

Texas A&M University-San Antonio

## Digital Commons @ Texas A&M University- San Antonio

---

Criminology and Criminal Justice Faculty  
Publications

College of Arts and Sciences

---

9-2019

### Transnational State-sponsored Cyber Economic Espionage: A Legal Quagmire

Brenda I. Rowe

Texas A&M University-San Antonio, [Brenda.Rowe@tamusa.edu](mailto:Brenda.Rowe@tamusa.edu)

Follow this and additional works at: [https://digitalcommons.tamusa.edu/crim\\_faculty](https://digitalcommons.tamusa.edu/crim_faculty)

 Part of the [Criminology and Criminal Justice Commons](#)

---

#### Repository Citation

Rowe, Brenda I., "Transnational State-sponsored Cyber Economic Espionage: A Legal Quagmire" (2019). *Criminology and Criminal Justice Faculty Publications*. 11.  
[https://digitalcommons.tamusa.edu/crim\\_faculty/11](https://digitalcommons.tamusa.edu/crim_faculty/11)

This Article is brought to you for free and open access by the College of Arts and Sciences at Digital Commons @ Texas A&M University- San Antonio. It has been accepted for inclusion in Criminology and Criminal Justice Faculty Publications by an authorized administrator of Digital Commons @ Texas A&M University- San Antonio. For more information, please contact [deirdre.mcdonald@tamusa.edu](mailto:deirdre.mcdonald@tamusa.edu).

**Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire**

Brenda I. Rowe\*  
Department of Social Sciences  
Texas A & M University – San Antonio  
One University Way  
San Antonio, TX 78224  
Email: [Brenda.Rowe@tamusa.edu](mailto:Brenda.Rowe@tamusa.edu)

\*Corresponding author

**About the Author**

Brenda I. Rowe, JD, PhD, is an assistant professor of Criminology and Criminal Justice at Texas A & M University – San Antonio. Her research interests include legal issues in criminal justice, criminal justice policy, criminal law and procedure, and police-prosecutor relationships

**Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire**

**Abstract**

Transnational state-sponsored cyber economic espionage poses a threat to the economy of developed countries whose industry is largely reliant on the value of information. In the face of rapid technological development facilitating cyber economic espionage from afar on a massive scale, the law has not developed apace to effectively address this problem. Applicable United States domestic laws have been ineffective in addressing the problem due to lack of enforcement jurisdiction, sovereign immunity, and inability to hold the state sponsor accountable. Customary international law principles offer little help in combatting the issue, as countermeasures are typically unavailable since espionage may not be ongoing by the time a victimized state can confidently attribute it to a state and retortions are a relatively weak response. Although existing treaties have not been effective in addressing this problem, a multilateral global treaty specifically addressing transnational state-sponsored cyber economic espionage may be a promising way forward.

**Keywords:** espionage; cybercrime; transnational crime; international law; state crime

**Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire**

Espionage for national security purposes has long been widely practiced and tacitly tolerated, with countries largely escaping any accountability for their espionage activities under international law – although individual spies can be prosecuted under domestic laws if subject to the jurisdiction of that country’s judicial system (Blinderman and Din, 2017; Lotrionte, 2015; Pun, 2017). Likewise, spying to gain economic advantage is certainly nothing new, despite various domestic laws which can be brought to bear to punish such conduct (Lotrionte, 2015; Reid, 2016). However, in recent years, technology has enabled economic espionage to be conducted on a massive scale, from afar without the need to physically cross national borders, relatively inexpensively, and often in relative anonymity (Crootof, 2018; Rowe, 2016). State sponsorship of cyber economic espionage has raised the stakes due to the organization and resources this provides to hackers, as well as the impact on national economies when wealth is systematically transferred from one country to another through theft of valuable information for the benefit of competing companies (Carlin, 2016; Lotrionte, 2015).

Transnational state-sponsored cyber economic espionage is a growing threat to developed economies which have robust industry largely reliant on the value of information – such as the United States economy (Lotrionte, 2015; Reid, 2016; Rowe, 2016). Numerous high profile hacking incidents by China, North Korea, and Russia perpetrated against companies based in the United States have raised public consciousness of the vulnerability of companies, and the United States economy more generally, to cyber espionage from abroad (Anderson, 2017; Banks, 2017b; Blinderman and Din, 2017; Carlin, 2016; Reid, 2016). Policymakers are grappling with how to craft effective, lawful responses which deter such espionage while avoiding an escalation into an all-out cyberwar (Blinderman and Din, 2017; Crootof, 2018). These efforts are

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

constrained by the lack of an effective legal framework for dealing with these incidents (Blinderman and Din, 2017).

Although the United States has several domestic laws applicable to cyber economic espionage, using such laws to hold perpetrators accountable or achieve restitution is often not possible when the perpetrators commit offenses from abroad and with state backing (Blinderman and Din, 2017; Perloff-Giles, 2018; Rowe, 2016). International law fails to specifically address transnational state-sponsored cyber economic espionage (Crootof, 2018; Walton, 2017). Despite efforts to reach consensus on how traditional international law principles apply to cyberspace, to date, there is little clarity with regard to cyber operations which occur in peacetime and do not constitute use of force (Crootof, 2018; Walton, 2017).

Unfortunately, the law has failed to keep pace with the breathtaking pace of technological development and thus is largely inadequate to effectively address transnational state-sponsored cyber economic espionage (Banks, 2017a; Rowe, 2016). Problematic issues include jurisdiction, sovereign immunity, attribution, the failure of international law to clearly address peacetime cyber espionage, and risks associated with available responses (Anderson, 2017; Blinderman and Din, 2017; Perloff-Giles, 2018; Rowe, 2016; Walton, 2017). This article discusses the problem of transnational state-sponsored cyber economic espionage, analyzes how the current United States domestic legal framework applies to this phenomenon and what legal issues complicate the effective use of these laws, examines the ineffectiveness of the current state of international law in dealing with this problem, and discusses the implications of our failure to develop laws better suited to addressing this vexing problem.

### **The Problem of Transnational State-Sponsored Cyber Economic Espionage**

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Transnational state-sponsored cyber economic espionage is the unauthorized cross-border collection of information by foreign governments or state-sponsored actors via cyber means for the purpose of gaining an economic benefit (Lotrionte, 2015; Reid, 2016).<sup>1</sup> In recent years, cyber economic espionage has become a pressing concern, with technological developments enabling espionage to be conducted remotely on a massive scale and with relatively low barriers to entry in terms of both cost and technical expertise, resulting in estimated losses to the United States economy in the billions of dollars per year (Anderson, 2017; Banks, 2017b; Carlin, 2016; Crootof, 2018; Reid, 2016; Rowe, 2016). While cyber economic espionage committed by insiders or organized crime groups without state sponsorship is also a significant issue (Inserra, 2017; Levandoski, 2018), this article will focus on transnational state-sponsored cyber economic espionage due to the unique concerns raised by this type of espionage.

When cyber economic espionage is state sponsored and targets other nations' private companies for the purpose of stealing intellectual property and trade secrets to benefit competitor companies, this poses a unique threat for several reasons (Lotrionte, 2015). First, state backing provides a level of organization and funding to hackers which a typical individual hacker is unlikely to possess (Argento, 2013). This creates a dynamic where individual private companies are trying to defend against cyber intrusions by a nation (Rowe, 2016). Second, when conducted systematically or on a large scale, it can erode a country's economy by removing the competitive edge of its private companies, undermining the return on those companies' investments in research and development (which disincentivizes such investments in the future), and transferring large amounts of wealth (in the form of valuable information) to foreign competitor companies who have not made such investments, thereby allowing the sponsoring state to take a shortcut to grow its economy through cheating and outright theft (Carlin, 2016; Lotrionte, 2015).

