grappling with complex legal problems in the area of digital spying. The law of cyber espionage as outlined by Tallinn 2.0, however, is substantially based on rules that have evolved outside of the digital context, and there exist serious ambiguities and limitations in its framework. This Article will explore gaps in the legal structure and consider future options available to states in light of this underlying mismatch.*

I. INTRODUCTION

Cyber espionage is unquestionably one of the most persistent and perplexing economic and security problems in the world today. It has and will continue to be a major source of friction between states into the foreseeable future.<sup>1</sup> While many nations have suffered data breaches resulting in serious

---

© 2019 Colonel David A. Wallace, Amy H. McCarthy, and Lieutenant Colonel Mark Visger.

\* Professor and Head, Department of Law, United States Military Academy, West Point. Colonel Wallace was assigned to the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia in fall 2017. Colonel Wallace would like to thank the NATO CCD COE Director, Merle Maigre, the Law Branch Chief, Lauri Aasmann, and all of the members of the Law Branch for their collegial assistance and support during the fellowship.

\*\* Assistant Professor, Department of Law, United States Military Academy, West Point.

\*\*\* Assistant Professor, Department of Law, United States Military Academy, West Point. The views contained in this Article are those of the authors and do not necessarily represent the views of the Department of Defense, the United States Army, the United States Military Academy, or the NATO CCD COE.

1. See, e.g., COLLIN ANDERSON & KARIM SADJADPOUR, CARNEGIE ENDOWMENT FOR INT'L PEACE, IRAN'S CYBER THREAT: ESPIONAGE, SABOTAGE, AND REVENGE 6 (2018), [http://carnegieendowment.org/files/Iran\\_Cyber\\_Final\\_Full\\_v2.pdf](http://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf) (detailing Iran's efforts in this arena); Tim Johnson, *Small Nations Join Hacking Game—and This Mideast One Got Big Results*, MCCLATCHY

ramifications from instances of digital espionage, most also quietly continue to engage in cyber spying as an integral part of national security efforts.<sup>2</sup> The interests of some states, however, are not limited to conventional political and military secrets. Private entities have also emerged as important players in this traditionally state-dominated activity.<sup>3</sup> Capabilities associated with cyber technology have changed the landscape in trade secret and proprietary data theft against states and private industry, creating serious financial perils for victims and threats of national economic destabilization.<sup>4</sup>

From the U.S. government perspective, cyber espionage has come to represent not only a serious external national security and economic threat, but a diplomatic and domestic public relations minefield. China has gained substantial military advantages in recent years by stealing information on some of the most advanced weapons systems in the American arsenal, including jet fighters and unmanned submersible vehicles.<sup>5</sup> In addition to the exposure of military secrets, the theft of intellectual property has also posed a threat to the country's economic health and defense strategy. Commenting on the impacts of economic cyber espionage specifically, a senior Department of Justice official in the Obama Administration observed:

This is a serious threat to our national security. I mean, our economy depends on the ability to innovate. And if there's a dedicated nation state who's using its intelligence apparatus to steal day in

---

DC BUREAU (Jan. 23, 2018), <https://www.mcclatchydc.com/news/nation-world/national/national-security/article196090329.html> (describing a long-term cyber espionage campaign by Lebanon against companies and individuals from twenty-one countries); Mariarosaria Taddeo, Opinion, *Qatar Crisis: Lessons to Learn in the Age of Cyber Attacks*, NEWSWEEK (July 22, 2017), <http://www.newsweek.com/qatar-crisis-lessons-learn-age-cyber-attacks-640446> (citing the hack of the Qatar News Agency and resulting friction between Qatar and the United Arab Emirates, among other recent instances).

2. See Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1096–98 (2004); see also Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyber War?*, NEW YORKER (Nov. 1, 2010), <https://www.newyorker.com/magazine/2010/11/01/the-online-threat> (describing the “EP-3E” incident as an example of China's interest and capability in the area of cyber espionage).

3. See Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 293 (2015) (discussing the rise of foreign surveillance on individuals); see also Johan Sigholm, *Non-State Actors in Cyberspace Operations*, 4 J. MIL. STUD. 1 (2013) (exploring the expanding role of non-state actors in offensive cyber activities).

4. See Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 443, 459–73 (2014). Domestic corporate victims of cyber espionage include Coca-Cola, Lockheed Martin, Adobe, Google, and many others. *Id.* at 454.

5. U.S.-CHINA ECON. AND SEC. REV. COMM'N, 114TH CONG., ANNUAL REP. TO CONGRESS 302 (2016), [https://www.uscc.gov/sites/default/files/annual\\_reports/2016%20Annual%20Report%20to%20Congress.pdf](https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf).

and day out what we're trying to develop, that poses a serious threat to our country.<sup>6</sup>

In 2015, the Office of Personnel Management (“OPM”) was the subject of a cyber-espionage operation by Chinese hackers<sup>7</sup> resulting in the release of the personal information of over twenty-two million people.<sup>8</sup> In another troubling and highly-publicized episode, a team with links to the Russian government hacked into the Democratic National Committee computer system in an effort to disrupt the 2016 U.S. presidential election.<sup>9</sup> Reports of America's own program of surveillance have also created ripples around the globe. Working for an intelligence contractor, Edward Snowden copied and then leaked highly classified National Security Agency (“NSA”) information that revealed, among other things, various intrusive cyber espionage activities by the United States and its allies.<sup>10</sup>

Despite an increased global awareness of the dangers of digital spying, international law currently does little to specifically address the practice.<sup>11</sup> In the absence of specific treaty provisions, international law is generally reactive—reflecting state practice that over time hardens into customary law. It is not surprising, then, that the international legal framework lags behind the pace of change in cyberspace. The governing legal framework for digital spying, in fact, evolved in the absence of modern digital capabilities. With cyber espionage showing no sign of abating, it is important to not only understand the current state of international law, the *lex lata*, regarding digital espionage, but also to recognize the gaps, ambiguities, and limitations in the

---

6. James Billington, *China's 'Great Brain Robbery' Hacking of U.S. Companies a National Security Emergency*, INT'L BUS. TIMES (Jan. 18, 2016), <http://www.ibtimes.co.uk/chinas-great-brain-robbery-hacking-us-companies-national-security-emergency-1538590>.

7. Ellen Nakashima, *Chinese Government Has Arrested Hackers It Says Breached OPM Database*, WASH. POST (Dec. 2, 2015), [https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb\\_story.html?utm\\_term=.03db1e4a7150](https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html?utm_term=.03db1e4a7150). It was unclear what, if any, relationship the hackers had to the Chinese government. *Id.*

8. Kevin Murnane, *Cyber Security: The World's Best and Worst Presented with a Well-Designed Infographic*, FORBES (May 4, 2017), <https://www.forbes.com/sites/kevinmurnane/2017/05/04/cyber-security-the-worlds-best-and-worst-presented-with-a-well-designed-infographic/#32233554416>.

9. Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html>.

10. Paul Szoldra, *This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, BUS. INSIDER (Sept. 16, 2016), <http://www.businessinsider.com/snowden-leaks-timeline-2016-9>. Snowden's disclosures resulted in international as well as domestic condemnation of the United States' cyber activities. See, e.g., *The NSA's Secret Spy Hub in Berlin*, SPIEGEL (Oct. 27, 2013), <http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>.

11. See *infra* Parts III, IV.

current legal architecture. Also important is a consideration of the road ahead, the *lex ferenda*, as the law evolves to fit this new digital context.

Fortunately for government and military officials, policy makers, legal advisers, academics, and others interested in cyber law and policy, the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*<sup>12</sup> (“*Tallinn Manual 2.0*” or “*Tallinn 2.0*”) is a foundational starting point for such an analysis. *Tallinn Manual 2.0* addresses several controversial legal matters surrounding cyber espionage as well as many other vital issues spanning public international law. By way of background and context, in 2009, the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (“NATO CCD COE”), a renowned cyber research and training institution in Tallinn, Estonia, invited an independent group of experts to compile a manual on the international law governing cyber warfare.<sup>13</sup> This effort brought together a group of international law scholars and practitioners—the International Group of Experts (“Experts”)—to explore and articulate how extant legal norms apply to cyber warfare.<sup>14</sup> The original *Tallinn Manual on International Law Applicable to Cyber Warfare*<sup>15</sup> was published in 2013. As a result of the success of the first *Tallinn Manual*, the NATO CCD COE launched a follow-on initiative to expand the scope of coverage, with the updated Manual to include international law governing cyber operations during peacetime. The reason for the new initiative by the NATO CCD COE was to respond to the realities of what was actually happening in cyberspace. That is, states were dealing with cyber issues below the use of force threshold on a frequent basis.<sup>16</sup>

The NATO CCD COE thus convened a second group of Experts, and their efforts led to the publication of *Tallinn Manual 2.0* in 2017. The greatly expanded Manual not only incorporates and updates the materials on cyber warfare from the first publication, but also includes coverage of legal regimes implicated by peacetime cyber activities.<sup>17</sup> *Tallinn Manual 2.0* contains 154

---

12. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN 2.0].

13. *Id.* at 1.

14. *Id.*

15. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

16. See *Tallinn Manual 2.0*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, <https://ccdcoe.org/research/tallinn-manual/> (last visited Feb. 13, 2019).

17. *Id.* Recent scholarship has explored *Tallinn 2.0*'s impact on areas involving sovereignty, state attribution, and international human rights law. See generally William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 TEX. L. REV. 1487, 1493 (2017); Robert E. Barnsby & Shane R. Reeves, *Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Law Chapter*, 95 TEX. L. REV. 1515, 1516 (2017); Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1640–41 (2017). Not surprisingly, *Tallinn 2.0* has generated a great deal of discussion and debate and, in some cases, disagreement about how international legal norms apply

rules, including two specific rules on cyber espionage—one for peacetime and the other for armed conflict.<sup>18</sup> These rules reflect the Experts’ determinations as to the current *lex lata* within the area of cyber operations. The commentary accompanying each rule not only provides some valuable insights into the deliberations of the Experts in terms of the legal basis for the rules and their normative context, but also offers practical implications of their application in a cyber environment.<sup>19</sup> Additionally, the commentaries to the rules articulate, in some depth, the various positions taken by the Experts in their discussions, including the relative consensus they could reach on a particular issue. This is helpful “[a]s neither treaty application nor [s]tate practice is well developed” with respect to cyber operations generally, or cyber espionage specifically.<sup>20</sup>

This Article will examine the legal landscape of cyber espionage under international law as delineated by *Tallinn 2.0*. First, the Article will explore the historical and legal evolution of digital spying.<sup>21</sup> The Article will then examine *Tallinn 2.0*’s specific rules pertaining to the practice.<sup>22</sup> Next, the Article will discuss the normative gaps, ambiguities, and limitations of the current state of the law, including an exploration of the international legal norms that directly and indirectly govern cyber espionage.<sup>23</sup> Finally, the Article will offer some thoughts on the *lex ferenda* for cyber espionage, both in peace and wartime, in light of current developments.<sup>24</sup> Significantly, the Article will evaluate whether the applicable international legal norms are adequate to regulate the pervasive and detrimental problem of digital spying for states and, by extension, commercial interests, and individuals.

## II. CYBER ESPIONAGE: HISTORICAL CONTEXT AND CHARACTERISTICS

Espionage has a multitude of definitions. Popularly, it is defined as “the practice of spying or using spies to obtain information about the plans and

---

to cyberspace and operations. Compare Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), <https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/#more-37812> (adopting the opinion that sovereignty is a foundational principle for the international norms on the prohibition on the use of force and the rule of non-intervention), with Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT’L L. 735, 740–41 (2017) (positing that “sovereignty is a principle that depends on the domain and the practical imperatives of states and is subject to adjustment in interstate application”). This Article will focus exclusively on *Tallinn 2.0*’s treatment of cyber espionage.

18. TALLINN 2.0, *supra* note 12, at 168–74 (Rule 32), 409–12 (Rule 89).

19. See, e.g., *id.* at 11–29 (discussing the issue of state sovereignty in the context of cyber operations).

20. *Id.* at 4.

21. See *infra* Part II.

22. See *infra* Part III.

23. See *infra* Part IV.

24. See *infra* Part V.

activities especially of a foreign government or a competing company.”<sup>25</sup> Put in a slightly different context, espionage includes, among other things, a state’s efforts to clandestinely acquire classified or otherwise protected information from a targeted state or from entities or individuals within the targeted state.<sup>26</sup> If knowledge is power, it is hardly surprising that states seek to obtain intelligence from and about each other. In the most traditional sense of spying, a state or one of its organs dispatches an agent into another state on a mission to access and obtain protected intelligence.<sup>27</sup>

### A. Historical Evolution

Espionage, for whatever purpose, is not new. Some have even said it is the world’s second oldest profession.<sup>28</sup> Antiquity is replete with stories of spies. The earliest known surviving record of espionage dates from the war between Pharaoh Ramses with the Hittites and the Battle of Kadesh in 1274 B.C.<sup>29</sup> The tools of the spy trade have undergone a staggering transformation over the course of human history. As technology has developed and progressed, astoundingly complex and creative means for carrying out espionage have been devised.<sup>30</sup> For example, around 500 B.C., the Spartans invented the skytale, a device composed of rods and papyrus designed to transport hidden messages.<sup>31</sup> In the Middle Ages, the Italian painter and polymath Leon Battista Alberti invented one of the first known mechanical devices for encoding messages—a cipher wheel.<sup>32</sup> A more sophisticated version of Alberti’s cipher wheel was still being used during the American Civil War.<sup>33</sup>

---

25. *Espionage*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/espionage> (last visited Jan. 18, 2019).

26. David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, 17 ASIL INSIGHTS (2013), <https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving>.

27. Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, in INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES 65–66 (Anna Maria Osula & Henry Røigas eds., 2016).

28. Paul Reynolds, *The World’s Second Oldest Profession*, BBC NEWS (Feb. 26, 2004), <http://news.bbc.co.uk/1/hi/world/americas/3490120.stm>.

29. Steven M. Kleinman, *The Promise of Interrogation v. The Problem of Torture*, 43 VAL. U. L. REV. 1577, 1579 (2009).

30. Leah Hoffmann, *The Evolution of Spy Tools*, FORBES (Apr. 19, 2006), [https://www.forbes.com/2006/04/15/intelligence-spying-gadgets\\_cx\\_lh\\_06slate\\_0418tools.html](https://www.forbes.com/2006/04/15/intelligence-spying-gadgets_cx_lh_06slate_0418tools.html).

31. More descriptively:

Skytales were long, slender rods which had been wrapped with a thin strip of papyrus, leather, or parchment. A message was written on the wrapping, and then the strip was unwound and passed on to a messenger (who often wore it as a belt). Only when it was rewound around a rod of the same diameter could the original message be deciphered.

*Id.*

32. *Id.*

33. *Id.*

The 20th Century also saw some interesting gadgets used for spying. For example, during World War I, the German military used pigeons outfitted with cameras to photograph troops and fortifications.<sup>34</sup> Upon return, intelligence officers then studied the aerial photos to gain information about enemy troop numbers, locations, and weapons.<sup>35</sup> The photographs also facilitated the creation of more precise topographical maps.<sup>36</sup> During World War II, brilliant allied mathematicians and engineers constructed a device that enabled intelligence officers to break the codes of the sophisticated German Lorenz SZ-40 cipher machine.<sup>37</sup> Nicknamed “Colossus,” it is now considered the world’s first fixed-program, digital, electronic, computer.<sup>38</sup>

In the aftermath of World War II, during the cloak and dagger drama of the Cold War, states leveraged technological innovations to further their espionage efforts. These advancements include everything from miniaturized cameras and shoe heel transmitters to high altitude U-2 spy planes, such as the one flown by Francis Gary Powers when he was shot down by the Soviet Union in 1960.<sup>39</sup>

In more recent years, technology has transformed and revolutionized methods of espionage. An explosion of technological advancements has led to the development of such platforms and capabilities as unmanned surveillance drones, highly sophisticated and classified spy satellites and, of course, computers, related information technology, and data-gathering techniques. In one of the earliest cases of cyber espionage, West German officials discovered a Soviet-backed spy ring had gained access to dozens of U.S. military computers during the late 1980s.<sup>40</sup> Incidents of cyber espionage have risen exponentially along with the ubiquitous use of computer technology.<sup>41</sup>

---

34. Dan Schlenoff, *Aerial Spying, 100 Years Before Drones*, SCI. AM.: ANECDOTES FROM THE ARCHIVE (Oct. 10, 2014), <https://blogs.scientificamerican.com/anecdotes-from-the-archive/aerial-spying-100-years-before-drones/>.

35. *Id.*

36. *Id.*

37. *Colossus*, CRYPTO MUSEUM, <http://www.cryptomuseum.com/crypto/colossus/index.htm> (last visited Sept. 13, 2017).

38. *Id.*

39. Michael Dobbs, *Gary Powers Kept a Secret Diary with Him After He Was Captured by the Soviets*, SMITHSONIAN MAG. (Oct. 15, 2015), <https://www.smithsonianmag.com/smithsonian-institution/gary-powers-secret-diary-soviet-capture-180956939/>. Powers was sentenced to ten years in prison by Russia for his admitted espionage but was released early in a prisoner exchange. *A Look Back. . . The Cold War: Strangers on a Bridge*, CENT. INTELLIGENCE AGENCY (Feb. 20, 2009), <https://www.cia.gov/news-information/featured-story-archive/strangers-on-a-bridge.html>.

40. John Markoff, *West Germans Raid Spy Ring That Violated U.S. Computers*, N.Y. TIMES (Mar. 3, 1989), <http://www.nytimes.com/1989/03/03/world/west-germans-raid-spy-ring-that-violated-us-computers.html>.

41. For a comprehensive examination of the extent of foreign economic espionage occurring in recent years with the aid of computer technology, see generally NAT’L COUNTERINTELLIGENCE AND SEC. CTR., *FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE* (2018), <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>.



Today, disturbing accounts of widespread cyber espionage activities, such as exfiltration, monitoring, and theft of digital information, dominate media reports.<sup>42</sup> No longer limited by geographical barriers, risk of capture, and lack of linguistic and cultural expertise, modern cyber spies operate on a dramatically different landscape than traditional spies. This shift has also opened the playing field to smaller states previously excluded from large-scale intelligence activities, traditionally dominated by major world powers.<sup>43</sup> For example, recent reports reveal the serious threat posed by North Korean-linked cyber spies against multiple countries including the United States, South Korea, and various Middle Eastern nations.<sup>44</sup>

### B. *The Rise of Economic Espionage*

State espionage has not been limited to the collection of military, political, or national security secrets. A historical analysis shows that nations have also engaged in widespread economic-based surveillance of foreign states and businesses—stealing trade secrets, intellectual property, and other proprietary data for the benefit of governments and private firms since at least the Cold War.<sup>45</sup> Economic espionage, sometimes also termed industrial or commercial espionage, has resulted in unfair business advantages for nations conducting these activities and enormous economic losses for state, institutional, and individual victims.<sup>46</sup>

---

42. See, e.g., Ryan Lucas, *U.S. Charges Alleged Chinese Government Spy with Stealing U.S. Trade Secrets*, NPR (Oct. 10, 2018), <https://www.npr.org/2018/10/10/656280811/u-s-charges-alleged-chinese-government-spy-with-stealing-u-s-trade-secrets> (reporting on the charges filed against a Chinese intelligence officer for economic espionage); Bruce Schneier, *What's Next in Government Surveillance*, ATLANTIC (Mar. 2, 2015), <https://www.theatlantic.com/international/archive/2015/03/whats-next-in-government-surveillance/385667/> (chronicling some modern instances of state-sponsored hacking, exfiltration, and espionage).

43. See Mark Galeotti, *Size Doesn't Matter for Spies Anymore*, FOREIGN POL'Y (Jan. 31, 2018), <http://foreignpolicy.com/2018/01/31/size-doesnt-matter-for-spies-anymore/> (discussing the robust espionage capabilities of Dutch spies, specifically).

44. See Eric Auchard, *Lesser-Known North Korea Cyber-Spy Group Goes International: Report*, REUTERS (Feb. 20, 2018), <https://www.reuters.com/article/us-northkorea-cyber/lesser-known-north-korea-cyber-spy-group-goes-international-report-idUSKCN1G42CH>.

45. See Lotrionte, *supra* note 4, at 444, 459–70 (explaining the dramatic rise in economic espionage as nations came to appreciate the significant role of financial stability in the maintenance of national power in the aftermath of the USSR's dissolution).

46. See *id.* (discussing the impact of economic espionage from the Cold War to modern day). Economic espionage has been defined in various ways. According to the Federal Bureau of Investigation:

Economic espionage is foreign power-sponsored or coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, designed to unlawfully or clandestinely influence sensitive economic policy decisions or to unlawfully obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies. This theft, through open and clandestine methods, can provide foreign entities with vital proprietary economic information at a fraction of the true cost of its research and development, causing significant economic losses.

The United States has publicly refused to take part in intelligence gathering for the benefit of private businesses since the 1970s.<sup>47</sup> In the wake of the Edward Snowden revelations, the White House reaffirmed its commitment to this principle.<sup>48</sup> Based on statements from former government officials within the past few years, the U.S. position on economic espionage appears to be relatively unique.<sup>49</sup> The French government, for example, has been breaking into hotel rooms of foreign business travelers and downloading the contents of their personal computers for the competitive advantage of French companies for years.<sup>50</sup> Although the American government has consistently affirmed that it does not conduct commercial espionage to benefit domestic companies, it is important to note that it does not deny that it collects economic information for its own use.<sup>51</sup>

---

*What Is "Economic Espionage"?*, FED. BUREAU OF INVESTIGATION, <https://www.fbi.gov/about/faqs/what-is-economic-espionage> (last visited Feb. 3, 2018).

47. Samuel J. Rascoff, *The Norm Against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections*, 83 U. CHI. L. REV. 249, 252 (2016). The President's Foreign Intelligence Advisory Board (PFIAB) under President Nixon was of the opinion that such sharing of information would be inappropriate and a conflict of interest. *Id.* (first citing JOHN J. FIALKA, *WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA* 7 (1997); then citing *The Threat of Foreign Economic Espionage to U. S. Corporations: Hearings Before the Subcom. on Economic and Commercial Law of the H. Committee on the Judiciary*, 102d Cong. 18 (1992) (statement of Gerard S. Burke)).

48. Press Release, Office of the Press Sec'y, Presidential Policy Directive on Signals Intelligence Activities (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>. According to this directive:

The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.

*Id.* (footnote omitted). Some limited exceptions do apply, however. The government may share specific information with a private firm, for example, indicating that the business is the victim of an offensive cyber operation. *See* Rascoff, *supra* note 47, at 257. Additionally, information regarding the involvement of foreign officials with suspect business transactions, including instances of bribery, may be conveyed to firms. *Id.*

49. Former CIA director Michael Hayden claimed that only four other countries followed this American norm. *Michael Hayden Says U.S. Is Easy Prey for Hackers; Former CIA and NSA Chief Says 'Shame on Us' For Not Protecting Critical Information Better*, WALL ST. J. (June 21, 2015), <https://www.wsj.com/articles/michael-hayden-says-u-s-is-easy-prey-for-hackers-1434924058>. This short list is most likely comprised of the United Kingdom, Canada, Australia, and New Zealand. Rascoff, *supra* note 47, at 256 & n.45 (citing Margaret Warner, *An Exclusive Club: The Five Countries That Don't Spy on Each Other*, PBS (Oct. 25, 2013), <https://www.pbs.org/newshour/world/an-exclusive-club-the-five-countries-that-dont-spy-on-each-other>).

50. Philip Ewing, *Gates: French Cyber Spies Target U.S.*, POLITICO (May 22, 2014), <https://www.politico.com/story/2014/05/france-intellectual-property-theft-107020>.

51. *See* Jack Goldsmith, *The Precise (and Narrow) Limits on U.S. Economic Espionage*, LAWFARE (Mar. 23, 2015, 7:09 AM), <https://www.lawfareblog.com/precise-and-narrow-limits-us-economic-espionage> (positing that U.S. practice does allow for economic espionage on foreign

Despite its own position, the United States has suffered the impacts of foreign economic espionage from a variety of governments over time, involving South Korea, Japan, France, Russia, Israel, China, and Germany.<sup>52</sup> China is a notable example. Chinese economic espionage is on an almost unfathomable industrial scale. Although exact figures are unknowable, the Commission on the Theft of American Intellectual Property estimated that the theft of American intellectual property totals approximately \$300 billion annually, with fifty to eighty percent of that resulting from China.<sup>53</sup> China's long-running campaign to steal valuable information and data from companies and government agencies includes the work of at least one unit from the People's Liberation Army—Unit 61398—as well as other highly effective government-sponsored cyber espionage organizations.<sup>54</sup> In his statement before the Senate Select Committee on Intelligence on May 11, 2017, the Director of National Intelligence, Daniel Coats, stated that Beijing would likely continue to actively target the U.S. government, its allies, and American companies with cyber espionage operations.<sup>55</sup>

The intersection of the advancement of cyber capabilities and concurrent rise in economic espionage is particularly significant. As described by retired U.S. Army General Keith Alexander, the former Director of the NSA and the Commander of U.S. Cyber Command, “The loss of industrial information and intellectual property through cyber espionage constitutes the ‘greatest transfer of wealth in history.’”<sup>56</sup> Problematically for most states, national governments generally lack control over the private digital networks and infrastructure subject to foreign economic espionage efforts.<sup>57</sup> This has

---

states and companies, and even theft of trade secrets, but does not allow the information to be passed along to U.S. firms).

52. Lotrionte, *supra* note 4, at 468 (citing JOHN J. FIALKA, *WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA* 5 (1997)).

53. Adam Segal, *How China Is Preparing for Cyberwar*, CHRISTIAN SCI. MONITOR (Mar. 20, 2017), <https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar>.

54. Ellen Nakashima & Ashkan Soltani, *FBI Warns Industry of Chinese Cyber Campaign*, WASH. POST (Oct. 15, 2014), [https://www.washingtonpost.com/world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453\\_story.html?utm\\_term=.3a4eb16c5ed4](https://www.washingtonpost.com/world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453_story.html?utm_term=.3a4eb16c5ed4).

55. *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 6–7 (2018) (statement of Daniel R. Coats, Director of National Intelligence).

56. Randolph Kahn, *Economic Espionage in 2017 and Beyond: 10 Shocking Ways They Are Stealing Your Intellectual Property and Corporate Mojo*, AM. BAR ASS'N (Sept. 19, 2018), [https://www.americanbar.org/groups/business\\_law/publications/blt/2017/05/05\\_kahn/](https://www.americanbar.org/groups/business_law/publications/blt/2017/05/05_kahn/).

57. In addition to maintaining security over Department of Defense networks, one of the interests of U.S. Cyber Command is coordinating with the private sector in ensuring digital security. See DEP'T OF DEFENSE, *DOD CYBER STRATEGY 7* (2015), [http://archive.defense.gov/home/features/2015/0415\\_cyber-strategy/final\\_2015\\_dod\\_cyber\\_strategy\\_for\\_web.pdf](http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf). The report also stated, “The United States government has a limited and specific role to play in defending the nation against cyberattacks of significant consequence. The private sector owns and operates over ninety percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense.”

been exacerbated further with the rise of cloud computing.<sup>58</sup> Where nations have historically maintained control over domestic borders and pertinent governmental assets, thereby mitigating the risk of traditional forms of intelligence gathering, this balance of control has been upset in the industrial cyber realm.

