Washington and Lee Law Review Online

Volume 71 | Issue 2 Article 5

9-2014

Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth

Lawrence L. Muir Jr.
Washington and Lee University School of Law, muirl@wlu.edu

Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth

Lawrence L. Muir, Jr.*

Abstract

In May 2014, the Federal Bureau of Investigation indicted five Chinese nationals for cybercrimes against American companies. That indictment was an impotent response. The United States has no extradition treaty with China, and the defendants will in all likelihood never be tried in the United States. The inefficacy of the indictments highlights a larger problem: State-controlled cyberunits can act with impunity under the present mix of international and domestic law. No laws govern conduct between nation-states, and, thus, neither victims nor nation-states have recourse against violators.

This Article suggests that the United States should pursue national interest diplomacy to triangulate Russia and China by negotiating a trilateral cyberlaw treaty. The Article first demonstrates why the United States has failed in bilateral negotiations with these two nations in the past. It proposes that the United States should shift strategies by beginning to pursue national interest diplomacy rather than multilateral diplomacy. This strategy would encourage rapprochement with Russia first, thereby putting pressure on China to join the treaty or else be isolated. Finally, the Article lays out a workable framework on which policymakers can construct the diplomatic means to secure restitution for the victims of cyber-attacks.

---

* Adjunct Professor of Law, Washington and Lee University School of Law.

Table of Contents

I. Introduction

On May 1, 2014, a federal grand jury in Pittsburgh, Pennsylvania, handed down a thirty-one count indictment[1] against five Chinese military officers alleging that they intruded into six organizations' networks, including five multinational corporations.[2] The primary purpose of these intrusions was to gain relative economic strength against the United States by stealing trade secrets and engaging in economic espionage to benefit the Chinese government.[3] The Chinese conducted these cyber-attacks as part of an effort to fight U.S. steel tariffs that targeted Chinese exports.[4] The United States does not have an

---

1. *See* Indictment, United States v. Wang Dong, Criminal No. 14-118 (W.D. Pa. May 1, 2014) (indicting Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui for conspiracy to commit computer fraud and abuse, computer fraud and abuse, damaging a computer, aggravated identity theft, economic espionage, and theft of trade secrets).

2. *See* Devlin Barrett & Siobahn Gorman, *U.S. Charges Five in Chinese Army with Hacking,* WALL ST. J. (May 19, 2014), http://online.wsj.com/news/articles/SB10001424052702304422704579571604060696532 (last visited July 29, 2014) (describing the allegations contained in the United States' indictment against Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui) (on file with the Washington and Lee Law Review).

3. *See* John W. Miller, *Pittsburgh-Area Firms Allegedly Targeted by Hacking*, WALL ST. J. (May 19, 2014), http://online.wsj.com/news/articles/SB10001424052702304422704579572273980220140 (last visited July 29, 2014) (discussing Chinese cyber-attacks on the United Steelworkers union, Alcoa, Inc., Westinghouse Electric Co., and Allegheny Technologies, Inc. in which the "conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time") (on file with the Washington and Lee Law Review).

4. *See id.* (discussing how U.S. steel tariffs imposed in 2001 have resulted in American steelmakers filing seven complaints against China for trade violations).

extradition treaty with China, rendering the probability the People's Liberation Army ("PLA") officers will ever be tried by a federal court virtually nil.[5]

The incidents detailed in the indictment against these PLA officials were not the first acts of Chinese espionage directed against American corporations or the U.S. government. Prior to the indictment, American cybersecurity firm Mandiant issued a report detailing the existence of a special advanced persistent threat[6] unit of the PLA, called Unit 61398, dedicated to the computer network infiltration of the corporations of English-speaking nations.[7] The Chinese were suspected in other cyber-attacks against American corporations even before Mandiant published its report.[8] For example, a set of high-profile cyber-attacks on large companies in 2009, dubbed Operation Aurora,

---

5. *See* Barrett & Gorman, *supra* note 2 (noting that it is "unlikely [that] the suspects will ever be brought to trial in the U.S., [because] there is no extradition treaty with China").

6. An advanced persistent threat is:

> [A] network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

Margaret Rouse, *Advanced Persistent Threat (APT)*, SEARCHSECURITY, http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT (last visited July 30, 2014) (on file with the Washington and Lee Law Review); *see also Advanced Persistent Threats: How They Work*, SYMANTEC CORP., http://www.symantec.com/theme.jsp?themeid=apt-infographic-1 (last visited July 30, 2014) (providing that an advanced persistent threat "uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term") (on file with the Washington and Lee Law Review).

7. *See* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3, 9, 20–26 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (discussing the existence and operations of China's specialized cyber-attack military unit called PLA Unit 61398).