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Third, the transnational nature of this espionage and the involvement of a state in perpetrating the offense make crafting an effective response within the existing legal framework extremely challenging (Blinderman and Din, 2017; Rowe, 2016). Thus, transnational state-sponsored cyber economic espionage is a uniquely intractable problem warranting a closer examination of the shortcomings of the current legal framework and the implications of our failure to develop laws capable of effectively combatting this threat.

### **Overview of Relevant United States Domestic Laws**

The current state of domestic law within the United States is inadequate to address transnational state-sponsored cyber economic espionage (Blinderman and Din, 2017; Rowe, 2016). In the United States, there are domestic laws at both the federal and state levels which can be used to address cyber economic espionage (Blinderman and Din, 2017; Rowe, 2016). At the state level, there are state trade secret theft statutes (providing a state civil private right of action for trade secret misappropriation; Beauchamp, 2017). Relevant federal statutes include the Economic Espionage Act (providing criminal penalties for trade secret misappropriation), the Defend Trade Secrets Act (providing a federal civil private right of action for trade secret misappropriation), and the Computer Fraud and Abuse Act (providing criminal sanctions and a federal civil private right of action for unauthorized access of a computer; Blinderman and Din, 2017; Levandoski, 2018; Rowe, 2016). Despite the existence of a number of applicable domestic laws, such laws fail to provide effective recourse in light of issues of jurisdiction, state sovereignty, and attribution (Anderson, 2017; Blinderman and Din, 2017; Perloff-Giles, 2018).

### **United States Domestic Laws Protecting Trade Secrets**

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

The first category of United States domestic laws specifically protects trade secrets. Nearly all states have state trade secret theft statutes patterned after the Uniform Trade Secrets Act, which allow victimized companies to bring civil litigation against parties who misappropriate their trade secrets (Beauchamp, 2017). However, reliance on a state law regime can be problematic for companies operating in multiple states since such laws, despite the “uniform” label, are not in fact uniform due to amendment of state laws over time and variation in state court interpretation of these laws (Beauchamp, 2017).

At the federal level, the Economic Espionage Act provides criminal penalties for domestic trade secret theft (18 U.S.C. § 1832) and trade secret theft for the benefit of foreign governments (18 U.S.C. § 1831; Banks, 2017a; Danielson, 2009; Levandoski, 2018; Rowe, 2016). Although concern regarding foreign economic espionage was the primary motivator for passage of the Economic Espionage Act, federal prosecutors have brought far more prosecutions for domestic trade secret theft (§ 1832 violations) than for foreign economic espionage (§ 1831 violations; Levandoski, 2018). Overall, the Economic Espionage Act has failed to live up to its promise, as there have been few prosecutions, even fewer convictions, and sentences have been relatively light (Levine and Seaman, 2018; Reid, 2016).

One complicating factor which prevents the Economic Espionage Act from being effective in combatting the problem of transnational state-sponsored cyber economic espionage is a lack of enforcement jurisdiction with regard to defendants who are not physically present within United States territory and have no assets within that territory (Perloff-Giles, 2018). In such cases, unless the United States can secure the cooperation of the country where the defendant is currently located in extraditing the defendant to the United States to face the charges in court, the United States will be powerless to enforce any judgment – thus, sentences will not



## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

be served and fines will not be collected (Perloff-Giles, 2018). In the case of state-sponsored transnational cyber economic espionage, such espionage can easily be conducted from abroad and, for obvious reasons, it is unlikely the country sponsoring the espionage is going to cooperate (Blinderman and Din, 2017; Danielson, 2009; Kosseff, 2019; Rowe, 2016).

Furthermore, the United States does not have extradition treaties with many of the countries who are known to be prime offenders of state-sponsored transnational cyber economic espionage, such as China, Russia, and North Korea – all of whom have sponsored recent high profile cyber economic espionage against companies in the United States (Carlin, 2016; Levandoski, 2018; Perloff-Giles, 2018).

Even if there is an extradition treaty and the country where the defendant is currently located is willing to cooperate, there may be other obstacles to extradition – such as extradition treaties’ dual criminality requirement (Brenner and Koops, 2004; Perloff-Giles, 2018). If the alleged conduct is not a crime in the country where the defendant is located, the defendant will not be extradited to the prosecuting country (Perloff-Giles, 2018). This is of particular concern with regard to cyber activities inflicting transboundary harms, as it is not uncommon for countries’ laws to fail to keep pace with technological developments facilitating relatively newer harmful acts (Marion, 2010; Perloff-Giles, 2018). Moreover, due to political, economic, and cultural differences between countries, not all countries share the United States’ view that intellectual property is a protected property right (Danielson, 2009; Reid, 2016). Thus, some countries may not criminalize trade secret misappropriation, in which case a defendant located in that country will not be extradited to the United States to face charges under the Economic Espionage Act, as the dual criminality requirement was not met (Perloff-Giles, 2018; Reid, 2016).

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Thus, even though the Economic Espionage Act provides for extraterritorial application, extraterritorial enforcement can be challenging (Levandoski, 2018). For example, in 2014, federal prosecutors initiated the first prosecution of state actors for hacking when a grand jury indicted five Chinese military officers for violating the Economic Espionage Act in connection with theft of trade secrets from power and metal industry companies in the United States (Carlin, 2016; Levandoski, 2018). However, because these Chinese military officers were not extradited to the United States, they never faced criminal punishment for these charges and thus the indictments were largely symbolic (Blinderman and Din, 2017; Carlin, 2016; Levandoski, 2018).

While it could be hoped that indictments in absentia (without the defendant's presence) may serve as a general deterrent, by sending a message to all who hear about the indictments, the impotence of such indictments may actually have the opposite impact – revealing the powerlessness of the United States to hold state-sponsored hackers accountable for stealing trade secrets from private companies in the United States (Lotrionte, 2015). Another problem with this approach is that indicting individuals does nothing to hold the offending country itself accountable for sponsoring cyber economic espionage because domestic criminal law holds individuals, not countries, accountable (Crootof, 2018).

Recently, Congress enacted another federal statute to protect trade secrets (Beauchamp, 2017; Levandoski, 2018). The Defend Trade Secrets Act (18 U.S.C. § 1836) amends the Economic Espionage Act to allow companies to bring private federal civil litigation against those who misappropriate their trade secrets, provided the trade secrets are related to foreign or interstate commerce (Beauchamp, 2017; Levandoski, 2018). This law is intended to make such civil litigation easier for companies than it would be when suing under the state trade secret theft statutes by providing uniformity, an obvious benefit to companies which operate in multiple

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

states within the United States, and also provides for an ex parte seizure remedy (allowing the court to seize property containing trade secret information pending completion of the litigation to prevent irreparable damage) and fewer whistleblower protections than state trade secret theft statutes do (Levine and Seaman, 2018).