### *C. Methods and Characteristics of Cyber Espionage*

As discussed below, the method used to accomplish an act of espionage is determinative in any legal analysis.<sup>59</sup> It is important, therefore, to briefly consider the varieties and characteristics of digital espionage operations. As a starting point, most acts of cyber spying could be fairly characterized as computer network “exploitation” rather than as an “attack,” as the aim is the collection of information rather than the destruction or degradation of digital capabilities.<sup>60</sup> Cyber espionage is one type of cyber intrusion. A helpful description of cyber espionage is contained in the NATO volume *Peacetime Regime for State Activities in Cyberspace*. It provides:

[C]opying of data that is publicly not available and which is in wireless transmission, saved or temporarily available on IT-systems or computer networks located on the territory or area under the exclusive jurisdiction of another [s]tate by a [s]tate organ, agent, or otherwise attributable to a [s]tate, conducted secretly, under disguise or false pretences, and without the (presumed) consent or approval of the owners or operators of the targeted IT-systems or computer networks or of the territorial [s]tate. Copying includes also the temporary copying of data into the random access or virtual memory of an IT-system for the purpose of mere visualization or acoustic exemplification of ([for example], voice over IP) data.<sup>61</sup>

In some important respects, cyber espionage is in a category by itself with regard to its characteristics and capabilities. First, cyber espionage has virtually unlimited reach given that a digital operation can be launched from and target almost anywhere in the world. Second, with the development and

---

*Id.* at 5. U.S. Cyber Command considers national economic security as a major cyber concern for the future. *Id.* at 2.

58. See J. Nicholas Hoover, *Compliance in the Ether: Cloud Computing, Data Security and Business Regulation*, 8 J. BUS. & TECH. L. 255, 260–62 (2013) (describing the security perils of cloud computing).

59. See *infra* Part IV.

60. See HEATHER HARRISON DINNISS, *CYBER WARFARE AND THE LAWS OF WAR* 156 (2012); see also Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 829 (2012).

61. Katharina Ziolkowski, *Peacetime Cyber Espionage—New Tendencies in Public International Law*, in *PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY* 429 (Katharina Ziolkowski ed., 2013).

evolution of the “internet of things” in which all things in societies are connected via data networks,<sup>62</sup> cyber espionage poses broad risks to human infrastructure. Third, it is also extraordinarily difficult to defend against. Hundreds of billions of dollars have been spent by states, businesses, and individuals on software, services, and hardware to prevent and mitigate the effects of cyber espionage.<sup>63</sup> Emerging technologies facilitate access to voluminous information and the ability to download it at an incredible speed.<sup>64</sup> Finally, one of the true Gordian knots of cyber operations generally, and cyber espionage specifically, is the difficulty of attribution. The attribution of cyber activities carried out through the internet is extraordinarily problematic and, in many cases, impossible to achieve.<sup>65</sup> Given these capabilities and characteristics of operating in cyberspace, it is no surprise that cyber espionage is a particularly attractive and effective method to acquire information. Of course, it is axiomatic that technology, by its very nature, develops more quickly than do most laws that regulate its use. This is certainly true with international law and cyber espionage. In fact, cyber espionage poses significant challenges to the legal framework governing traditional espionage practices.

#### D. Traditional Legal Framework

As background, it is important to understand the legal status of traditional forms of espionage, both in times of peace and of conflict. As a threshold matter, the international legality of state conduct is articulated in the 1927 landmark Permanent Court of International Justice opinion in the *Lotus* case.<sup>66</sup> According to that decision, states have significant discretion, limited only in certain cases by prohibitive rules and, in the absence of such rules, a

---

62. See Jacob Morgan, *A Simple Explanation of ‘The Internet of Things,’* FORBES (May 13, 2014), <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7d48b45f1d09>.

63. David J. Kappos & Pamela Passman, *Cyber Espionage Is Reaching Crisis Levels,* FORTUNE (Dec. 12, 2015), <http://fortune.com/2015/12/12/cybersecurity-amsc-cyber-espionage/>.

64. Consider the statement of a senior U.S. government source: “A spy might once have been able to take out a few books’ worth of material . . . Now they take the whole library. And if you restock the shelves, they will steal it again.” *Cyberwar: War in the Fifth Domain,* ECONOMIST (July 1, 2010), <https://www.economist.com/node/16478792>.

65. See generally Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229 (2012) (examining the issues endemic to cyber operation attribution).

66. S.S. “*Lotus*” (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 9, at 18–19 (Sept. 7). The court held:

Now the first and foremost restriction imposed by international law upon a [s]tate is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another [s]tate. In this sense jurisdiction is certainly territorial; it cannot be exercised by a [s]tate outside its territory except by virtue of a permissive rule derived from international custom or from a convention.

*Id.*

state is free to adopt the principles that it believes are best and most suitable to its interests.<sup>67</sup>

### 1. *In Peacetime*

Considerable uncertainty surrounds the legal status of traditional foreign espionage during peacetime. International law is virtually silent on this issue.<sup>68</sup> The Vienna Convention on Consular Relations does grant immunity to a foreign diplomatic official discovered to be involved in espionage activities.<sup>69</sup> Such person will generally be deemed a *persona non grata*<sup>70</sup> and removed from the host state.<sup>71</sup> Aside from this limited circumstance, however, significant legal ambiguity exists in the area of peacetime espionage. Although there is some disagreement in the literature,<sup>72</sup> the scholarly consensus appears to be that the practice is either *not illegal* or it is affirmatively *legal* under international law.<sup>73</sup> Simply put, no international treaty specifically prohibits espionage, and there exists a long-established and widespread state practice of employing spies. The lack of mutual agreements in this area is not surprising, however. Nations have strong national security and political justifications for spying.<sup>74</sup> States are understandably reluctant to reveal their own capabilities and methods in foreign intelligence gathering, and bilateral or multilateral discussions on this issue may necessitate disclosing such information.<sup>75</sup> Even if specific terms could be agreed upon, espionage is inev-

---

67. Buchan, *supra* note 27, at 67–68.

68. See A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 601–03 (2007). According to one scholar, “[T]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture.” *Id.* at 602 (alteration in original) (quoting Richard A. Falk, *Foreward to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW*, at v (Roland J. Stanger ed., 1962)).

69. Vienna Convention on Diplomatic Relations, art. 31, ¶ 1, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95.

70. Literally, “unwelcome” or “unacceptable” person. See Ben Zimmer, “*Persona non grata*”: *The Diplomatic Way to Say ‘You’re Unwelcome*,” WALL ST. J. (Jan. 5, 2017), <https://www.wsj.com/articles/persona-non-grata-the-diplomatic-way-to-say-youre-unwelcome-1483631639> (explaining this term in the context of diplomatic relations).

71. Vienna Convention on Diplomatic Relations, *supra* note 69, art. 9, ¶ 1; see Lotrionte, *supra* note 4, at 460–61 (noting American and Russian instances of this practice from the Cold War).

72. Scholars have taken the varying views that peacetime espionage is legal, illegal, or in a gray area between the two. Radsan, *supra* note 68, at 602–06.

73. See Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 608 (2016); see also Darien Pun, Comment, *Rethinking Espionage in the Modern Era*, 18 CHI. J. INT'L L. 353, 360–61 (2017) (exploring the tolerability of this uncertainty in the modern day).

74. See, e.g., Arthur S. Hulnick & Daniel W. Mattausch, *Ethics and Morality in United States Secret Intelligence*, 12 HARV. J.L. & PUB. POL'Y 509, 515 (1989) (arguing that foreign intelligence gathering fits within a state’s general obligation to protect citizens).

75. Deeks, *supra* note 3, at 314.

itably cloaked in secrecy, and violations of such agreements would be difficult to detect.<sup>76</sup> In other words, states would lack adequate assurances that legal agreements would be effective and domestically beneficial.

Despite the paucity of substantive prohibitions of espionage in international law, states themselves have long criminalized espionage under their own domestic laws.<sup>77</sup> Foreign spies are subject to apprehension, prosecution, and perhaps execution if discovered.<sup>78</sup> This arrangement creates a strange legal duality: Although spying is criminally proscribed by domestic law if conducted within and against the host country, the state itself engages in the same practice with its own intelligence assets around the globe.<sup>79</sup> This framework of risk is one that virtually all states are willing to accept. Indeed, almost every developed country in the world engages in foreign intelligence gathering.<sup>80</sup> In a practical sense, spying during peacetime may be seen as a responsible state tradition aimed at maintaining vital national interests and curbing potential external threats.<sup>81</sup> Espionage may also serve to facilitate a reduction in friction between states in international relations.<sup>82</sup> Nations have been operating in these legally uncertain waters for many years.<sup>83</sup>

## 2. *During Conflict*

In contrast to peacetime espionage, several treaty provisions govern the international legal framework regarding spying during wartime.<sup>84</sup> The first

---

76. *Id.*

77. Lotrionte, *supra* note 4, at 461 (noting that although states may prosecute and imprison spies under their own domestic law, it has been a frequent historical practice for states to exchange captured spies with opposing states).

78. See the case of Ethel and Julius Rosenberg for example. *Rosenberg v. United States*, 346 U.S. 273 (1953). For a thorough exploration of that trial, see Atossa M. Alavi, *The Government Against Two: Ethel and Julius Rosenberg's Trial*, 53 CASE W. RES. L. REV. 1057 (2003).

79. See, e.g., Radsan, *supra* note 68, at 618–19.

80. *Id.* at 613.

81. *Id.*

82. Lotrionte, *supra* note 4, at 445.

83. See Deeks, *supra* note 3, at 313–15 (discussing the relative “agnosticism” of states in the area of espionage under international law).

84. A condition precedent to the application of the law of armed conflict is, not surprisingly, an armed conflict. The law of armed conflict classifies armed conflicts into two types, namely: international and non-international armed conflicts. As a matter of law, no other type of armed conflict exists. The criteria for an international armed conflict, which is derived from Common Article 2 of the 1949 Geneva Conventions, involves two or more sovereign states using armed force against each other regardless of the reasons or the intensity of the confrontation. See Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 2, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85. Under the plain language of Common Article 2, a declaration of war and an occupation, partial or total, can also trigger the application of the entirety of the 1949 Geneva Conventions. *Id.* art. 2. Conversely, non-international armed conflicts, as delineated by Common Article 3, are between governmental forces and non-governmental armed groups, or between such groups only. *Id.* art. 3; see Int'l Comm. of the Red Cross [ICRC], *How is the Term “Armed Conflict” Defined in International Humanitarian*

treaty governing spies in wartime is Convention (IV) Respecting the Laws and Customs of War on Land and its annex, Regulations Concerning the Laws and Customs of War on Land (1907)—the Hague Relations.<sup>85</sup> It has three relevant articles:

ARTICLE 29.

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

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

ARTICLE 30.

A spy taken in the act shall not be punished without previous trial.

ARTICLE 31.

A spy who, after rejoining the army to which he belongs, is subsequently captured by the enemy, is treated as a prisoner of war, and incurs no responsibility for his previous acts of espionage.<sup>86</sup>

Importantly, the concept of espionage in the context of an armed conflict only applies to international armed conflicts—those occurring between states.<sup>87</sup> Taken together, and as supplemented and developed by Article 46 of Additional Protocol I to the Geneva Convention,<sup>88</sup> these provisions not

---

*Law?*, at 1–2, Opinion Paper (Mar. 2008), <https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf>.

85. Hague Convention No. IV, Respecting Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, 205 Consol. T.S. 277 [hereinafter Hague IV].

86. *Id.* art. 29–31.

87. *TALLINN 2.0*, *supra* note 12, at 410. This is because neither the concept of combatant immunity nor the status of prisoner of war (as discussed below) pertains to non-international armed conflicts. *Id.*

88. Article 46 reaffirms the traditional rules on espionage in the Hague Relations with some variations. Article 46 provides:



only define what it means for a member of the armed forces to engage in espionage, but also consequences of such conduct during an armed conflict. Article 31 of the Hague Relations is a unique and extraordinary provision in several respects.<sup>89</sup> First, spying is a status issue, not a war crime. If a member of the armed forces is captured while clandestinely engaging in the act of spying in the zone of operations of a belligerent, they do not retain the privileges afforded to members of the armed forces and, instead, may be prosecuted and punished for spying.<sup>90</sup> Under Article 31, a spy can regain their status as a prisoner of war (“POW”) and receive prosecutorial immunity if—after escape from capture—they are able to rejoin their army.<sup>91</sup> By comparison, there exists no similar dispensation for civilians.<sup>92</sup> That is, the civilian remains subject to trial and punishment under the domestic criminal laws of the targeted state upon capture. Additionally, if a civilian engages in espionage during an armed conflict, they may be considered to be taking a direct part in hostilities, thereby jeopardizing their protected status as a civilian under the law of armed conflict and making that person targetable during the period of participation.<sup>93</sup>

---

1. Notwithstanding any other provision of the Conventions or of this Protocol, any member of the armed forces of a Party to the conflict who falls into the power of an adverse Party while engaging in espionage shall not have the right to the status of prisoner of war and may be treated as a spy.

2. A member of the armed forces of a Party to the conflict who, on behalf of that Party and in territory controlled by an adverse Party, gathers or attempts to gather information shall not be considered as engaging in espionage if, while so acting, he is in the uniform of his armed forces.