8. *See, e.g.*, Matthew J. Schwartz, *Google Aurora Hack Was Chinese Counterespionage Operation,* INFO. WK. (May 21, 2013), http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060? (last visited July 29, 2014) (discussing a set of cyber-attacks conducted by the Chinese government on at least thirty-four American companies in 2009) (on file with the Washington and Lee Law Review).

included attacks on Google to obtain Google's source code for its web search engine, information from private Gmail accounts, and information on undercover Chinese operatives contained in Google's law enforcement portal.[9] China was also suspected of engineering the malware that led to the theft of the security algorithm of RSA security tokens,[10] which eventually led to the hacking of Lockheed Martin and the theft of the plans for the U.S. military's F-35 fighter jet.[11] Akamai Technology published its *State of the Internet* report in which it found that approximately 41% of all cyber-attacks originated from China.[12]

China is not the only nation working against the United States' economic, military, and diplomatic interests. The Department of Justice is likely preparing an indictment against Russians for similar activity.[13] On June 30, 2014, the Financial Times reported that a Russian-linked hacking group entered the

---

9. *See id.* (explaining that the cyber-attack on Google stole information that "would have given attackers insight into active investigations being conducted by the FBI and other law enforcement agencies that involved undercover Chinese operatives").

10. An RSA token is either hardware or software "which is assigned to a computer user and which generates an authentication code at fixed intervals" to allow a user to join a secured network or access a secured network resource. *SecurID*, WIKIPEDIA, http://en.wikipedia.org/wiki/SecurID (last visited July 30, 2014) (on file with the Washington and Lee Law Review).

11. *See* Michael Joseph Gross, *Enter the Cyber-Dragon,* VANITY FAIR (September 2011), http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109 (last visited July 29, 2014) (discussing various Chinese cyber-attacks on American companies, including those on RSA, and the United States' responses) (on file with the Washington and Lee Law Review). The stolen information included plans for the fifth-generation fighter jet F-35, which has a remarkably similar Chinese counterpart: the J-20. *See* Ami Rojkes Dombe, *Lockheed Martin's Secrets in China's New Stealth Fighter*, ISRAEL DEF. (Mar. 16, 2014), http://www.israeldefense.com/?CategoryID=472&ArticleID=2811 (last visited July 29, 2014) (discussing the cyber-attacks conducted on Lockheed Martin and the similarities between the United States' and China's latest stealth fighter jets) (on file with the Washington and Lee Law Review).

12. *See* 7 AKAMAI'S STATE OF THE INTERNET 1, 4 (2014), http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf?WT.mc_id=soti_Q114 (providing statistics on the geographical origin of cyber-attacks by country for those countries with the highest origination traffic).

13. *See* Barrett & Gorman, *supra* note 2 (noting that "alleged hackers in Russia are likely to be charged soon" and that "U.S. agencies have also been investigating incidents with possible ties to Iran and Syria").

"industrial control systems of hundreds of European and [American] energy companies" and infected them with malware called "Energetic Bear."[14] The malware "allows its operators to monitor energy consumption in real time," indicating that Energetic Bear is primarily a tool for economic espionage.[15] The malware could, however, be repurposed to provide remote control over infected systems or to physically cripple them.[16] Speculation is that the hackers were working for the Federal Agency of Government Communications and Information (FAPSI)—the Russian equivalent of the NSA—but were not agents of the Russian military.[17]

The Russian military has units with cyber capabilities, like PLA 61398.[18] While PLA 61398 has engaged primarily in economic missions, the Russian units have stayed closer to a military mission. Prior to the Russian invasion of the nation of Georgia, the Russian military conducted cyber-warfare operations aimed at the Georgian government.[19] The Russians have more

---

14. *See* Sam Jones, *Energy Companies Hit By Cyber Attack from Russia-Linked Group,* FIN. TIMES (June 30, 2014), http://www.ft.com/cms/s/0/606b97b4-0057-11e4-8aaf-00144feab7de.html#axzz38shTkXxk (last visited July 29, 2014) (discussing a cyber-attack on the "industrial control systems of hundreds of European and US energy companies" conducted by "a state-backed group with apparent ties to Russia") (on file with the Washington and Lee Law Review).

15. *Id.*

16. *See id.* (noting that Energetic Bear could be used to "cripple physical systems such as wind turbines, gas pipelines and power plants at will" and comparing it to "the Stuxnet compute program created by the US and Israel that succeeded in infecting and sabotaging Iran's uranium enrichment facilities").

17. *See id.* (discussing "a former MI6 and military intelligence officer and founder of KCS Group['s]" opinion that the perpetrators were "working with F[APSI] . . . ; working to support mother Russia").