Despite political rhetoric during the time leading up to the passage of the Defend Trade Secrets Act regarding this legislation being needed to combat state-sponsored cyber economic espionage, in practice the Defend Trade Secrets Act has primarily been used to address trade secret misappropriation by insiders (e.g., former employees), not transnational hacking (Levine and Seaman, 2018). The Defend Trade Secrets Act, at least in its infancy, has not borne much fruit in fighting state-sponsored cyber economic espionage – with only 6% of federal court civil lawsuits brought under this law in its first year alleging trade secret misappropriation by a foreign defendant and only 9% alleging unauthorized access of a computer network (Levine and Seaman, 2018). Thus, the early empirical evidence suggests there may be a need for further legislative action more tailored to addressing cyber economic espionage in order to adequately address this problem (Levine and Seaman, 2018).

### **The Computer Fraud and Abuse Act**

In addition to laws specifically protecting trade secrets, there is another United States domestic law at the federal level which can be used to address transnational state-sponsored cyber economic espionage: the Computer Fraud and Abuse Act (Blinderman and Din, 2017; Rowe, 2016). The Computer Fraud and Abuse Act provides both criminal sanctions and a private right to bring a federal civil suit for unauthorized access of a computer or intentionally damaging an internet-connected computer via use of computer program or computer code

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

(Argento, 2013; Banks, 2017a; Blinderman and Din, 2017). This law can thus be used to prosecute hackers (Argento, 2013; Banks, 2017a).

The Computer Fraud and Abuse Act is plagued by a number of issues, including the enforcement jurisdiction issue discussed above in connection with the Economic Espionage Act (Blinderman and Din, 2017; Perloff-Giles, 2018). While the Computer Fraud and Abuse Act did not originally explicitly confer extraterritorial (legislative) jurisdiction, subsequent amendments changed the definition of a “protected computer” to clearly indicate this includes any computer affecting interstate or foreign communication or commerce of the United States, regardless of whether the computer is located within or outside of the United States, thus conferring on the United States jurisdiction to prosecute offenses impacting such computers (Brenner and Koops, 2004). However, even though the United States may have extraterritorial jurisdiction to prosecute such transnational offenses, this will often be impractical due to the country where the offender is located refusing to extradite the offender (generally rendering the United States unable to enforce any judgment obtained), such as when the conduct is not illegal in the country of offender’s location (thus not satisfying the double criminality requirement of extradition treaties) or when the United States does not have an extradition treaty with that country (Brenner and Koops, 2004). Furthermore, due to the governmental involvement in the offense of transnational state-sponsored cyber economic espionage, if the perpetrator is currently located within the territory of the country which sponsored the act, it is exceedingly unlikely that country will agree to extradite the offender (Blinderman and Din, 2017; Kosseff, 2019; Lotrionte, 2015; Rowe, 2016). Furthermore, domestic criminal prosecution does nothing to hold the state sponsor itself accountable and any attempt to bring civil litigation against the state sponsor would be

stymied by sovereign immunity (Anderson, 2017; Blinderman and Din, 2017; Crootof, 2018; Yannakogeorgos, 2013).

### **Legal Issues Complicating Use of United States Domestic Law**

A number of legal issues complicate efforts to deter transnational state-sponsored cyber economic espionage through the use of United States domestic law. First, jurisdictional issues plague attempts to use domestic law to deter transnational cyber offenses, and this is exacerbated by state sponsorship of such offenses (Perloff-Giles, 2018). Although jurisdictional issues were briefly touched on in the discussion of specific statutes above, a more in depth discussion of these issues is warranted here due to their complexity and importance. Three dimensions of territorial jurisdiction can present issues when using domestic law to address transnational cyber offenses -- legislative jurisdiction, judicial jurisdiction, and enforcement jurisdiction (Perloff-Giles, 2018).

With regard to legislative jurisdiction, does the domestic statute have extraterritorial application (Perloff-Giles, 2018)? In other words, does it apply to the cyber conduct simply because it has effects in the United States, regardless of where the offender was when he committed the offense (Perloff-Giles, 2018)? Where a statute does not explicitly provide for extraterritorial application, courts are reluctant to find legislative intent for a law to apply extraterritorially (Blinderman and Din, 2017; Perloff-Giles, 2018). And with good reason, as extraterritorial application of domestic law to state-sponsored transnational cyber economic espionage entails a risk that a prosecutor's decision to prosecute foreign actors may trigger retaliation by the other country, such as trade restrictions or ceasing cooperation in judicial matters or military operations (Blinderman and Din, 2017). However, in the United States, there

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

is a recent trend of broadening legislative and judicial jurisdiction to allow extraterritorial application of certain statutes and grant courts authority to hear certain cases against foreign defendants (Perloff-Giles, 2018). For example, the Economic Espionage Act explicitly provides for extraterritorial application (Levandoski, 2018). Likewise, the Computer Fraud and Abuse Act was amended to allow for extraterritorial application (Brenner and Koops, 2004).

Another jurisdictional issue is whether the court has jurisdiction to adjudicate the case (Perloff-Giles, 2018). This requires that there be a sufficient connection between the offense and the geographic area over which the court has jurisdiction (Perloff-Giles, 2018). This can often be satisfied based on the harmful effects occurring in that geographic area – e.g., the computer server that was hacked was located within the court’s jurisdiction (Rowe, 2016).

A highly problematic jurisdictional issue is whether the United States has jurisdiction to enforce judgments (Perloff-Giles, 2018). If neither the defendant nor the defendant’s assets are located within the United States’ territory, the defendant will never serve any sentence and no fines will be collected unless the country where the defendant is currently located extradites the defendant to the United States to face charges there (Perloff-Giles, 2018). In contrast to the multinational corporations (with facilities and assets in numerous countries including the United States) successfully prosecuted by the United States for transnational bribery using a domestic extraterritorial enforcement approach (Hock, 2017), typical offenders may be individual hackers located in other countries or government officials of other countries who have no ties to the United States thus making transnational state-sponsored cyber economic espionage less amenable to such an approach due to the enforcement jurisdiction obstacle.

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

State sponsorship of transnational cyber economic espionage greatly exacerbates the usual transnational crime enforcement jurisdiction issue because it is very unlikely that the country which sponsored the espionage will cooperate by extraditing its hackers to the United States to face charges under domestic law (Kosseff, 2019; Lotrionte, 2015). Even if the hacker is currently located in a different country than the country which sponsored the espionage, extradition may not be possible if the United States does not have an extradition treaty with that country or if the conduct at issue is not criminalized in that country (due to extradition treaties' dual criminality requirement), as may be the case when that country's laws have failed to keep up with technological advances facilitating new forms of harmful conduct or when a country does not protect intellectual property in the way the United States does (Perloff-Giles, 2018; Reid, 2016). And if digital evidence located in another country's territory is needed to prove the case, can the United States secure that country's cooperation in obtaining that evidence in a timely manner and with sufficient technical expertise (Perloff-Giles, 2018)? Mutual Legal Assistance Treaties, by which countries agree to assist each other in criminal cases, may not be of much help, as they only apply if the conduct is a crime in both of the countries involved and may be processed so slowly that digital evidence has disappeared (Perloff-Giles, 2018).