3. A member of the armed forces of a Party to the conflict who is a resident of territory occupied by an adverse Party and who, on behalf of the Party on which he depends, gathers or attempts to gather information of military value within that territory shall not be considered as engaging in espionage unless he does so through an act of false pretences or deliberately in a clandestine manner. Moreover, such a resident shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured while engaging in espionage.

4. A member of the armed forces of a Party to the conflict who is not a resident of territory occupied by an adverse Party and who has engaged in espionage in that territory shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured before he has rejoined the armed forces to which he belongs.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 46, June 8, 1977, 1125 U.N.T.S. 3, 16 I.L.M. 1391 [hereinafter Additional Protocol I].

89. Hague IV, *supra* note 85, art. 31.

90. *Id.*

91. *Id.*

92. YORAM DINSTEIN, *THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT* 221 (2d ed. 2010).

93. TALLINN 2.0, *supra* note 12, at 410.

As contemplated under international law, traditional forms of espionage involve “acting clandestinely or on false pretences” in the context of employing human resources behind enemy lines.<sup>94</sup> It does not specifically address espionage conducted by other intelligence-gathering methods, such as the use of electronic devices, wiretapping, code breaking, and aerial or satellite photography.<sup>95</sup> To put a finer point on the concept of “acting clandestinely,” the soldier must be engaged in activities undertaken secretly or secretively designed to conceal the identity of persons involved or the fact that it had occurred.<sup>96</sup> By contrast, “on false pretences” has been interpreted to mean that certain conduct created the impression that the individual concerned was entitled to access the information in question.<sup>97</sup> The most commonly envisioned example of spying under the law of armed conflict is a member of the armed forces captured in civilian clothing, or in an enemy uniform, gathering intelligence behind enemy lines.<sup>98</sup>

The above provisions show that the international community may consider spying during wartime, like in peacetime, to be an accepted reality. Despite the fact that espionage does not constitute a war crime, it is still an activity that is commonly criminally proscribed by states.<sup>99</sup> A captured spy, whether soldier or civilian, may be prosecuted by the detaining military for violating an applicable law of the detaining force.<sup>100</sup>

### III. CYBER ESPIONAGE, INTERNATIONAL LAW, AND *TALLINN 2.0*

Mirroring the legal framework addressed in the previous section, *Tallinn Manual 2.0* also articulates two distinct rules covering cyber espionage—one for peacetime and the other for armed conflict.

#### A. *In Peacetime*

Under Rule 32 of *Tallinn 2.0*, peacetime cyber espionage is defined as “any act undertaken clandestinely or under false pretences that uses cyber

---

94. See Hague IV, *supra* note 85, art. 29.

95. See *id.*

96. *TALLINN 2.0*, *supra* note 12, at 410.

97. *Id.*

98. GARY D. SOLIS, *THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR* 240 (2d ed. 2016).

99. For a comprehensive list of state practices regarding captured spies during armed conflict, see *Practice Relating to Rule 107. Spies*, INT’L COMM. OF THE RED CROSS, [https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2\\_rul\\_rule107\\_sectionb](https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule107_sectionb) (last visited Dec. 28, 2018).

100. In an early American example, British Major John Andre was sentenced to death by a U.S. military commission after being apprehended behind enemy lines in civilian clothes following his meeting with Benedict Arnold to arrange the defeat of West Point. See *John Andre: Case Officer*, CENT. INTELLIGENCE AGENCY (May 8, 2007), [https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol5no3/html/v05i3a07p\\_0001.htm](https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol5no3/html/v05i3a07p_0001.htm). For a thorough review of espionage under American military law, see David A. Anderson, *Spying in Violation of Article 106, UCMJ: The Offense and the Constitutionality of its Mandatory Death Penalty*, 127 MIL. L. REV. 1, 3 (1990).

capabilities to gather, or attempt to gather, information.”<sup>101</sup> The Experts enumerated a non-exhaustive list of examples of conduct or activities that potentially could involve cyber espionage: surveillance, monitoring, capturing, or exfiltrating electronically transmitted or stored communications, data, or other information.<sup>102</sup> Importantly, the Experts included within the term “cyber espionage” actions that are directed at states and private businesses—to specifically include industrial and economic espionage.<sup>103</sup> In terms of its scope of applicability, Rule 32 is applied to states and those whose actions can be attributed to states.<sup>104</sup>

The *Tallinn 2.0* Experts’ bottom line legal analysis for peacetime cyber espionage is quite clear: “[P]eacetime cyber espionage by [s]tates does not *per se* violate international law, [although] the method by which it is carried out might do so.”<sup>105</sup> Once examined more closely, this conclusion is an unsurprising statement of existing law. In neither cyber espionage nor traditional forms of espionage in peacetime are there specific international treaties that regulate this practice.<sup>106</sup> The Experts did acknowledge that because cyber espionage has become so widespread and damaging, it has spurred a debate about whether a new customary international law norm prohibiting espionage has developed.<sup>107</sup> In fact, the Experts could point to several facts which tended to indicate that such a norm might be developing.<sup>108</sup> Ultimately, however, the Experts concluded that there was insufficient state practice and *opinio juris*<sup>109</sup> to support the conclusion that a norm prohibiting states from engaging in cyber espionage has emerged.<sup>110</sup>

The Experts specifically left open the possibility that cyber espionage might violate international law in the way that it is conducted, however.<sup>111</sup> They indicated that certain methods of cyber espionage may violate principles of international law—particularly sovereignty and the prohibition

---

101. TALLINN 2.0, *supra* note 12, at 168.

102. *Id.* The Experts were careful to caveat their definition and description of cyber espionage in peacetime. More specifically, they cautioned that the term “cyber espionage” was proffered in the *Tallinn Manual* for the purpose of Rule 32 and had no independent legal significance. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. Buchan, *supra* note 27, at 68; *see infra* Part IV (discussing treaties which may be adapted to this purpose).

107. TALLINN 2.0, *supra* note 12, at 169.

108. *Id.* at 169 nn.384 & 386. The Experts indicated a number of instances where states have begun to ban the practice of cyber espionage among themselves. *Id.* at 169 n.386.

109. That is, a subjective belief on behalf of a state that a certain obligation need be followed. *See infra* text accompanying note 265.

110. TALLINN 2.0, *supra* note 12, at 169.

111. *Id.* at 170.

against intervention, which is discussed in the following sections.<sup>112</sup> In addition, the Experts were clear to note that stylizing a cyber operation as espionage does not, thereby, render an otherwise illegal operation legal.<sup>113</sup> In the commentary to Rule 32, they emphasized:

[I]f an aspect of a cyber espionage operation is unlawful under international law, it renders the cyber espionage unlawful. By stylizing a cyber operation as a ‘cyber espionage operation’, a [s]tate cannot therefore claim that it is by definition lawful under international law; its lawfulness depends on whether the way in which the operation is carried out violates any international law obligations that bind the [s]tate.<sup>114</sup>

This construct creates a situation where the severity of damage caused by the espionage does not determine the legality of the act.<sup>115</sup> Instead, the legal analysis centers upon whether the method of cyber espionage violates some other norm of international law. In other words, it does not matter that a state purloined nuclear launch codes via cyber espionage, but if the spying state damages or destroys a computer in the process, then that state has violated the sovereignty of the target state.<sup>116</sup> As another example, if a state uses the premises of a diplomatic post to conduct cyber espionage, that state may be in violation of international law—specifically the Vienna Convention on Diplomatic Relations.<sup>117</sup>

### *B. During Conflict*

The legal framework for cyber espionage in wartime, on the other hand, relies on the adaptation of rules found in the Geneva Conventions and Hague Relations. The espionage provisions found in these two marquee law of armed conflict treaties reflect customary international law.<sup>118</sup> Not surprisingly, *Tallinn 2.0* tracks these rules fairly closely. *Tallinn 2.0* Rule 89 provides, “A member of the armed forces who has engaged in cyber espionage in enemy-controlled territory loses the right to be a prisoner of war and may be treated as a spy if captured before rejoining the armed forces to which

---

112. See *infra* Sections IV.A–B.

113. *TALLINN 2.0*, *supra* note 12, at 170.

114. *Id.*

115. On this point, a minority of the Experts did posit that cyber espionage that seriously undermined the security of a state, such as exfiltration of nuclear launch codes, might be sufficient to violate sovereignty. *Id.* at 171. This was not the dominant position, however. *Id.*

116. Compare *id.* at 173 (noting that an operation which inadvertently damaged a computer in the target state would violate that state’s sovereignty), with *id.* at 171 (noting that a majority of experts opined that cyber espionage of another state’s nuclear launch codes would not per se violate international law).

117. *Id.* at 227–29.

118. *Id.* at 410.

[they] belong[.]”<sup>119</sup> In other words, such an individual is not treated as a member of the armed forces with associated POW treatment and immunity from prosecution as a combatant.

As can be seen when compared with the relevant Geneva and Hague provisions, this Rule is based on the law regarding traditional spying in wartime, which generally provides for immunity for a spy when the spy rejoins the armed forces but otherwise allows a spy to be subject to prosecution under domestic law if apprehended.<sup>120</sup> The Experts were clear that, as applied to cyber espionage, “[t]his Rule is limited to situations in which the individual concerned engages in cyber espionage while in ‘enemy controlled territory.’”<sup>121</sup> As a result, remote cyber operations are not subject to this Rule, as such cyber operators are not operating behind enemy lines and, accordingly, do not need to “rejoin” their armed force. This Rule would then have very limited applicability to situations where a cyber operator was required to clandestinely travel into enemy territory to conduct the necessary operation—such as intercepting signal communication or physical delivery of a flash drive into an enemy system.<sup>122</sup>

Much like peacetime cyber espionage, the *Tallinn 2.0* Experts made clear that cyber spying is not a per se violation of the law of armed conflict, although it is subject to the body of law and may violate its provisions.<sup>123</sup> That is, the spy is neither a war criminal nor is the act of espionage a war crime as in the case of traditional methods of spying.<sup>124</sup> Rule 89 merely concerns the classification of detained personnel. The collection of enemy intelligence during armed conflicts is a long-recognized method of warfare, and this tradition applies equally to the cyber context.<sup>125</sup>

#### IV. CYBER ESPIONAGE: NORMATIVE GAPS, AMBIGUITIES, AND LIMITATIONS

An examination of *Tallinn 2.0*'s treatment of cyber espionage reveals certain normative gaps, ambiguities, and limitations in the application of customary law to digital spying. The struggle to fit cyber espionage into traditional legal underpinnings is evident even from *Tallinn 2.0*'s foundational parameters. Regarding peacetime espionage, for example, the Experts noted

---

119. *Id.* at 409.

120. *Id.* at 411; *see supra* notes 86, 88 and accompanying text.

121. TALLINN 2.0, *supra* note 12, at 411.

122. *Id.*

123. *Id.*

124. LESLIE C. GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 145 (3d. ed. 2008); TALLINN 2.0, *supra* note 12, at 169.

125. TALLINN 2.0, *supra* note 12, at 169.

that cyber espionage can be facilitated in each of the three layers of cyberspace: physical, logical, and social.<sup>126</sup> The physical layer includes the physical network components, such as hardware, cables, routers, servers, and so on. The logical layer includes the connections between networked devices. Finally, the social layer includes all of the individuals and groups that are involved in cyber activities who are susceptible to social engineering attacks.<sup>127</sup> These descriptions used to define modes of cyber espionage in *Tallinn 2.0* serve to underscore the differences between prototypical cyber espionage and traditional espionage.<sup>128</sup> In both, the critical work to conduct the cyber espionage can be completed without stepping foot in the targeted country. While one can conceive of some instances of espionage that may require physical presence, most do not and a prudent cyber spy would take care to avoid such a scenario.<sup>129</sup> Further limitations in *Tallinn 2.0*'s statement of the law become clear when considering the application of existing international legal limits on state behavior.

After examining the current state of international law, the *Tallinn 2.0* Experts concluded that espionage, in peacetime or wartime, does not per se violate international law.<sup>130</sup> That is, the fact that an operation is cyber espionage does not render the operation illegal, but the way in which the operation is carried out may render it unlawful. *Tallinn 2.0* describes specific violations of international law that may be applicable to peacetime cyber espionage operations.<sup>131</sup> As will be seen, the doctrines of sovereignty, non-intervention, and protection of privacy may provide some substantive, albeit imprecisely defined, legal restrictions on state conduct in this field. The issues of non-state actors and the state duty of due diligence, as well as the specific issue of weaponized honeypots, also constitute important legal considerations.

#### A. *State Sovereignty*

In the case of peacetime espionage, the most likely international legal provision to be implicated is that of sovereignty. A cornerstone of international law, this precept protects nations from unwanted intrusions by foreign states.<sup>132</sup> The protection of sovereignty is noted in Rule 4 of *Tallinn 2.0*,

---

126. *Id.* at 168–69.

127. *Id.*

128. *Id.* at 169–70.

129. In fact, the five Chinese officers recently indicted by the United States for hacking American companies all allegedly conducted their criminal acts while sitting at a workstation in Beijing. See *infra* notes 249–251 and accompanying text.

130. *TALLINN 2.0*, *supra* note 12, at 410.

131. *Id.* at 170–71.