18. *See Russia Announces Development of Cyber Military Unit*, TRIPWIRE (Feb. 4, 2014), http://www.tripwire.com/state-of-security/top-security-stories/russia-announces-development-cyberwar-military-unit/ (last visited Aug. 4, 2014) (providing that "Russian government officials . . . announced [that] they intended to create a designated military unit devoted to preventing cyber-based attacks from disrupting vital systems devoted to Russian military operations") (on file with the Washington and Lee Law Review). Russia's newest cyber unit appears to be defensive in nature, however. *See id.* (noting that the Russian cyber unit "is intended to defend Russian armed forces' critical infrastructure from computer attacks" (internal quotation marks omitted)).

19. *See* John Markoff, *Before the Gunfire, Cyberattacks,* N.Y. TIMES (Aug.

recently complemented military action with cyber-attacks in activities connected to the Crimean secession from Ukraine and realignment with Russia.[20]

Foreign cyber-attacks have jeopardized the United States' iron grip on its standing as the world's foremost economic and military power. Token gestures, like the empty indictments of foreign nationals who will likely never have to account for their actions, underscore the impotence of the United States' reaction to Chinese cyber-espionage and Russian cyber-enhanced adventurism. This article suggests a course of action that will enable the United States to pursue its national interest in combatting foreign cyber-attacks by effectively imposing law and order upon itself, China, and Russia. The United States should enter into negotiations with China and Russia to form a trilateral treaty (hereinafter referred to as the "Cyber Treaty") establishing the rights and responsibilities of each nation when conducting cyber operations against one another.

This Article predicts that this triangulation will benefit the United States in the cyber realm in much the same way that President Richard Nixon's opening of China forced the Soviet Union to improve relations with the United States, thereby hastening the end of the Cold War. It begins by providing a condensed background on the *raison d'état* school of international relations, an overview of Cold War triangulation between these three nations, and a brief explanation of Sino-Russian relations

---

12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 (last visited Sept. 21, 2014) (discussing Russian cyber-attacks directed at Georgia prior to the Russian invasion, including distribution denial-of-service attacks that "effectively shut down Georgian servers") (on file with the Washington and Lee Law Review).

20. *See* Mark Clayton, *Massive Cyberattacks Slam Official Sites in Russia, Ukraine*. CHRISTIAN SCI. MONITOR (Mar. 18, 2014), http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0318/Massive-cyberattacks-slam-official-sites-in-Russia-Ukraine (last visited July 29, 2014) (describing a "back-and-forth volley of cyberattacks that began last week between Ukraine and Russia") (on file with the Washington and Lee Law Review). On the day of the Crimean referendum to secede from Ukraine, forty-two cyber-attacks hit Ukrainian government websites. *See id.* (noting that "Ukrainian government websites were hit by a wave of 42 cyberattacks during Crimea's vote to secede from Ukraine and join Russia").

to provide context for why triangulation will work in this updated cyber context. This Article then shifts focus from why triangulation will be effective to how the Cyber Treaty must look to be effective. It provides a framework that establishes a three-judge tribunal, specific extradition between the nations, and a set of substantive and procedural laws that define what can and cannot be done, by what actors, and against which targets. This Article demonstrates why the proposed Cyber Treaty is the most effective way to protect American corporate and national interests, safeguard civilian populations, and encourage governmental oversight of cyber-activities. Because historically, and today, Russia and China have much more to fear from each other than the United States,[21] this Cyber Treaty can pull each nation closer to the United States to effect the United States' national interest in restricting cyber-operations aimed at weakening the U.S. government and the businesses that give the United States its economic strength.

II. Foreign Policy Underlying the Cyber Treaty

A. The Cost of Cybercrime to the United States and Its Lack of Options to Act

The cost of cybercrime to the United States is staggering. Cybercrime causes financial losses to businesses and reduced economic growth for the nation, which in turn results in decreased employment figures. A recent McAfee report approximated that economic losses from cybercrime "could cost as many as 200,000 American jobs."[22] The labor force participation rate in the United States for 2013 was 63.2%, a thirty-five year

21. *See* HENRY KISSINGER, DIPLOMACY 729 (1994) (describing President Nixon's diplomacy with China as being based on the idea that "America's bargaining position would be strongest when America was closer to *both* communist giants than either was to the other").

22. CTR. FOR STRATEGIC AND INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME: ECONOMIC IMPACT OF CYBERCRIME II 3 (2014) [hereinafter MCAFEE REPORT], http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

low.[23] McAfee's estimate of job loss to cybercrime would add over a full tenth of a percentage to labor force participation. Cybercrime targets intellectual property, the research and development upon which future economic growth relies. McAfee estimates that cybercrime creates a 0.8% drag on global gross domestic product (GDP).[24] The U.S. Department of Commerce estimated the loss of intellectual property to American companies due to cybercrime to be a minimum of $200 billion annually.[25] That figure was not translated into a percentage drag on U.S. GDP, though the loss certainly retards economic growth.