Sovereign immunity is another legal issue complicating the use of domestic law to deter transnational state-sponsored cyber economic espionage (Anderson, 2017; Blinderman and Din, 2017). Recourse against the perpetrators of transnational state-sponsored cyber economic espionage through civil litigation is often elusive due to sovereign immunity (Anderson, 2017). Creating an exception to the Foreign Sovereign Immunities Act (FSIA) allowing corporations to sue foreign governments for damages caused by state-sponsored cyber intrusions is a possible solution (Anderson, 2017; Blinderman and Din, 2017). Such an exception to sovereign

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

immunity is not without precedent, as prior legislation has created an exception allowing civil suits against state sponsors of terrorism, and may change would-be hackers' cost-benefit calculation and thus serve as a deterrent in addition to facilitating companies recouping their economic losses (Blinderman and Din, 2017). However, passage of legislation creating a sovereign immunity exception for state-sponsored cyber intrusions may prompt other countries to enact similar laws, which could be used to address the United States' cyber espionage operations (Blinderman and Din, 2017).

Attribution is also a major obstacle to addressing transnational state-sponsored cyber economic espionage via domestic law. Identifying which individual or group perpetrated the acts constituting cyber economic espionage and where they are located is extremely challenging due to perpetrators' use of anonymizing tools, spoofing, public Wi-Fi networks, and botnets spanning multiple countries (Finnemore and Hollis, 2016; Schmitt and Vihul, 2014; Tran, 2018; Yannakogeorgos, 2013). Even if authorities are able to identify the computer from which the cyber economic espionage operation originated, there remains the additional challenge of linking that computer to the individuals who committed the act (Tran, 2018). This obstacle, however, is equally applicable to use of international law -- and the difficulty is amplified in that context due to the need to further link the individuals involved to the state sponsor (Blinderman and Din, 2017; Schmitt and Vihul, 2014; Tran, 2018), thus the difficulties of attribution will be discussed in greater detail in a later section of this article.

Finally, the lack of sanctions on the state sponsor itself is another drawback to using an approach of extraterritorial application of domestic law instead of an international solution (Crootof, 2018; Yannakogeorgos, 2013). Thus, there is a need for an international approach that



can specifically address transnational state-sponsored cyber economic espionage in a way that facilitates holding accountable the state sponsoring it (Crootof, 2018; Yannakogeorgos, 2013).

### **Application of International Law to State-Sponsored Cyber Economic Espionage**

The international legal community is grappling with how to apply international law, developed using terms and classifications better suited to the physical domain, to cyberspace (Crootof, 2018). At the invitation of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE), an International Group of Experts (IGE) wrote the *Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual)* and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0)*, authoritative yet non-binding sources providing the experts' views on how established international law norms apply to cyber attacks constituting use of force (*Tallinn Manual*) and cyber operations falling below the level of use of force (*Tallinn Manual 2.0*), respectively (Banks, 2017b; Margulies, 2013). Due to the unsettled nature of international law in the cyber realm, these restatement projects (intended to reflect the law as it currently exists) necessarily provide general applicable principles and often leave ambiguity or indicate the experts' diverging views on applications of these principles to specific cyber scenarios (Banks, 2017b). Efforts to clarify international law norms on cyber operations falling below the use of force threshold are impeded by a dearth of *opinion juris* (state declarations that they are legally obligated to engage in or abstain from certain conduct), a result of states' hesitancy to characterize cyber operations as international law violations, even when they are the victims, lest they limit their own options going forward (Schmitt and Vihul, 2014).

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Despite political rhetoric characterizing transnational state-sponsored cyber economic espionage as acts of cyberwar, the laws of war generally do not aid in combatting this problem since it rarely rises to the level of use of force (Crootof, 2018; Walton, 2017). The United Nations Charter restricts unilateral use of force to self-defense in case of armed attack (Crootof, 2018; Schmitt and Vihul, 2014). For a cyber action to constitute an armed attack, it must cause death or serious injury or physical damage (Schmitt, 2013; Schmitt and Vihul, 2014). While some scholars have attempted to stretch the meaning of terms in the laws of war (*jus ad bellum*, governing when a state may use force, and *jus in bello*, international humanitarian law governing the conduct of war) to cover lower level cyber intrusions, this is ill advised (Crootof, 2018; Walton, 2017). Because cyber economic espionage does not typically inflict any physical damage at all and certainly not physical damage equivalent to an armed attack, use of force in response to cyber economic espionage would not comply with the laws of war (Crootof, 2018; Perloff-Giles, 2018). Rather, the damage inflicted by cyber economic espionage is economic and thus the political rhetoric regarding cyberwar is misplaced (Crootof, 2018).

The customary international law principles of state sovereignty and non-intervention likewise offer little respite (Walton, 2017). There is no general consensus on how state sovereignty applies in cyberspace – or even whether sovereignty has the force of a rule of conduct versus whether it is more of an underlying (unenforceable) principle (Walton, 2017). The interconnected nature of cyberspace makes it difficult to determine the boundaries of a state's territory in this realm (Walton, 2017). Moreover, states have been reluctant to pursue establishing an international legal framework addressing covert intrusions on state sovereignty or imposing an outright prohibition on cross-border cyber intrusions, lest such a framework impede states' own espionage activities conducted for national security purposes or unduly interfere with

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

routine telecommunications and commercial activities having extraterritorial effects (Walton, 2017). The non-intervention principle is rarely implicated since routine transnational state-sponsored cyber economic espionage generally lacks the required element of coercion of another state's governmental functions (Walton, 2017).

International law is strangely silent as to how countries can respond to lower level cyber intrusions which cause massive economic damages, but do not constitute acts of war (Crootof, 2018; Walton, 2017). In fact, what little international law does say only serves to restrict targeted countries' lawful options for engaging in self-help responses (Crootof, 2018). This reflects a preference in international law for keeping the peace by avoiding retaliatory escalation cycles even if that comes at the expense of tolerating minor infringements (Crootof, 2018).

The customary law of countermeasures permits temporary, proportional, nonviolent countermeasures (responses that would violate international obligations, such as those created by treaty, if not undertaken as a response to an internationally wrongful act) when necessary to induce an international law violator to cease the violation and make reparation (Banks, 2017b; Crootof, 2018; Schmitt and Vihul, 2014; Schmitt and Vihul, 2017; Walton, 2017). In the context of transnational state-sponsored cyber economic espionage, hacking back may be a useful countermeasure (Schmitt and Vihul, 2014). However, the law of countermeasures does not allow countermeasures for the purpose of punishment (Banks, 2017b; Crootof, 2018; Schmitt and Vihul, 2014; Schmitt and Vihul, 2017). Often, cyber economic espionage is discovered and attributed to a country long after it occurred (Crootof, 2018). In such cases, the targeted state cannot lawfully employ countermeasures because the wrongful act has already ceased and punitive countermeasures are not permitted under international law (Crootof, 2018).

Furthermore, use of countermeasures is fraught with risk – if the targeted state misattributes the

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

cyber economic espionage to the wrong party, then the countermeasure will actually constitute a violation of the targeted state's international obligations (Crootof, 2018).

Thus, countries' self-help options under international law are limited to retortions, which are lawful self-help measures constituting political retaliation such as expelling diplomats, imposing financial sanctions, ending economic aid, etc. (Crootof, 2018; Schmitt and Vihul, 2014). Unfortunately, retortions do not appear to be an effective deterrent to state-sponsored cyber economic espionage (Crootof, 2018). The lack of a clear international legal framework well suited to dealing with cyber intrusions has led to minimalist state responses, which likely only emboldens hackers (Crootof, 2018).