132. Speaking to the foundational importance of sovereignty in international law, scholar Russell Buchan observed,

which provides: “A [s]tate must not conduct cyber operations that violate the sovereignty of another [s]tate.”<sup>133</sup> The *Tallinn 2.0* Experts did not precisely delineate when a cyber operation would constitute a violation of sovereignty. At a minimum, a violation of sovereignty would occur “when one [s]tate’s cyber operation interferes with or usurps the inherently governmental functions of another [s]tate.”<sup>134</sup> In addition, sufficient “infringement upon the target [s]tate’s territorial integrity”<sup>135</sup> would also qualify. While the degree necessary to constitute a sufficient infringement upon territorial integrity was not specified, the Experts identified three levels of possible infringement: “(1) physical damage; (2) loss of functionality; and (3) infringement upon territorial integrity falling below the threshold of loss of functionality.”<sup>136</sup>

One type of cyber espionage operation that might implicate sovereignty is the operation that physically takes place in the sovereign territory of the target nation. The Experts were divided on whether such an operation violated sovereignty, but the majority believed that it did in fact violate the precept.<sup>137</sup> For example, in a cyber espionage operation by an agent of one state that is physically present in the targeted state, the majority of Experts were of the view that such conduct would violate the principle of sovereignty.<sup>138</sup> The rationale is that if agents of one state are physically present in another state’s territory and conduct cyber operations without consent or other legal justification, the targeted state’s sovereignty has been violated by the former state.<sup>139</sup> The minority, however, took the position that “extensive [s]tate practice of conducting espionage on [a] target [s]tate’s territory has created an exception to the generally accepted [view] that non-consensual activities attributable to a [s]tate while physically present on another[] [state’s] territory

---

The principle of state sovereignty is often regarded as a constitutional norm of international law and is the basis ‘upon which the whole of international law rests.’ However, ‘[s]overeignty has different aspects’ and in order to protect the different features of state sovereignty the international community has developed various principles of international law. These include the principle of territorial sovereignty, which protects the territory of a state from external intrusion; the principle of non-intervention, which protects the political integrity of a state from coercion; the prohibition against the use of force, which protects states against the use of violence, and where the use of violence is of sufficient scale and effects international law casts such conduct as an armed attack entitling the victim state to use force in self-defence.

Buchan, *supra* note 27, at 68 (alteration in original) (footnotes omitted) (first quoting *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 263 (June 27); then quoting OPPENHEIM’S INTERNATIONAL LAW 382 (Robert Jennings & Adam Watts eds., 9th ed. 1996)).

133. TALLINN 2.0, *supra* note 12, at 17.

134. *Id.* at 21.

135. *Id.* at 20.

136. *Id.*

137. *Id.* at 19–20.

138. *Id.* at 19.

139. *Id.*

violate[s] sovereignty.”<sup>140</sup> Interestingly, the majority’s view indicates that they would consider most traditional methods of espionage to be violations of the doctrine of sovereignty, as they tended to occur within the territorial jurisdiction of the victim state.<sup>141</sup>

The more relevant and pressing issue of remote cyber espionage similarly caused cognitive dissonance for the Experts. They could not achieve consensus on the issue of whether remote cyber espionage could reach a particular threshold of severity and, thereby, violate the sovereignty of the targeted state.<sup>142</sup> In a hypothetical provided by the Experts, a state remotely accesses another state’s military or intelligence cyber systems and exfiltrates significant amounts of highly classified data over an extended period of time.<sup>143</sup> The majority of Experts believed that the exfiltration did not violate the targeted state’s sovereignty and, what is more, the legal issue was not one of severity but of the method employed.<sup>144</sup> Interestingly, a few of the Experts were of the opinion that if the consequences suffered by the cyber espionage were so severe—if large amounts of classified data were exfiltrated over a long period, for example—it would amount to a violation of sovereignty regardless of the method used.<sup>145</sup> Under this sovereignty approach, important factors would include whether computer systems were damaged or destroyed—not the nature, quality, or quantity of information purloined.<sup>146</sup>

On the other hand, if a remote cyber espionage operation results in a loss of functionality within a state’s digital infrastructure, the Experts agreed that it may constitute a violation of that state’s sovereignty.<sup>147</sup> This is true regardless of whether the infrastructure is owned by the country itself or private industry.<sup>148</sup> This finding is in line, generally, with *Tallinn 2.0*’s guidelines regarding sovereignty in the context of any type of cyber operation.<sup>149</sup>

---

140. *Id.* There are significant pitfalls to such an approach, particularly the danger that such an exception would swallow Rule 4 and undermine the entire concept of sovereignty. Perhaps anticipating such an objection, the minority stressed that this exception is narrow and limited to espionage. *Id.*

141. The literature on this issue does not seem to strongly support the majority view. *See supra* notes 69–74 and accompanying text.

142. *TALLINN 2.0*, *supra* note 12, at 170.

143. *Id.* at 170–71.

144. *Id.*

145. *Id.* at 171.

146. This understanding would give small consolation to states who have suffered massive data losses due to foreign hacking.

147. *Id.* at 170.

148. *Id.* at 14.

149. *See id.* at 20–21 (stating that “the remote causation of loss of functionality of cyber infrastructure located in another [s]tate sometimes constitutes a violation of sovereignty”).



It remains unclear, however, the exact threshold needed to constitute a violation of sovereignty in this way.<sup>150</sup> According to the Experts, a cyber operation that necessitates repair to physical components of the digital infrastructure amounts to a violation.<sup>151</sup> However, no consensus was reached as to whether a breach of sovereignty has occurred when an operation merely necessitates reinstallation of a computer operating system, for example.<sup>152</sup> Further, the Experts could not reach a consensus on cyber espionage operations that install “backdoors” to access data, cause cyber programs to operate in a different manner, or activities which alter or delete data stored within the cyber infrastructure.<sup>153</sup> Legal nuances surrounding the effects of various means of digital espionage remain uncertain.

### B. *Non-Intervention*

In addition to sovereignty, customary international law also establishes the principle of non-intervention—that is, a state must not interfere in the affairs of another state.<sup>154</sup> Violation of this principle requires the offending state, or individual acting at the behest of that state, to act coercively in the internal or external affairs of the victim state.<sup>155</sup> The Experts paid considerable attention to the issue of state non-intervention in regards to cyber operations.<sup>156</sup> For the specific issue of cyber espionage, they were of the opinion that it does not qualify per se as intervention, as it is not necessarily coercive in nature.<sup>157</sup> However, certain activities within the realm of cyber espionage may rise to the level of state intervention. For example, the majority of Experts posited that in the event one state gained access to another state’s government computer system, accessed sensitive domestic intelligence data, and then made such records public, that activity could constitute unlawful intervention if the goal was to alter an internal political debate over the victim state’s surveillance practices.<sup>158</sup> On the other hand, mere intrusion into a foreign nation’s cyber infrastructure, which necessitates breaching cyber barriers—including overcoming firewalls or password protection—would be inadequate to qualify as intervention.<sup>159</sup>

Unfortunately, *Tallinn 2.0* gives little attention to the possibility of economically-oriented espionage, including theft of trade secrets and intellectual

---

150. *Id.* at 21.

151. *Id.*

152. *See id.* (noting that an intrusive cyber activity that merely required a “reboot” would probably not qualify as a violation of sovereignty).

153. *Id.* at 21.

154. *Id.* at 312.

155. *Id.* at 314.

156. *Id.* at 323.

157. *Id.*

158. *Id.* at 320.

159. *Id.* at 323.

property, which may rise to the level of intervention.<sup>160</sup> Indeed, it is likely that economic and industrial espionage pose a particularly vexing problem in terms of intervention, as these activities are likely to financially disadvantage the victim state and ultimately impact that state's economic and trade policies.<sup>161</sup> Significant ambiguity persists regarding this issue.

### C. *Non-State Actors and Due Diligence*

The legal category of "espionage" presupposes conduct by a state agent or a person acting under the direction of a state. The theft of government or industry secrets by individuals acting in a private capacity is just that: theft. Likewise, non-state actors hacking into foreign government or corporate network does not constitute espionage, but it is commonly proscribed by domestic law.<sup>162</sup> The international law precept of due diligence, however, requires states to ensure that their own territory and other objects<sup>163</sup> over which they have control are not used in a way that harms other states.<sup>164</sup> Does this principle require states, in the absence of a treaty agreement on point, to end the digital theft by domestic non-state actors when their conduct harms foreign nations? In the view of the Experts, states may violate the principle of due diligence if domestic non-state actors conduct operations which result in serious adverse consequences and affect the rights of a target state.<sup>165</sup> The exact threshold of "serious adverse consequence[]" is unsettled in international law<sup>166</sup> and poses a challenging issue in the arena of cyber hacking. The Experts agreed that cyber operations that result in a major impact to a state's economy, or one that severely disrupts government functions or business, may be sufficient to trigger the rule.<sup>167</sup>

The Experts were careful to specify, however, that the precept of due diligence is only implicated when a non-state actor engages in an activity that, if done by the territorial state, would breach an international legal obligation, such as violating sovereignty or would constitute intervention.<sup>168</sup> Thus, digital intelligence gathering by non-state actors may be a violation of

---

160. The International Court of Justice specifically included economic intervention in its list of possible unlawful state actions. See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, 108, ¶ 205 (June 27).

161. Lotrionte, *supra* note 4, at 503. Other coercive goals could include destabilization of the victim state's economy or preventing the state from regulating its own economic affairs. *Id.* at 508–09.

162. See, e.g., 18 U.S.C. § 1030(a)(1)–(a)(4) (2012); 18 U.S.C. § 2511 (2012).

163. Objects may include government cyber infrastructure located onboard sea vessels, on foreign military installations, or in international airspace. See *TALLINN 2.0*, *supra* note 12, at 33.

164. *Id.* at 30.

165. *Id.* at 35.

166. *Id.* at 36–37.

167. *Id.* at 38.

168. *Id.* at 36.

domestic law, but in itself does not trigger the due diligence rule absent specific unlawful activity. Like state espionage, digital intrusions by non-state actors only run afoul of international law when specific conduct violates other international legal provisions. In that case, the territorial state has the obligation to take feasible measures to end the offending cyber operation.<sup>169</sup>

#### *D. Right to Privacy*

Customary international law also restricts states in terms of affirmative human rights guarantees.<sup>170</sup> Importantly for this discussion, the Experts opined that the status of economic rights is unclear as a matter of customary law.<sup>171</sup> Instead, such rights are subject to the provisions of state treaty commitments.<sup>172</sup> The right to privacy, however, is more established. Cyber espionage activities may implicate the right to individual privacy, although espionage itself does not per se violate the rule.<sup>173</sup> The Experts agreed that the right to privacy is one guaranteed by customary international law, but that its scope is not well-defined.<sup>174</sup> The legality of examining the content of electronic communications, particularly, is complicated by whether such data was inspected by humans or machines.<sup>175</sup> The Experts agreed that the collection of personal data of individuals did implicate this right—although they were unable to agree on a definition of “personal data.”<sup>176</sup> Collection of metadata may violate this rule if it is later linked to an individual and has a nexus to that individual’s private life.<sup>177</sup> Notably, the right to privacy is not absolute and may be subject to some limitations, including national security justifications.<sup>178</sup>

The Experts cautioned, however, that the application of this body of law is significantly limited by territorial concerns.<sup>179</sup> The majority agreed that customary international human rights law applies to persons within a state’s territory as well as within the physical territory where that state exercises “power or effective control.”<sup>180</sup> The Experts could not reach a consensus on whether state cyber activities could constitute such power or effective control over territory or persons as opposed to physical power or control, triggering the applicability of this customary rule—although the majority rejected this

---

169. *Id.* at 43.

170. These rights include certain civil, political, economic, social, and cultural rights. *Id.* at 187.

171. *Id.* at 194.

172. *Id.*

173. *Id.* at 193.

174. *Id.*

175. *Id.* at 190.

176. *Id.* at 191.

177. *Id.* at 192.

178. *Id.* at 189, 202–03.

179. *Id.* at 182–85.

180. *Id.* at 184.

contention.<sup>181</sup> The majority believed that physical control over territory or an individual person was necessary to trigger international human rights laws.<sup>182</sup> In fact, the Experts noted a lack of evidence evincing an *opinio juris* that state intelligence-gathering activities directed at persons on foreign territory triggered the international right to privacy.<sup>183</sup> In other words, the right to privacy does not likely apply extraterritorially in most cases of international digital spying. This finding indicates that the current legal understanding may not effectively limit foreign cyber intelligence collection by states.

#### *E. Honeypots*

Another interesting cyber espionage issue raised by the Experts is that of a “weaponized” honeypot. These devices may be used by states to deter and punish foreign cyber espionage attempts. *Tallinn Manual 2.0* defines a honeypot as a deception technique to defend a computer system against malicious operations that use a physical or virtual environment designed to lure the attention of intruders with the aim of deceiving the intruders about the nature of the environment.<sup>184</sup> Honeypots can be created for the purpose of wasting intruder resources, for gathering counter-intelligence information about the intruder’s intent, and for identifying the individual’s means and methods of cyber operations.<sup>185</sup> A weaponized honeypot is one that contains files that, once exfiltrated, will cause significant disruption and damage to the intruder’s own cyber system.<sup>186</sup> Again, the Experts were divided in terms of how international law applies to this twist to cyber espionage.<sup>187</sup> A minority of Experts opined that the state that created the honeypot, at least, violated the sovereignty of the intruding state. Their theory was that the state that created the honeypot set in motion the events and are, therefore, responsible under the law of state responsibility for an internationally wrongful act.<sup>188</sup> The majority saw this issue rather differently. They believed that the intruding state factually transmitted the weaponized files into their own cyber infrastructure. As such, the state that created the honeypot and laid the trap did not, in fact, conduct the actual activity that caused the harm.<sup>189</sup>

In sum, although peacetime cyber espionage by states is not a per se violation of international law, it is inextricably linked and intertwined with

---

181. *Id.* at 185.

182. *Id.*

183. *Id.*

184. *Id.* at 565.

185. *Id.*

186. *Id.*

187. *Id.* at 150–52.

188. *Id.*

189. *Id.*

other internationally prohibited conduct. The legality of peacetime cyber espionage operations is dependent upon the specific conduct used to accomplish the act of espionage—in other words, whether specific activities associated with the espionage violate some norm of international law. The unsettled limits of these provisions raise serious concerns about the current state of the law.

*F. Application in Times of Conflict*

The *Tallinn 2.0* legal framework for wartime cyber espionage differs substantially from the preceding analysis. Rather than providing a possible legal basis for declaring particular cyber espionage operation unlawful, it closely tracks the existing law as applied to the status of spies during wartime.<sup>190</sup> In other words, the framework is primarily about the status of captured personnel, rather than the legality of state conduct. Because they are grounded on geographic location and the spy's return to their military as a key trigger to immunity, the existing rules do not translate well to the digital context. This Section will examine *Tallinn 2.0's* cyber espionage rules in wartime, noting the incongruities that render this law difficult to apply. The gaps, ambiguities, and limitations of cyber espionage in the context of armed conflict are largely a function of a discord between traditional notions of spying in warfare and the realities of cyber espionage.

The primary mismatch is the geographical limitation trigger for spying under the law of armed conflict. For example, Hague Regulation Article 29 specifies that the spy must obtain or endeavor to obtain information “in the zone of operations of a belligerent.”<sup>191</sup> Similarly, Article 46 of Additional Protocol I uses somewhat comparable language: “[T]erritory controlled by an adverse Party” to convey a similar idea.<sup>192</sup> Because the aim of the Experts in the *Tallinn Manual 2.0* is to state the *lex lata*, Rule 89 appropriately incorporates the geographical limitation by specifying “who has engaged in cyber espionage in enemy-controlled territory.”<sup>193</sup> The Experts were also careful to note that cyber espionage performed from outside enemy territory does not violate Rule 89.<sup>194</sup> The geographical limitation trigger for wartime cyber espionage is problematic and somewhat anachronistic when applied to cyber espionage. One of the primary features and benefits of cyber operations generally, and cyber espionage specifically, is the ability to operate remotely. To gather intelligence and other information, cyber spies can and do operate

---

190. *Id.* at 409–12.

191. Hague IV, *supra* note 85, art. 29.

192. Additional Protocol I, *supra* note 88, art. 46(2).

193. TALLINN 2.0, *supra* note 12, at 409.

194. *Id.* at 411.

from virtually anywhere. Aside from speed and anonymity, having the ability to act remotely and achieve the same effects is one of the game-changing advantages of using digital means.

Cyber capabilities may lessen the need to employ human resources on the ground in conflict zones. One of the last places a cyber spy would want to be is in enemy territory. The Experts acknowledged that given the geographical limitation to enemy-controlled territory, cyber spying would most likely occur as a so-called “close access cyber operation,” which requires physical proximity to the targeted system.<sup>195</sup> The example provided by the Experts involved a member of the armed forces using a flash drive to access a computer system or intercepting signals while acting clandestinely.<sup>196</sup> To the extent that a spy is doing a close access cyber operation or intercepting signals, the cyber aspect of the espionage mission is not particularly unique or dispositive relative to other types of spying activities. Put in a slightly different way, the close access operation is just another way of gathering intelligence, analogous to taking pictures, drawing maps, or stealing documents. It lacks some of the defining and most important characteristics of the pertinent digital context.

A second, and related, mismatch involves the requirement that the act of espionage must be carried out “clandestinely or under false pretences.”<sup>197</sup> To provide clarity to the meaning of the “clandestinely or under false pretences,” the Experts explained:

“Clandestinely” refers to activities undertaken secretly or secretly, as with a cyber espionage operation designed to conceal the identity of the persons involved or the fact that it has occurred. An act of cyber information collection is “under false pretences” when conducted so as to create the impression that the individual concerned is entitled to access the information in question.<sup>198</sup>

It is somewhat obvious that acting “clandestinely or under false pretences” in the real world is a rather different situation than in a virtual one. This can be seen with three hypothetical situations. In the first hypothetical, a combatant, operating behind enemy lines, takes off their uniform and dons civilian clothing to facilitate sneaking into enemy headquarters with a flash drive to steal plans from the enemy’s computer system. This hypothetical represents a clear case of spying under the law of armed conflict. Upon capture, the combatant has lost their combatant immunity and POW status and can be prosecuted under the domestic criminal law of the enemy state. In the second hypothetical, the only difference is the combatant neither takes off their uniform nor puts on civilian clothes. In this case, upon almost certain

---

195. *Id.*

196. *Id.*

197. *Id.* at 168.

198. *Id.* at 410 (footnotes omitted).

capture in the headquarters, the combatant is not a spy and retains combatant immunity and POW status. In the third hypothetical, the combatant, while operating behind enemy lines, continues to wear their uniform. The combatant is a computer specialist attempting to intercept enemy signals messages. While online, they act anonymously to steal enemy passwords that give them access to classified enemy communications. The combatant is captured by the enemy while still wearing their uniform and before they rejoin their army.

The third hypothetical is somewhat problematic because, in the real world, the combatant did not act “clandestinely or under false pretences.” They continued to wear a uniform to distinguish themselves as a combatant. In cyberspace, they absolutely acted secretly or secretively to conceal their identity during this mission to intercept enemy signals. Moreover, by stealing the enemy’s passwords, they created the impression that they were entitled to access to the enemy’s network and information. Given those facts, is the combatant now a spy subject to prosecution, even though, to the outside world, they appeared to be a combatant for the duration of the operation?

Complicating the third hypothetical further is the concept of ruses under the law of armed conflict. Ruses are acts intended to mislead an adversary or to induce them to act recklessly but which infringe no rule of the law of armed conflict.<sup>199</sup> Examples of ruses in armed conflict are “the use of camouflage, decoys, mock operations and misinformation.”<sup>200</sup> *Tallinn Manual 2.0*, Rule 123, provides examples of permissible ruses in cyberspace, including using false computer identifiers, networks, and transmissions, as well as enemy codes, signals, and passwords.<sup>201</sup> The third scenario represents an important, but blurry, intersection between the rules regarding spying and ruses. Given the facts in the third hypothetical, it is very difficult to conclude such conduct would amount to spying under Rule 89.

A final issue that divided the Experts involved the nature of the information collected. The majority of the Experts believed that the nature of the information collected has no bearing on the characterization of the activities as cyber espionage.<sup>202</sup> The only stipulation was that it had to be collected on behalf of a party to the international armed conflict.<sup>203</sup> Alternatively, the minority thought that the information involved must have some military value.<sup>204</sup> This lack of consensus among the Experts further muddies the water of the legal parameters of espionage during wartime.

While reflecting on the *lex lata* of espionage, the Experts’ formulation unfortunately does not effectively address several unique problems raised by

---

199. Additional Protocol I, *supra* note 88, art. 37(2).

200. *Id.*

201. TALLINN 2.0, *supra* note 12, at 495–96.

202. *Id.* at 412.

203. *Id.*

204. *Id.*

the realities of the digital environment. Particularly, *Tallinn 2.0*'s discussion of wartime espionage is inapposite to the current developments, as it heavily relies on the aforementioned "behind enemy lines" nexus. The next Part of this Article considers these dynamics and proposes a path ahead for the *lex ferenda* as states begin to substantively grapple with the current state of the law.

## V. THE ROAD AHEAD: THE *LEX FERENDA*

### A. *Political and Military-Based Cyber Espionage*

Considerable ambiguity continues to exist regarding the legal limits of cyber espionage, both in peacetime and during conflict, after *Tallinn 2.0*. Importantly, however, traditional methods of espionage have always existed in a relative "black hole" of legality—domestically, but not internationally, proscribed and widely practiced.<sup>205</sup> The current legal framework for cyber espionage offers wide leeway and interpretive flexibility for states. In the absence of voluntary change in practice, international agreement, or emerging legal custom, states will likely continue to comfortably operate within the uncertain sphere of cyber espionage, conducting intelligence-gathering operations against foreign nations, institutions, and individuals. In particular, nations will continue foreign digital spying in order to gain military and political advantages, and to maintain national interests and security. This conduct is strongly rooted in history, and nations continue to have powerful justifications for widespread intelligence collection in the modern day.<sup>206</sup>

Indeed, there exist few intrinsic disincentives to cease these long-practiced activities.<sup>207</sup> In fact, cyber capabilities have somewhat mitigated the risk for state-sponsored spies in terms of potential for capture. Further, attribution problems in cyber operations make it difficult for states to ensure

---

205. See *supra* Part II.

206. See, e.g., Ellen Nakashima, *Officials: Surveillance Programs Foiled More Than 50 Terrorist Plots*, WASH. POST (June 18, 2013), [https://www.washingtonpost.com/world/national-security/officials-surveillance-programs-foiled-more-than-50-terrorist-plots/2013/06/18/d657cb56-d83e-11e2-9df4-895344c13c30\\_story.html?utm\\_term=.8d1ad55a31c7](https://www.washingtonpost.com/world/national-security/officials-surveillance-programs-foiled-more-than-50-terrorist-plots/2013/06/18/d657cb56-d83e-11e2-9df4-895344c13c30_story.html?utm_term=.8d1ad55a31c7) (discussing congressional testimony by National Security Agency officials that the agency's surveillance activities had thwarted more than fifty incidents of terrorism).

207. Conversely, some scholars have theorized that states should have strong intrinsic interests in solidifying the rules of state-sanctioned espionage even in security-related intelligence gathering, apart from political pressures. Most convincingly, clear legal guidelines would facilitate intelligence sharing between allies where one state has been previously restricted in doing so by domestic legal concerns over the second state's surveillance activities. See Deeks, *supra* note 3, at 315–16 (noting particularly condemnation of surveillance practices carried out by the United States and the United Kingdom). Additionally, states would benefit by tighter control of foreign surveillance over their own citizens. *Id.* at 326. At least one head of state, for example, has expressed the view that multiple practices involved in cyber intelligence gathering, such as foreign electronic surveillance, violate international law. U.N. GAOR, 68th Sess., 5th plen. mtg. at 7, U.N. Doc. A/68/PV.5 (Sept. 24, 2013).



foreign compliance with any future international agreements, reducing the benefit of entering into arrangements that would limit their own intelligence-gathering operations.<sup>208</sup> Additionally, states and corporations will continue to be subject to malevolent cyber intrusions from private entities—both foreign and domestic—necessitating major investments in cyber security regardless of existing international agreements that limit state conduct. Therefore, despite major gaps and mismatches in the existing legal framework, nations generally lack robust motivations to close them. Political influences, however, including public opposition from citizens, humanitarian groups, and foreign leaders may effectively curb some of the most concerning state practices.<sup>209</sup>

Internal and external political pressures can result in changes to domestic law and policy. So-called “naming and shaming” has been influential in the modification of the U.S. government’s own surveillance policies, for example, after it faced enormous public backlash at home and abroad in the wake of Edward Snowden’s disclosures.<sup>210</sup> Electronic surveillance practices may be uniquely susceptible as the target of grassroots “naming and shaming” campaigns because they directly implicate the privacy of individuals.<sup>211</sup> Traditional methods of espionage, on the other hand, rarely reached far into the private sphere.<sup>212</sup> Although the Experts stated that the international customary right to privacy was not effectively implicated due to the extraterritorial nature of foreign cyber espionage, states will likely be subject to considerable public pressure to limit these activities even in the absence of applicable law on point.<sup>213</sup> Additional influences from corporations who risk losing business due to state surveillance practices that infringe upon privacy may also spur domestic change.<sup>214</sup>

---

208. Indeed, the advent of cyber capabilities may exacerbate this long-standing source of state reluctance to adopt espionage-limiting agreements. *See supra* notes 73–76 and accompanying text. *See generally* William Banks, *State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0*, 95 TEX. L. REV. 1487 (2017) (discussing the critical role of cyber attribution in state responses to cyber operations and the difficulties in establishing proper attribution).

209. Deeks, *supra* note 73, at 635–36.

210. *See* Sarah Childress, *How the NSA Spying Programs Have Changed Since Snowden*, FRONTLINE (Feb. 9, 2015), <https://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/> (chronicling the changing in surveillance policy resulting from domestic and international backlash over the Snowden leaks). This event also prompted other state governments to likewise re-examine their surveillance policies. Deeks, *supra* note 73, at 636 (citing David Omand, *Understanding Digital Intelligence and the Norms that Might Govern It*, in GLOBAL COMM’N ON INTERNET GOVERNANCE, at 17 (Paper Ser. No. 8, 2015), [https://ourinternet-files.s3.amazonaws.com/publications/gcig\\_paper\\_no8.pdf](https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no8.pdf)).

211. *See* Deeks, *supra* note 3, at 319.

212. *See id.*

213. *See id.* at 297 (noting that democratic nations are more susceptible to public pressures in this regard as compared to non-democratic and partly-democratic states, such as Russia and China).

214. *Id.* at 338–39 (stating that the profits of domestic technology firms may be undermined due to reluctance by foreign entities to allow data to be stored within the United States where it will be subject to surveillance).