Affected states often have few effective responses available and may be reluctant to exercise certain options due to fear of escalation (Crootof, 2018). States may also be reluctant to label cyber intrusions as violating international law lest those words be used against them when they engage in questionable cyber operations in the future (Crootof, 2018; Watts and Richard, 2018). The United States, for example, refrained from claiming North Korea's Sony hack violated international law even though it arguably violated state sovereignty – although how the international law norm of territorial sovereignty applies in cyberspace is currently unsettled (Crootof, 2018; Watts and Richard, 2018). Given the United States' aggressive cyber operations in pursuit of national security objectives, this restraint is perhaps unsurprising (Crootof, 2018; Watts and Richard, 2018).

Part of the problem in the international law arena is a lack of clarity with regard to where to draw the line between tolerable cyber espionage and unlawful cyber espionage under international law (Banks, 2017a; Reid, 2016). Espionage conducted by governments for national

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

security purposes is a long-standing, widespread practice – typically addressed through domestic laws and diplomacy (Banks, 2017a; Lotrionte, 2015; Reid, 2016). However, when espionage serves an economic purpose, the issue becomes murkier (Banks, 2017a; Reid, 2016). While government espionage conducted for the purpose of giving a country an advantage in trade negotiations is arguably acceptable, state-sponsored international espionage for the purpose of gaining an economic advantage for companies is generally considered beyond the pale (Banks, 2017a; Reid, 2016).

The United States takes the position that espionage for national security purposes is conducted by all countries and thus tolerated, but that conducting espionage for the purpose of stealing intellectual property and sharing that with private companies is unacceptable, criminal conduct (Lotrionte, 2015; Reid, 2016). However, critics have pushed back on this position, arguing that the United States also spies on economic institutions (Reid, 2016). The United States does not accept this criticism, arguing that it only collects economic information for the purpose of informing trade negotiations, but does not share this information with private companies (Lotrionte, 2015; Reid, 2016). Countries' differing political, social, and economic structures, as well as their strategic interests given differing statuses with regard to level of economic and technological development, contribute to differences in how they view intellectual property and the propriety of government espionage for the purpose of giving corporations a competitive advantage (Danielson, 2009; Reid, 2016).

There is a pressing need to develop clear international law prohibiting such cyber economic espionage and providing an effective enforcement framework (Banks, 2017a). Possible ways to draw the line distinguishing between tolerable cyber espionage and unlawful cyber espionage under international law include prohibiting espionage for any purpose other than

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

national security (although it may not always be easy to make this distinction) or prohibiting government espionage for the purpose of providing economic benefit to private companies (Banks, 2017a) – although such a distinction can quickly become a grey area since some governments either own or exercise a high level of control over companies located within their borders (e.g., North Korea, China; Wu, 2016). The U.S.-China bilateral security agreement, which prohibits state-sponsored cyber economic espionage among the signatory countries for commercial advantage, is an example of the latter approach, but is ineffectual due to its lack of an enforcement mechanism, the difficulty of establishing the identity of cyber attack perpetrators, and its limited scope which fails to offer protection against the most common types of attacks such as intellectual property theft (Anderson, 2017).

### **The Budapest Convention**

Treaties hold promise as a potential solution for addressing transnational state-sponsored cyber economic espionage, yet have fallen short to date (Al Azzam, 2019; Marion, 2010). The Council of Europe's 2001 Convention on Cybercrime (Budapest Convention) is the most significant multilateral treaty governing cybercrime (Al Azzam, 2019; Broadhurst and Chang, 2013; Cerezo *et al*, 2007; Eichensehr, 2017a). The Budapest Convention calls for parties to enact domestic legislation criminalizing certain conduct constituting cybercrimes – including illegally accessing computer systems (hacking), illegally intercepting computer data, interfering with stored data, interfering with computer systems, and misusing devices (Bande, 2018; Broadhurst and Chang, 2013; Cerezo *et al*, 2007). It also calls for parties to establish procedures to facilitate domestic investigation and prosecution of those offenses (subject to parties' existing domestic laws protecting individual rights) and seeks to establish a framework for cooperation among parties to better facilitate prosecution of cybercrimes (Al Azzam, 2019; Bande, 2018;

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Broadhurst and Chang, 2013; Cerezo *et al*, 2007; Clough, 2014). International cooperation among parties takes the form of mutual assistance, extradition, and established points of contact available around the clock (Broadhurst and Chang, 2013; Cerezo *et al*, 2007; Clough, 2014).

The Budapest Convention's effectiveness in dealing with transnational state-sponsored cyber economic espionage is lacking for several reasons. First and foremost, by taking a domestic law enforcement approach, it does not provide a method for sanctioning the state sponsor – at most, the individuals involved may be prosecuted (Crootof, 2018; Yannakogeorgos, 2013).

Second, if the individuals involved are located within the territory of the state which sponsored the cyber economic espionage, it is exceedingly unlikely that state will cooperate with extradition and thus the victimized state will not have enforcement jurisdiction over those individuals (Blinderman and Din, 2017; Kosseff, 2019; Lotrionte, 2015; Rowe, 2016). Parties to the Budapest Convention are not obligated to extradite unless there is an existing extradition treaty with the requesting party and both parties' laws provide a maximum punishment of at least one year imprisonment for the offense (Cerezo *et al*, 2007; Clough, 2014). The United States does not have extradition treaties with many of the states known to be prime offenders (Carlin, 2016; Levandoski, 2018; Perloff-Giles, 2018). While the Budapest Convention sought to overcome the obstacle to extradition presented by the dual criminality requirement in calling for harmonization of domestic criminal laws related to cybercrime, in practice parties' establishment of domestic criminal laws adequately governing cybercrimes has been inconsistent and there is no effective enforcement mechanism to force parties to expeditiously pass domestic laws adequately addressing the problem (Ajayi, 2016; Al Azzam, 2019; Marion, 2010). Thus, even if there is a relevant extradition treaty, the party in whose territory the individual offenders are

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

located may not have a law criminalizing the conduct or its laws may not punish that conduct with a maximum punishment of at least one year in prison (Ajayi, 2016; Al Azzam, 2019; Cerezo *et al*, 2007; Clough, 2014; Marion, 2010). Even if the dual criminality requirement is not an issue, the decision whether to extradite is up to the party of which extradition is requested and may be refused on various grounds, such as when extradition is requested for prosecuting what is viewed as a political offense or when the person may be subjected to inhumane punishments (Clough, 2014). Thus, there are loopholes which could be exploited by a party which does not want to cooperate with extradition.

Finally, the Budapest Convention is inapplicable to nations which are not parties to the treaty – including China, Russia, North Korea, and Iran, states known as primary threats due to their history of perpetrating state-sponsored cyber economic espionage (Bande, 2018; Broadhurst and Chang, 2013; Carlin, 2016; Inserra, 2017; Kosseff, 2019; Levandoski, 2018; Lotrionte, 2015; Perloff-Giles, 2018; Reid, 2016; Rowe, 2016). The vast majority of parties to the Budapest Convention are European and Western and many countries have refused to join the Budapest Convention due to concerns regarding their lack of input into its development, concerns that its transborder data access provision violates state sovereignty, and privacy concerns (Bande, 2018; Cerezo *et al*, 2007; Clough, 2014; Eichensehr, 2017a; Inserra, 2017).