Concerning espionage conducted for the purposes of accessing foreign state political and military secrets, then, country practices will ultimately be limited by a combination of legal interpretation and policy objectives—themselves shaped by diplomatic concerns and internal political factors. These same pressures may eventually persuade states to enter into multilateral agreements restricting some offensive forms of cyber espionage by the major world players—particularly those practices that most infringe on privacy—but that possibility seems remote at the present time.<sup>215</sup> States may instead agree to limit espionage in this realm with strategic partners, as these agreements may be in the best interests of states and tend to bolster collective national security frameworks.<sup>216</sup>

---

215. See *infra* note 270 and accompanying text. Existing treaty laws do, to some extent, circumscribe some state surveillance activities. The International Covenant on Civil and Political Rights (“ICCPR”), for example, is a rights-based treaty which states that “[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.” International Covenant on Civil and Political Rights, art. 17(1), Dec. 16, 1966, 999 U.N.T.S. 171, 6 I.L.M. 368. Most states are a party to this treaty, including the United States and Russia. *International Covenant on Civil and Political Rights*, UNITED NATIONS TREATY COLLECTION 2, 3, <https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20IV/IV-4.en.pdf> (last visited Jan. 1, 2019). The article covers surveillance conducted within a state against persons within that state, whether citizen or not. Considerable debate, however, surrounds the standard of state “arbitrariness” necessary to violate this provision. The United States’ position is that the ICCPR does allow interference by states as long as it is in accordance with transparent laws and for a legitimate state purpose. *United States Response to OHCHR Questionnaire on “The Right to Privacy in the Digital Age,”* UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMM’R FOR HUMAN RIGHTS, <http://www.ohchr.org/Documents/Issues/Privacy/United%20states.pdf> (last visited Jan. 1, 2019). The European Court of Human Rights (“ECtHR”) disagrees, stipulating that the lawful state interference must be necessary, proportional, and accomplished according to well-tailored laws. See Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT’L L.J. 81, 133 (2015); see also Deeks, *supra* note 3, at 305–06. Such difference in interpretation may result in disparate legal analyses on issues such as bulk intelligence gathering against individuals. Deeks, *supra* note 3, at 306. Most problematically, there is little consensus among scholars whether the ICCPR applies extraterritorially, thus limiting foreign surveillance activities. *Id.* at 306–07. The United States maintains that it does not apply extraterritorially. *Id.* at 307. The United Nations (“UN”) Human Rights Committee, charged with overseeing state compliance with ICCPR, made concluding observations regarding the United States, recommending that the country take measures to ensure it was conforming to the covenant in its foreign surveillance activities. Human Rights Comm., Concluding Observations on the Fourth Periodic Rep. of the United States, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014), <https://undocs.org/CCPR/C/USA/CO/4>. It is the UN’s position, then, that it does apply extraterritorially. Short of a treaty amendment, this jurisdictional hurdle makes the ICCPR inadequate to address the most pervasive and troubling, at least to states, forms of surveillance—those happening across international borders.

216. For example, the United States, United Kingdom, Australia, Canada, and New Zealand—the so-called “Five Eyes”—established a pact to refrain from spying on one another. See Margaret Warner, *An Exclusive Club: The Five Countries That Don’t Spy on Each Other*, PBS (Oct. 25, 2013), <https://www.pbs.org/newshour/world/an-exclusive-club-the-five-countries-that-dont-spy-on-each-other>.

### B. *Espionage in Wartime*

The object of much less public attention, rules regarding wartime espionage are unlikely to face political pressure of the nature described above. Importantly, gaps in wartime cyber espionage discussed in the previous Part do not seem to expose particularly pressing matters in the international legal order. That is, although the rules are quite limited in application, and do not fit well with the realities of most cyber operations, they do not pose especially disturbing concerns for military leaders. Espionage in wartime is primarily an issue of personnel status—whether a captured spy will receive formal POW treatment and immunity from prosecution—rather than a restriction on state conduct. In reality, the capture of an enemy cyber spy, whether territorially or extraterritorially, will likely be a remote possibility. Further, the issue of personnel classification is relatively untroubling in most cases, as the policy of many nations is to give “POW-like” status to all detainees, regardless of actual technical status.<sup>217</sup> Additionally, the rules regarding wartime cyber spying, as in traditional wartime spying, are only applicable in international armed conflicts, not the more common non-international armed conflicts that primarily exist globally today.<sup>218</sup> As a result, it is unlikely that states will advocate for adjusting this legal regime in the near future. It may be possible that wartime cyber espionage will be addressed as part of a comprehensive legal agreement, should there be sufficient pressure to produce a multilateral treaty addressing the many problems endemic to the application of conventional laws of armed conflict to cyber warfare.<sup>219</sup> In the interim, much like other law of war matters, one should expect that the legal framework will evolve in response to discrete issues as they arise.

### C. *The Unique Case of Cyber Economic Espionage*

Economic and industry-based cyber espionage, on the other hand, have emerged as a uniquely problematic practice on the international stage. For many states, economic cyber espionage is unacceptably laden with risk, offers limited value,<sup>220</sup> and is less predictable and domestically controllable

---

217. See generally Derek Jinks, *The Declining Significance of POW Status*, 45 HARV. INT’L L.J. 367 (2004).

218. See, e.g., David Wallace et al., *Trying to Make Sense of the Senseless: Classifying the Syrian War Under the Law of Armed Conflict*, 25 MICH. ST. INT’L L. REV. 555, 593 (2017) (classifying the hostilities in Syria as primarily non-international armed conflicts); Nathalie Weizmann, *Why U.S. Being a Party to Armed Conflict in Afghanistan May Not End Soon*, JUST SECURITY (Jan. 7, 2015), <https://www.justsecurity.org/18904/u-s-forces-transition-drawdown-afghanistan/> (assuming that at least one non-international armed conflict is occurring and will continue to occur in Afghanistan).

219. See, e.g., Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 877 (2012) (discussing the desirability and proposed parameters of such a treaty).

220. Motivations to curb economic espionage, however, may ultimately be linked to the relative risks versus rewards that the practice offers individual countries. See Goldsmith, *supra* note 51, at

than traditional espionage for the purpose of national security.<sup>221</sup> Numerous countries have begun to seek both domestic and international solutions to this issue.

Worldwide, government officials have taken strong positions against commercial spying.<sup>222</sup> Based on this emerging sentiment, states may agree to distinguish traditional economic intelligence gathering from all other kinds and regulate breaches through multilateral treaties.<sup>223</sup> In practical terms, the content of agreements and likelihood of compliance will be rooted in the relative interests, risks, and incentives facing individual states.<sup>224</sup> Based on this assumption, it seems unlikely that the major players in international cyber espionage, including the United States, United Kingdom, China, and Russia, would unanimously agree to a comprehensive set of limitations.<sup>225</sup> One rather surprising development in this area, however, is the 2015 cyber agreement between the United States and China. In an effort to stem the tide of pernicious cyber espionage, both governments agreed that neither would support nor conduct cyber-enabled theft of intellectual property.<sup>226</sup> China replicated these efforts with both Canada and the United Kingdom.<sup>227</sup> Given the

---

44–45 (noting that the United States has much to lose, but little to gain, in the field of economic espionage). State governments with a strong nexus to domestic industry understandably stand to benefit the most from these activities.

221. Most national governments do not have control over the cyber infrastructure used by domestic firms. Some, like the United States, have made recent attempts to strengthen ties to private companies to ensure robust cyber security on these private networks. *See generally* Madeline Carr, *Public-Private Partnerships in National Cyber-Security Strategies*, 92 INT'L AFF. 43 (2016).

222. *See* Ellen Nakashima, *World's Richest Nations Agree Hacking for Commercial Benefit Is Off-Limits*, WASH. POST (Nov. 16, 2015), [https://www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b\\_story.html](https://www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html).

223. *See* William C. Banks, *Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage*, 66 EMORY L.J. 513, 523 (2017).

224. Deeks, *supra* note 3, at 338–40.

225. *Id.* at 339–40.

226. Press Release, Office of the Press Sec'y, FACT SHEET: President Xi Jinping's State Visit to the U.S. (Sept. 25, 2015), <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>. According to the statement, "[N]either 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." *Id.* Ambiguity exists as to the interpretation of this agreement's terms. *See* Jack Goldsmith, *Correction/Update: China Did Accept the American Formulation in the Cyber Deal*, LAWFARE (Sept. 27, 2015, 9:50 PM), <https://www.lawfareblog.com/correctionupdate-china-did-accept-american-formulation-cyber-deal>.

227. *See* *China, Canada Vow Not to Conduct Cyber Attacks on Private Sector*, REUTERS (June 25, 2017), <https://www.reuters.com/article/us-canada-china-cyber/china-canada-vow-not-to-conduct-cyber-attacks-on-private-sector-idUSKBN19H06A>; Foreign & Commonwealth Office, *UK-China Joint Statement on Building a Global Comprehensive Strategic Partnership for the 21st Century*, GOV.UK (Oct. 22, 2015), <https://www.gov.uk/government/news/uk-china-joint-statement-2015>; *U.S.-China Cyber Deal Takes Norm Against Last Economic Espionage Global*, COUNCIL ON

magnitude and length of China's pattern of cyber espionage abuses, however, it is easy to be skeptical of these agreements.<sup>228</sup> Of note, diplomatic agreements such as these may not be legally binding.<sup>229</sup>

One challenge in regulating economic cyber espionage is drawing clear distinctions between permissible and impermissible conduct.<sup>230</sup> For example, collecting data regarding the private manufacture or flow of certain goods that may be used by a state's military, such as aircraft or satellites, may be of both economic and national security consequence. Likewise, information about trade negotiations, a foreign state's gold reserves, or plans to alter prevailing interest rates are also of strategic significance.<sup>231</sup> It would be difficult to accurately define the parameters of acceptable data collection, since commercial information commonly does have some nexus to national security. Nations could agree that although economic data may be collected, it must not be used to benefit or advantage domestic companies. For example, although the United States has consistently engaged in intelligence gathering with a nexus to the activities of foreign businesses, including investigating private industry corruption that impacts U.S. interests, it has also consistently reaffirmed that the information is not shared with private corporations for their financial benefit.<sup>232</sup> Compliance with a distinction like this would understandably be complicated in states with strong ties between government and industry. Assuming that a line could be agreed upon and defined—by crafting limits based on the intent, purpose, or effect of economic intelligence gathering, for example<sup>233</sup>—there are numerous possible mechanisms for international legal codification and enforcement.

---

FOREIGN REL. (Sept. 28, 2015), <https://www.cfr.org/blog/us-china-cyber-deal-takes-norm-against-economic-espionage-global>.

228. Fundamentally, it is unclear what benefit China would reap by complying with this agreement other than avoiding public international condemnation. See Jack Goldsmith, *China and Cybertheft: Did Action Follow Words?*, LAWFARE (Mar. 18, 2016, 9:26 PM), <https://www.lawfareblog.com/china-and-cybertheft-did-action-follow-words>. Data does indicate a drop in Chinese commercial theft after the adoption of this agreement. See David E. Sanger, *Chinese Curb Cyberattacks on U.S. Interests, Report Finds*, N.Y. TIMES (June 20, 2016), [https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html?\\_r=0](https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html?_r=0). But see Jack Goldsmith & Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE (Nov. 30, 2017, 1:00 PM), <https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage> (discussing the 2017 indictment of three Chinese hackers under U.S. law for commercial espionage and possible links between the hackers and the Chinese government).

229. See Goldsmith & Williams, *supra* note 228.

230. See Lotrionte, *supra* note 4, at 464–65 (discussing instances in which economic information of foreign powers would be useful to the maintenance of U.S. national security).

231. *Id.* at 464 (stating that these examples have traditionally been viewed as valid state uses of surveillance).

232. See *supra* notes 48–52 and accompanying text.

233. See Jessica Malekos Smith, *The Cyber Espionage Predominant Purpose Test*, SMALL WARS J. (Oct. 20, 2016), <http://smallwarsjournal.com/jrnl/art/the-cyber-espionage-predominant>

It may be feasible to adapt existing international legal frameworks and forums for governing and adjudicating cyber espionage issues, such as through the Trade Related Aspects of Intellectual Property Rights Agreement (“TRIPS”)<sup>234</sup> and the World Trade Organization (“WTO”).<sup>235</sup> Parties to the TRIPS Agreement must protect against the wrongful acquisition, disclosure, or use of protected information, including proprietary trade secrets.<sup>236</sup> The treaty does, however, allow for wide latitude on the part of states to create exceptions to domestic implementing legislation for actions deemed essential to the state’s own financial development, potentially allowing states to continue forms of economic espionage.<sup>237</sup> Also, as interpreted by many today, TRIPS does not protect against economic espionage by foreign states.<sup>238</sup> If amended to include instances of foreign economic espionage, cases could be adjudicated through the WTO’s existing Dispute Settlement Body.<sup>239</sup> It is also possible, though unlikely, that the WTO could adjudicate cases of economic espionage through other pertinent rules.<sup>240</sup>

Other scholars suggest broadening the terms of the Cybercrime Convention to cover instances of international state-sponsored cyber espionage.<sup>241</sup> The Cybercrime Convention currently requires party states to enact domestic

---

purpose-test (proposing the adoption of a predominant purpose test to distinguish economic and traditional espionage under international law).

234. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 108 Stat. 4809, 1869 U.N.T.S. 299 [hereinafter TRIPS]. See Banks, *supra* note 223, at 524; Scott J. Shackelford, *The Law of Cyber Peace*, 18 CHI. J. INT’L L. 1, 24–26 (2017).

235. The WTO has jurisdiction to hear disputes arising out of TRIPS. For an exploration of possible ways that economic-based cyber espionage activities may be adjudicated by the WTO, see Jamie Strawbridge, *The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation*, 47 GEO. J. INT’L L. 833, 837 (2016). See also JAMES A. LEWIS, CTR. FOR STRATEGIC & INT’L STUDIES, CONFLICT AND NEGOTIATION IN CYBERSPACE 49–51 (2013).

236. Lotrionte, *supra* note 4, at 491.

237. TRIPS, *supra* note 234, art. 8.

238. See Lotrionte, *supra* note 4, at 492; see also David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, ASIL INSIGHTS (Mar. 20, 2013), <https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving>.