### **The Challenge of Attribution**

Attribution issues are a major obstacle which often hinder efforts to use either domestic or international law to combat transnational state-sponsored cyber economic espionage (Blinderman and Din, 2017). The challenge of attributing transnational state-sponsored cyber economic espionage is two-fold (Schmitt and Vihul, 2014; Tran, 2018). First, there is the often



## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

difficult task of technical attribution, identifying which individual or group perpetrated the acts constituting cyber economic espionage and where that perpetrator is located (Schmitt and Vihul, 2014; Tran, 2018; Yannakogeorgos, 2013). Once this is accomplished, another challenge awaits – attributing the espionage to a state (Schmitt and Vihul, 2014; Tran, 2018).

Technical attribution can be difficult due to the anonymity afforded by the internet (Yannakogeorgos, 2013). Due to vulnerabilities in the standardized internet protocol used for transmitting information among computers, perpetrators can easily hide their location by using anonymizing tools, such as the use of proxy servers or onion routing (Tran, 2018; Yannakogeorgos, 2013). Sophisticated perpetrators can implicate innocent computer users as the originators of the hacking incident by spoofing internet protocol (IP) addresses (Finnemore and Hollis, 2016; Yannakogeorgos, 2013). This not only complicates technical attribution, but also may undermine confidence in attribution when those accused predictably claim they have been set up by the true perpetrators (Finnemore and Hollis, 2016). Furthermore, identifying the computer from which a cyber economic espionage operation originated is only one hurdle, as it is also necessary to determine the individuals who committed the act and this is not always a straightforward determination, given that perpetrators may use public Wi-Fi networks or covertly control others' devices to employ them in their schemes (Tran, 2018).

Technical attribution may also be challenging due to perpetrators' use of elaborate means to commit cyber economic espionage – such as botnets, networks of remotely controlled computers that may be located in multiple countries, some of which may have been selected by the perpetrator specifically for their qualities which maximize the difficulty of attribution such as lack of technical capacity necessary for effective investigations or being on unfriendly terms with the country in which the victimized corporation is located (Yannakogeorgos, 2013). Even

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

when cyber economic espionage is accomplished by simpler means, in this era of cloud computing -- where data may be located in multiple countries and it can even be difficult to determine the location of the necessary data -- collecting the data needed to ascertain the identity of the perpetrator may involve making requests for assistance from multiple countries pursuant to mutual legal assistance treaties (MLATs), which can be problematic as the slow pace at which such assistance requests are processed tends to be ill suited to obtaining digital evidence before it disappears (Eichensehr, 2017a).

Even if the individual or group who perpetrated the acts constituting transnational cyber economic espionage is identified, attributing the espionage to a state can be extremely challenging (Schmitt and Vihul, 2014). State sponsors may use independent hackers acting on the state's behalf, which allows these foreign governments to deny responsibility with some degree of believability (Office of the National Counterintelligence Executive, 2011; Yannakogeorgos, 2013). State involvement may be suspected when the cyber economic espionage aligns with a state's interests, but presuming state involvement is hazardous given the relatively low cost and technical expertise barriers to conducting cyber espionage, as it is not unfeasible for cyber espionage to be conducted by non-governmental individuals or groups (Schmitt and Vihul, 2014). Is the non-state actor simply a patriot acting on its own accord in a manner that aligns with the state's interests, a non-state actor pursuing its own interests in a manner which happens to also support the state's interests, or a non-state actor committing cyber economic espionage at the state's urging or with state support (Schmitt and Vihul, 2014)?

Under customary international law's state responsibility doctrine, transnational cyber economic espionage can be attributed to a state when conducted by: (1) an organ of the state (exercising governmental functions) -- such as an intelligence agency -- regardless of whether the

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

espionage was authorized; or (2) a non-state actor (e.g., private individuals, groups, corporations, etc.) acting upon the state's instructions or under its direction or control with regard to the cyber economic espionage operation (Banks, 2017b; Schmitt and Vihul, 2014; Schmitt and Vihul, 2017; Tran, 2018). Transnational cyber economic espionage will not be attributed to a state merely because it provided funding to the non-state actor that committed the espionage, nor is mere encouragement by the state enough for such attribution (Banks, 2017b; Margulies, 2013; Schmitt, 2013; Schmitt and Vihul, 2014). When technical attribution identifies a group of private individual hackers as the culprit, it can be difficult to prove with reasonable certainty that the state had the requisite level of control over their actions which constituted cyber economic espionage (Schmitt and Vihul, 2014; Tran, 2018).

There is also an additional hurdle – a state can only be held responsible, thus warranting countermeasures, if the action attributed to the state actually violates an international legal obligation, which are generally established by either treaties or customary international law (Banks, 2017b; Schmitt and Vihul, 2014). In the absence of a treaty prohibiting transnational cyber economic espionage (e.g., the U.S.-China Bilateral Security Agreement), it is debatable whether such activity violates an international legal obligation – arguably, it could be construed as a violation of state sovereignty, but this is far from settled international law (Anderson, 2017; Walton, 2017). Note that a state cannot be held responsible under customary international law for violation of a domestic law (Banks, 2017b).

Even if the cyber economic espionage violates an international legal obligation, it is likely that attribution to a state will occur too late for countermeasures to be an option, as states may hesitate to make such an accusation until they arrive at a high level of confidence in their assessment – an often lengthy process since it relies on considering a combination of digital

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

forensics, signals intelligence, human intelligence, and circumstantial evidence based on context (Banks, 2017b). If the violation is no longer ongoing (and thus any countermeasures employed may be viewed as punitive), a state's only available response may be retortions, which pale in comparison to the seriousness of the losses caused by the cyber espionage (Banks, 2017b).

While state sponsorship of transnational cyber economic espionage may often be suspected, the bar for establishing state responsibility is set high in light of the potential consequences of misattribution -- or even correct attribution without convincing evidence -- and restraint is typically the order of the day (Blinderman and Din, 2017). Any efforts to hold the perpetrators to account, whether that be through criminal prosecution, civil litigation, diplomacy, other governmental response, targets' self-help measures, or other means, are fraught with risk of international diplomatic ramifications, public relations disaster, retaliation, and escalation (Blinderman and Din, 2017; Crootof, 2018). Attribution of cyber espionage to a country has foreign policy impacts, as it may lead to suspension of important diplomatic negotiations, tensions in diplomatic relations, and even retaliatory hacking (Blinderman and Din, 2017). Thus, a targeted state may be reluctant to attribute transnational cyber economic espionage to a state in light of the aforementioned risks and the fact that available legal responses often end up being symbolic due to lack of jurisdiction or sovereign immunity and likely governmental responses, owing to reticence to start an escalating cyber war, may be extremely weak in comparison to the gravity of the offense (Blinderman and Din, 2017).

### **Conclusion**

In recent years, transnational cyber economic espionage has become a growing threat due to technological advances facilitating espionage from afar and the vulnerabilities associated with

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

mass digital storage of information and the interconnectedness of people and companies across borders in a globalized information economy (Argento, 2013; Crootof, 2018; Rowe, 2016). Technological advancement combined with state sponsoring of economic espionage has raised the stakes for finding a way to deter cyber economic espionage, prompting policymakers to pass domestic legislation seeking to address this problem and the international law community to grapple with formulating an understanding of how existing international law applies in the cyber context (Blinderman and Din, 2017; Carlin, 2016; Crootof, 2018; Lotrionte, 2015; Walton, 2017).

The United States has several domestic laws applicable to cyber economic espionage (Blinderman and Din, 2017; Rowe, 2016). However, when the perpetrators are foreign governments or private actors located abroad and acting under the direction of those governments, these laws are largely ineffective due to issues such as difficulty in attributing the bad acts to the perpetrators with sufficient certainty, inability to extradite the perpetrators to the United States to face prosecution and punishment, and sovereign immunity (Anderson, 2017; Blinderman and Din, 2017; Perloff-Giles, 2018). The relatively few attempts to use domestic laws to address transnational state-sponsored cyber economic espionage have had little more than symbolic value, which only serves to reveal the shortcomings of such an approach (Blinderman and Din, 2017; Carlin, 2016; Levandoski, 2018; Lotrionte, 2015).

International law does no better a job at addressing this pressing problem, offering little clarity regarding the regulation of transnational state-sponsored cyber economic espionage during peacetime (Walton, 2017). Despite rhetoric characterizing cyber attacks as acts of war, countries have not in practice retaliated as they would to acts of war due to the difficulties inherent in applying the law of armed conflict international legal framework, developed with

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

reference to the physical realm, to actions occurring in the information realm (Beard, 2014).

Neither the laws of war nor the customary international law principles of state sovereignty and non-intervention provide an effective legal framework for addressing transnational state-sponsored cyber economic espionage (Walton, 2017). As it currently stands, international law mainly functions only to limit a country's self-help options and offers little help in formulating effective responses to transnational state-sponsored cyber economic espionage (Crootof, 2018). Because countermeasures cannot lawfully be employed for purposes of punishment, targeted countries are often limited in their self-help response to retortions, a relatively weak response which allows states to escape any meaningful accountability for sponsoring transnational cyber economic espionage (Crootof, 2018).

A lack of clarity regarding how existing international law applies in the cyber context, compounded by difficulties in reaching the consensus necessary to formulate new international norms governing peacetime cyber espionage, leaves targeted countries with few effective options for combatting transnational state-sponsored cyber economic espionage without risking an escalating cyber war (Crootof, 2018; Reid, 2016). As it stands, we lack an adequate legal framework for effectively responding to the threat of transnational state-sponsored cyber economic espionage. Despite numerous legislative attempts to remedy this state of affairs, domestic law in the United States falls short due to the challenges of combatting a harm perpetrated from afar with the support of a foreign power using technology which readily obscures responsibility for such conduct (Blinderman and Din, 2017; Perloff-Giles, 2018). Given the massive scope of the problem, international law is astoundingly silent, by and large, on how nations can address peacetime transnational state-sponsored cyber economic espionage (Walton, 2017). Further complicating matters, nations with advanced cyber capabilities, such as

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

the United States, have incentives to not push for clarification of international law as it applies to cyberspace through norm building, lest they restrict their own options in dealing with national security threats (Crootof, 2018; Watts and Richard, 2018).

Treaties hold promise for addressing the problem, but have fallen short to date (Al Azzam, 2019; Marion, 2010). The Budapest Convention does not effectively address transnational state-sponsored cyber economic espionage because: (1) it does not provide a way to sanction the state sponsor itself since it takes a domestic law enforcement approach; (2) it relies on existing extradition treaties and does nothing to close loopholes which may allow the requested party to refuse extradition; and (3) its reach falls short of being truly global and does not bind nonparties – including states with a serious track record of transnational state-sponsored cyber economic espionage (Bande, 2018; Broadhurst and Chang, 2013; Carlin, 2016; Cerezo *et al*, 2007; Clough, 2014; Crootof, 2018; Inserra, 2017). The U.S.-China Bilateral Security Agreement attempts to directly address the problem of transnational state-sponsored cyber economic espionage, but is ineffective due to its lack of an enforcement mechanism (Anderson, 2017).

While certainly not an easy task, the most promising way forward is to develop a multilateral treaty under the auspices of the United Nations which specifically prohibits transnational state-sponsored cyber economic espionage, with provisions for an international tribunal to adjudicate attribution and impose sanctions on states which engage in transnational state-sponsored cyber economic espionage (Clough, 2014; Perloff-Giles, 2018; Tran, 2018). This solution provides the prospect of setting norms with a global reach – which is essential to effectively addressing transnational state-sponsored cyber economic espionage (Finnemore and Hollis, 2016). It also has the virtue of providing a mechanism for holding states accountable for

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

state sponsorship of transnational state-sponsored cyber economic espionage through multilateral action, thus avoiding the escalation risks posed by a victimized state's use of a unilateral response pursuant to customary international law in the absence of clarity regarding how international law norms developed for the physical realm apply in the cyber realm (Blinderman and Din, 2017; Crootof, 2018). Availability of sanctions may serve as a deterrent to stem the tide of transnational state-sponsored cyber economic espionage once states realize they can no longer engage in such conduct with impunity (Crootof, 2018; Inserra, 2017; Lotrionte, 2015). It certainly has the potential for improved deterrence compared to reliance on symbolic indictments under domestic law where the individuals involved receive no punishment due to lack of enforcement jurisdiction (Crootof, 2018; Lotrionte, 2015). Unlike countermeasures under customary international law, the availability of these sanctions would not be contingent on being able to attribute transnational cyber economic espionage to a state with reasonable certainty before the espionage has ceased – rather, the sanctions can provide an after-the-fact remedy that is punitive and intended as a deterrent for future similar transgressions (Banks, 2017b). While attribution will still be a challenging endeavor, such a treaty can at least provide a remedy in those cases where there is sufficient evidence to attribute transnational state-sponsored cyber economic espionage and can accommodate the reality that attribution may often come only after a lengthy investigation (Banks, 2017b).

Developing treaty provisions specifically addressing transnational state-sponsored cyber economic espionage will be extremely challenging, given countries' differing views regarding where to draw the line for what constitutes impermissible espionage (Banks, 2017a; Reid, 2016). However, the U.S.-China bilateral security agreement, followed by the G-20 countries subsequently embracing the norm against cyber espionage for commercial advantage, gives some



## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

hope that perhaps achieving consensus on an agreement narrowly addressing transnational state-sponsored cyber economic espionage, as opposed to cybercrime more generally, may have a shot at being successful (Finnemore and Hollis, 2016). Given the high economic stakes (Carlin, 2016; Reid, 2016) and potential for international conflict inherent in unilateral enforcement (Blinderman and Din, 2017), we cannot afford to shy away from doing the difficult work necessary to reach agreement on such treaty provisions.

Until such an agreement is reached, we are in a legal quagmire, with little in the way of effective options for deterring a growing economic threat (Crootof, 2018). Until the legal system develops a more effective legal framework for combatting transnational state-sponsored cyber economic espionage, private companies are left to play continual defense against cyber intrusions by well-organized, state-supported hackers (Crootof, 2018). However, the absence of effective legal recourse poses the risk that companies may choose to pursue vigilante justice by hacking back, which is fraught with perils in terms of foreign policy implications (Eichensehr, 2017b; Perloff-Giles, 2018). Hacking back poses a risk of harm to innocent parties due to misattribution, excessively punitive responses, and potential violations of domestic or international laws (Rowe, 2016). The time is long past for developing a multilateral global treaty specifically addressing transnational state-sponsored cyber economic espionage and providing an effective enforcement mechanism. Hopefully, it does not take a cataclysmic event to motivate countries to look beyond their own parochial interests in order to come to a consensus on a legal framework which can protect the long-term economic prosperity that comes with economic security.