239. See Lotrionte, *supra* note 4, at 491. This body can authorize trade sanctions.

240. See Strawbridge, *supra* note 235, at 860. A victim state could allege a breach of good faith, for example. *Id.* at 860–62. It may also be possible to invoke the General Agreement on Tariffs and Trade (“GATT”) against an offending state to substantiate trade restrictions. *Id.* at 862. The likelihood of success for either of these approaches appears to be slim. *Id.* at 863. See also Fidler, *supra* note 238.

241. Banks, *supra* note 223, at 524.

legislation forbidding cyber theft.<sup>242</sup> The Agreement does not, however, effectively limit state-sanctioned espionage.<sup>243</sup> The Agreement also relies on domestic definitions of cybercrimes and does not definitively proscribe economic espionage.<sup>244</sup> Amendments could be made to incorporate a duty to criminalize the stealing of electronic information for the benefit of domestic corporations.<sup>245</sup>

Running parallel to the rise in international public disapproval of economic espionage, domestic prosecution efforts have also escalated. United States federal laws proscribing espionage have been somewhat effective in addressing instances of foreign espionage—although, the effects may be more symbolic than practical. The Economic Espionage Act,<sup>246</sup> for example, was enacted to specifically address foreign economic espionage.<sup>247</sup> The legislation applies to actions committed by individuals for the benefit of foreign state powers and has been the basis of several indictments so far, including those charging Chinese military hackers accused of commercial data theft against U.S. corporations.<sup>248</sup> In 2014, five members of Unit 61398 were indicted and charged for hacking into the networks of Westinghouse Electric, the United States Steel Corporation, and other companies.<sup>249</sup> Like other domestic laws potentially regulating international cyber behavior, the legislation's impact is limited due to issues in determining attribution of the cyber activities, ensuring extradition of defendants, and identifying proper judicial forums for cases.<sup>250</sup> Indeed, the five Chinese hackers will likely never face trial for their actions because of extradition problems.<sup>251</sup> Despite this fact,

---

242. Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13,174, 2296 U.N.T.S. 167. The relevant articles provide that “[e]ach Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.” *Id.* art. 2. However, states are allowed wide berth in setting the parameters for such laws. *Id.* Article 3 of the Convention similarly outlines provisions for the unlawful interception of data. *Id.* art. 3.

243. Banks, *supra* note 223, at 525. The terms of this Agreement are subject to a wide latitude of state interpretation. For example, it does not clearly define the term “cybercrime.” *Id.*

244. *Id.*

245. *See id.*

246. 18 U.S.C. §§ 1831–1839 (2012).

247. 142 CONG. REC. 27111–12 (1996) (statement of Sen. Specter).

248. Press Release, 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), <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

249. Michael S. Schmidt & David E. Sanger, 5 in *China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014), <https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html>.

250. Shackelford, *supra* note 234, at 22 (noting other domestic laws on point that also suffer from similar shortfalls, including the Computer Fraud and Abuse Act, the National Stolen Property Act, and the 2016 Defend Trade Secrets Act).

251. No extradition treaty exists between the United States and China. *See* Brendan Pierson & Jonathan Stempel, *Explainer: How Does Extradition to the U.S. Work?*, REUTERS (Dec. 6, 2018),

the case was effective in sending a strong message of condemnation to the Chinese government, as the incident played an important role in prompting the bilateral cyber agreement with China.<sup>252</sup> Further, public criminal prosecutions through domestic law may also play an important role in the development of international norms in the area of cyber espionage.<sup>253</sup>

The effectiveness of domestic legislation ultimately hinges on logistical considerations in bringing foreign actors to justice. Mutual legal assistance and extradition treaties form the bedrock of international cooperation in prosecuting defendants outside national borders.<sup>254</sup> Some are fairly comprehensive in the range of crimes that trigger state duties to cooperate in foreign prosecution of criminals and ostensibly include cyber-related incidents.<sup>255</sup> However, many lack meaningful enforcement obligations, as exemplified by Russia's refusal to extradite Edward Snowden despite a U.S.-Russia mutual legal assistance treaty.<sup>256</sup> Some also lack specificity regarding cyber crimes.<sup>257</sup> These agreements could be strengthened by providing sanctions for states that do not comply with extradition guarantees and by amendments that clearly outline state obligations in the cyber arena.

Given the significant jurisdictional issues with existing frameworks, bilateral investment treaties ("BITs") may present a more effective, if piecemeal, approach to limit certain unwanted activities within state-sanctioned cyber espionage. As noted above, domestic legislation—such as the Economic Espionage Act, which criminalizes foreign state theft of trade secrets—is, in reality, limited in its effectiveness due to difficulties in determining attribution, extraditing defendants, and finding proper forums for

---

<https://www.reuters.com/article/us-usa-china-huawei-tech-explainer/explainer-how-does-extradition-to-the-u-s-work-idUSKBN1O528Y>. In 2018, a Chinese spy was extradited to the United States for prosecution after he was lured to Belgium by American officials. See Ellen Nakashima, *In a First, a Chinese Spy Is Extradited to the U.S. After Stealing Technology Secrets*, *Justice Dept. Says*, WASH. POST (Oct. 10, 2018), [https://www.washingtonpost.com/world/national-security/chinese-spy-charged-with-stealing-us-military-secrets-and-extradited-for-prosecution/2018/10/10/b2a7325c-cc97-11e8-920f-dd52e1ae4570\\_story.html?utm\\_term=.f03969b038f2](https://www.washingtonpost.com/world/national-security/chinese-spy-charged-with-stealing-us-military-secrets-and-extradited-for-prosecution/2018/10/10/b2a7325c-cc97-11e8-920f-dd52e1ae4570_story.html?utm_term=.f03969b038f2).

252. Shackelford, *supra* note 234, at 22.

253. See Ashley Deeks, *Moving Forward on Cyber Norms, Domestically*, LAWFARE (July 10, 2017, 1:10 PM), <https://lawfareblog.com/moving-forward-cyber-norms-domestically>.

254. The United States is a part of several such agreements. Shackelford, *supra* note 234, at 38.

255. *Id.* at 38–39.

256. Mutual Legal Assistance in Criminal Matters, U.S.-Russ., June 17, 1999, S. Treaty Doc. No. 106-22 (2002). The treaty states that the parties agree to "provide to each other . . . comprehensive mutual legal assistance in criminal matters," including "assistance provided by the Parties in connection with: prevention, suppression, and investigation of crimes; criminal prosecutions; and other proceedings related to such criminal matters." *Id.* art. 1. The agreement lacks specific extradition provisions, however, for persons not already in custody. See *id.*

257. See Gail Kent, *The Mutual Legal Assistance Problem Explained*, CTR. INTERNET & SOC'Y (Feb. 23, 2015, 1:06 PM), <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained>.



adjudication.<sup>258</sup> BITs may be more efficient tools for dealing with these criminal activities. Such agreements would provide victim businesses with a legal avenue to pursue remedies against foreign states directly and a forum to do so.<sup>259</sup> These instruments would also fix another endemic problem in frameworks of domestic prosecution: harmonizing the applicable substantive law.<sup>260</sup>

Based on the serious risks posed by modern industrial cyber espionage, and a lack of governing international law framework, many states have enacted internal legislation to mitigate threats to their own government and domestic industries. Some have passed data localization laws ensuring domestic control over cyber infrastructure. Kazakhstan, for example, requires new businesses to use internet servers physically located within the country.<sup>261</sup> Taiwanese law allows government authorities to restrict international transfers of data based on national interests.<sup>262</sup> Others have adopted policies regarding computer hardware or software. In 2017, for example, President Trump signed a law purging Kaspersky antivirus software from U.S. government computers over a concern of cyber espionage.<sup>263</sup> These developments display the utility of state efforts to act protectively within their own borders in the absence of applicable comprehensive international legal framework providing remedies for security breaches.

Finally, as states continue to make efforts to eradicate economic espionage, this could lead to the development of customary international law. The formation of customary law in this area, in fact, seems more probable than a consensus by the major world powers on a multilateral legal agreement.<sup>264</sup> As defined by the International Court of Justice, customary law requires that states generally and uniformly follow a certain practice, and those states believe that the practice is required by international law (also referred to as *opinio juris*).<sup>265</sup> Unlike traditional forms of espionage which rarely resulted in states publicly rebuking foreign governments—instead, quietly expelling or prosecuting the spy involved—modern cases involving economic espionage show the opposite trend.<sup>266</sup> Current events indicate that states are becoming more willing to draw a distinction between economic and other forms

---

258. Shackelford, *supra* note 234, at 22.

259. *Id.* at 23 (identifying the benefits of these agreements to include recourse to arbitration).

260. *See id.*

261. Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 682 (2015).

262. *Id.*

263. Dustin Volz, *Trump Signs into Law U.S. Government Ban on Kaspersky Lab Software*, REUTERS (Dec. 12, 2017), <https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4>.

264. Deeks, *supra* note 3, at 342.

265. Statute of the International Court of Justice, art. 38, ¶ 1b, June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993.

266. Complicating this pattern of public condemnation, however, are statements made by public officials which indicate that the state practice of refraining from economic sabotage is ultimately

of espionage.<sup>267</sup> In addition to the multiple bilateral agreements involving China, the United States, United Kingdom, and Canada, G-20<sup>268</sup> leaders agreed in 2015 to refrain from conducting espionage for financial benefit.<sup>269</sup> This general trend toward international consensus is not without exception, however. In June 2017, after years of making progress toward the establishment of comprehensive cyber norms, discussions at the United Nations ended in deadlock.<sup>270</sup> Despite this recent setback, an international custom may emerge as states continue to affirm individual commitments to refrain from economic espionage and those commitments are solidified into legally-binding agreements.

## VI. CONCLUSION

The nature of espionage to date generally required a person to place themselves at risk by physically traveling into a hostile country—in peacetime or wartime—to obtain the information being sought. Because states were able to substantively prohibit espionage within their sovereign borders or within their zone of military operations, they could meaningfully police activities within their jurisdiction yet continue to engage in espionage operations abroad. Cyber espionage fundamentally altered this equation and upended the accompanying risk analysis. No longer does a spy have to cross into hostile territory to obtain the desired information—it can be done from the comfort of a desk with a computer workstation. Moreover, states have

---

rooted in domestic concerns about fairness, rather than a duty to the international community. For example, a common justification for the United States' position against the sharing of business secrets with private industry is that it would unfairly preference those selected businesses over others who are not recipients of the state-gathered intelligence. See Rascoff, *supra* note 47, at 259. Secondly, the position is also justified as an effort to strengthen attempts at prosecuting foreign defendants under domestic economic espionage legislation, such as the Economic Espionage Act, which may otherwise be undermined by similar state practice. *Id.* at 260. Interestingly, however, this second justification seems undermined by espionage for the purpose of national security, in which foreign agents have long been prosecuted. *Id.*

267. See Lotrionte, *supra* note 4, at 489 (discussing the significance of the United States' public condemnation and criminal prosecution of Chinese military officials).

268. The G20 is comprised of nineteen countries and the European Union—representing the world's largest economies. See *What Is the G20 Summit?*, G20 2019 JAPAN, <https://g20.org/en/summit/about/#participants> (last visited Jan. 7, 2019).

269. See Nakashima, *supra* note 222. Leaders of the G-20 promised that “no country should conduct or support [cyber]-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.” *Id.* (alteration in original).

270. See Owen Bowcott, *Dispute Along Cold War Lines Led to Collapse of UN Cyberwarfare Talks*, *GUARDIAN* (Aug. 23, 2017), <https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges>; see also Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, *JUST SECURITY* (June 30, 2017), <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> (positing that Cuba, Russia, and China were outliers in state consensus).

lost much direct control over espionage targeting domestic industry, as the data and digital infrastructure is privately owned and cyber intrusion requires neither a government entry visa nor diplomatic papers. Meanwhile, the effects of intellectual property and proprietary theft on private corporations is felt quite strongly at the national level and poses a distinct threat of national economic harm. The current international law framework for espionage, however, is ultimately rooted in traditional methods of spying—developed in the absence of this unique digital environment.

*Tallinn 2.0* has accomplished a great deal to assist states in dealing with the issue of cyber espionage. By comprehensively documenting the *lex lata*, the Experts have made it possible to focus on the developments of cyber espionage in relation to the current international law framework and expose its ensuing flaws. The process of international law development via customary law and treaty can be interminably slow, and developments in technology generally outpace the development of international law. As the *Tallinn 2.0* framework is substantially based on traditional rules regarding espionage, there understandably exist many areas of uncertainty. The legal thresholds and parameters regarding the violation of sovereignty and intervention, for example, remain particularly unclear. The limits of the state duty of due diligence in preventing actions of non-state actors also seem opaque. Ambiguity still exists as to the applicability of the right to privacy and the extent to which it may restrict state cyber spying. Most obviously, the rules as applied to wartime seem to be especially unhelpful and inapplicable, as they are tied to espionage taking place within the geographic territory of the victim state.

Despite these uncertainties in the *lex lata*, most states are unlikely to insist on more concrete guidelines within the field of cyber spying for political and military secrets. Espionage itself has traditionally existed in a nebulous legal status, and nations have comfortably operated within this sphere both in peacetime and during conflict. Advances in digital technology have no doubt altered the playing field of state-on-state espionage, but nations still lack strong incentives to curb most cyber intelligence gathering through legally binding agreements. While governments, institutions, and individuals may have to resign themselves to the continuing ubiquity of cyber spying for national security and military purposes, the tide may be turning in the specific case of economic espionage. Economic espionage poses a particularly risk-laden and unmanageable threat to states, and world leaders have increasingly publicized their opposition to the practice. States, in fact, face a multitude of options to meaningfully limit incidents of economic-based espionage in the future.