**Notes**

<sup>1</sup> Cyber means relating to information technology such as computers, computer networks, and the internet (Nato Cooperative Cyber Defence Center of Excellence, n.d.).

**References**

- Ajayi, E.F.G. (2016) Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems* 6: 1-12.
- Al Azzam, F.A.F. (2019) The adequacy of the international cooperation means for combatting cybercrime and ways to modernize it. *JANUS.NET E-journal of International Relations* 10: 66-83.
- Anderson, P.C. (2017) Cyber attack exception to the Foreign Sovereign Immunities Act. *Cornell Law Review* 102: 1087-1113.
- Argento, Z. (2013) Killing the golden goose: The dangers of strengthening domestic trade secret rights in response to cyber-misappropriation. *Yale Journal of Law & Technology* 16: 172-235.
- Bande, L.C. (2018) Legislating against cyber crime in Southern African Development Community: Balancing international standards with country-specific specificities. *International Journal of Cyber Criminology* 12: 9-26.
- Banks, W. (2017a) Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory Law Journal* 66: 513-525.
- Banks, W. (2017b) State responsibility and attribution of cyber intrusions after Tallinn 2.0. *Texas Law Review* 95: 1487-1513.
- Beard, J.M. (2014) Legal phantoms in cyberspace: The problematic status of information as a weapon and a target under international humanitarian law. *Vanderbilt Journal of Transnational Law* 47: 67-144.

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Beauchamp, K. (2017) The failures of federalizing trade secrets: Why the Defend Trade Secrets Act of 2016 should preempt state law. *Mississippi Law Journal* 86: 1031-1074.

Blinderman, E. and Din, M. (2017) Hidden by sovereign shadows: Improving the domestic framework for deterring state-sponsored cybercrime. *Vanderbilt Journal of Transnational Law* 50: 889-931.

Brenner, S.W. and Koops, B.-J. (2004) Approaches to cybercrime jurisdiction. *Journal of High Technology Law* 4: 1-46.

Broadhurst, R. and Chang, L.Y. (2013) Cybercrime in Asia: Trends and challenges. In: *Handbook of Asian Criminology*. New York, NY: Springer, pp. 49-63.

Carlin, J.P. (2016) Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. *Harvard National Security Journal* 7: 391-435.

Cerezo, A.I., Lopez, J., and Patel, A. (2007) International cooperation to fight transnational cybercrime. *Proceedings of the International 2<sup>nd</sup> Annual Workshop on Digital Forensics & Incident Analysis; 27 August 2007, Samos, Greece*, doi: *10.1109/WDFIA.2007.4299369*

Clough, J. (2014) A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization. *Monash University Law Review* 40: 698-736.

Crootof, R. (2018) International cybertorts: Expanding accountability in cyberspace. *Cornell Law Review* 103: 565-644. Danielson, M.E.A. (2009) Economic espionage: A framework for a workable solution. *Minnesota Journal of Law, Science & Technology* 10(2): 503-548.

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Eichensehr, K.E. (2017a) Data extraterritoriality. *Texas Law Review* 95: 145-160. Eichensehr,

K.E. (2017b) Public-private cybersecurity. *Texas Law Review* 95: 467-538.

Finnemore, M. and Hollis, D.B. (2016) Constructing norms for global cybersecurity. *American Journal of International Law* 110: 425-479.

Hock, B. (2017) Transnational bribery: When is extraterritoriality appropriate? *Charleston Law Review* 11: 305-352.

Insera, D. (2017) Cybersecurity beyond U.S. borders: Engaging allies and deterring aggressors in cyberspace. The Heritage Foundation, 14 July, <https://www.heritage.org/cybersecurity/report/cybersecurity-beyond-us-borders-engaging-allies-and-deterring-aggressors>, accessed 20 July 2019.

Kosseff, J. (2019) Hacking cybersecurity law. SSRN, 8 February, doi: 10.2139/ssrn.3331350.

Levine, D.S. and Seaman, C.B. (2018) The DTSA at one: An empirical study of the first year of litigation under the Defend Trade Secrets Act. *Wake Forest Law Review* 53: 105-156.

Levandoski, S.D. (2018) To seize the initiative: Assessing constitutional due process challenges to the Defend Trade Secret Act's ex parte seizure provision. *New York University Law Review* 93: 865-902.

Lotrionte, C. (2015) Countering state-sponsored cyber economic espionage under international law. *North Carolina Journal of International Law and Commercial Regulation* 40: 443-541.

Marion, N.E. (2010) The Council of Europe's cyber crime treaty: An exercise in symbolic legislation. *International Journal of Cyber Criminology* 4: 699-712.

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Margulies, P. (2013) Sovereignty and cyber attacks: Technology's challenge to the law of state responsibility. *Melbourne Journal of International Law* 14: 496-520.

NATO Cooperative Cyber Defence Center of Excellence (n.d.) Cyber definitions.

<https://ccdcoe.org/cyber-definitions.html>, accessed 6 January 2019.

Office of the National Counterintelligence Executive (2011) Foreign Spies Stealing U.S.

Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011. Washington, DC: Office of the Director of National Intelligence.

Perloff-Giles, A. (2018) Transnational cyber offenses: Overcoming jurisdictional challenges.

*Yale Journal of International Law* 43: 191-227.

Pun, D. (2017) Rethinking espionage in the modern era. *Chicago Journal of International Law*

18: 353-391.

Reid, M. (2016) A comparative approach to economic espionage: Is any nation effectively

dealing with this global threat? *University of Miami Law Review* 70: 757-829.

Rowe, E. A. (2016) RATs, TRAPs, and trade secrets. *Boston College Law Review* 57: 381-426.

Schmitt, M. N. (ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber*

*Warfare*. Cambridge, United Kingdom: Cambridge University Press.

Schmitt, M.N. and Vihul, L. (2014) Proxy wars in cyberspace: The evolving international law of

attribution. *Fletcher Security Review* I(II): 55-73.

## CYBER ECONOMIC ESPIONAGE: A LEGAL QUAGMIRE

Schmitt, M. N. and Vihul, L. (eds.) (2017) Tallinn Manual 2.0 on the International Law

Applicable to Cyber Operations. Cambridge, United Kingdom: Cambridge University Press.

Tran, D. (2018) The law of attribution: Rules for attributing the source of a cyber-attack. *Yale Journal of Law & Technology* 20: 376-441.

Walton, B. A. (2017) Duties owed: Low-intensity cyber attacks and liability for transboundary torts in international law. *Yale Law Journal* 126: 1460-1519.

Watts, S. and Richard, T. (2018) Baseline territorial sovereignty and cyberspace. *Lewis & Clark Law Review* 22: 772-840.

Wu, M. (2016) The “China, Inc.” challenge to global trade governance. *Harvard International Law Journal* 57: 261-324.

Yannakogeorgos, P.A. (2013) *Strategies for Resolving the Cyber Attribution Challenge*.

Montgomery, AL: Air University Press. Air Force Research Institute Paper CPP-1.

### **Statutes**

Computer Fraud and Abuse Act (1986), 18 U.S.C. § 1030 (2015)

Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836 (2012 & Supp. IV 2017)

Economic Espionage Act of 1996, 18 U.S.C. §§1831-1839 (2012)

Uniform Trade Secrets Act (1979)