It is clearly in the best interest of the United States, American businesses, and American workers to reduce the losses caused by cybercrime and cyber-espionage. What is less clear, and certainly has not been determined, is the most effective way to bring about this reduction. The traditional manner of handling criminal activity, trial and punishment,[26] is not fully effective in this context because the United States does not have extradition treaties with Russia or China, and therefore cannot enforce violations of American domestic law.[27] If domestic laws are unenforceable, then the United States must seek recourse through international law.

The only operative cybercrime convention—the European Union Convention on Cybercrime—has been signed and ratified by the United States, even though it is a non-member of the Council of Europe. China has not signed the convention; nor has

---

23. *See* Ali Meyer, *Labor Force Participation in 2013 Lowest in 35 Years*, CSNNEWS.COM (March 3, 2014), http://cnsnews.com/news/article/ali-meyer/labor-force-participation-2013-lowest-35-years (last visited July 29, 2014) (noting that the "average annual labor force participation rate hit a 35-year-low of 63.2 percent in the United States in 2013, according to data from the Bureau of Labor Statistics") (on file with the Washington and Lee Law Review).

24. MCAFEE REPORT, *supra* note 22, at 11.

25. *See id.* at 12 (noting that the Department of Commerce report found that "IP theft (all kinds, not just cybercrime) costs US companies $200 to $250 billion annually").

26. For example, restitution, fines, or imprisonment.

27. *See List of United States Extradition Treaties*, WIKIPEDIA, http://en.wikipedia.org/wiki/List_of_United_States_extradition_treaties (last visited July 29, 2014) (showing that the United States does not currently have an extradition treaty with China or Russia) (on file with the Washington and Lee Law Review).

Russia, despite being a member of the Council. The United States, therefore, has no recourse in domestic or international law to enforce cybercrime laws. To achieve the United States' goal of reducing cybercrime to enhance domestic economic growth, this lack of recourse must be remedied through precise diplomatic means.

1. Historic and Current Bilateral Diplomatic Failures Involving China and Russia

In the bipolar world between the start of the Cold War and the opening of China, relations between the United States and the Soviet Union were marked by a lack of discernible progress for the United States. The Soviet sphere of influence spread into Eastern Europe with little American opposition;[28] a diplomatic stalemate for the United States at best. The Historian of the State Department described President Kennedy's foreign policy with the Soviets, which continued through President Johnson's administration, as "marred by a string of failures."[29] While the United States diplomatic failures with the Soviets allowed the Soviet Union to dictate terms, the United States diplomatic posture towards China was non-recognition of the government and blockage of China's joining the United Nations until 1971.[30]

---

28. The Soviets toppled a freely elected non-Communist government in Hungary, and invaded Czechoslovakia in 1968. *See generally The 1956 Hungarian Revolution: A History in Documents*, THE NAT'L SEC. ARCHIVE, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB76/ (last visited Aug. 11, 2014) (discussing how the Soviet Union crushed the Hungarian Revolution of 1956) (on file with the Washington and Lee Law Review); *Soviet Invasion of Czechoslovakia, 1968*, U.S. DEP'T OF STATE OFFICE OF THE HISTORIAN, https://history.state.gov/milestones/1961-1968/soviet-invasion-czechoslavkia (last visited Aug. 11, 2014) (discussing the Soviet invasion of Czechoslovakia in 1968) (on file with the Washington and Lee Law Review).

29. *A Short History of the Dep't of State*, U.S. DEP'T OF STATE OFFICE OF THE HISTORIAN, https://history.state.gov/departmenthistory/short-history/jfk-foreignpolicy (last visited July 29, 2014) (describing American foreign policy defeats to the Soviet Union over the Berlin Wall and at the Vienna Summit) (on file with the Washington and Lee Law Review).

30. *See China and the United Nations*, WIKIPEDIA, http://en.wikipedia.org/wiki/China_and_the_United_Nations (last visited July 29, 2014) (discussing the history of China's admittance to the U.N. Security

Both nations, individually, were enemies of the United States. The United States' performance with these two nations in bilateral negotiations has not fared better in the last forty years. The next section addresses very recent diplomatic American diplomatic failures.

a. Bilateral Failures with China: Failing to Understand China's Pursuit of Its National Self-Interest.

The United States has repeatedly sought cooperation directly from China on the issue of cybercrime, but each bilateral meeting has failed to produce any accords between the two nations.[31] In June 2013, President Obama stated to Chinese President Xi Jinping that "he want[ed] a world where all countries play by the same rules on cybersecurity."[32] However, the fledgling cooperation between China and the United States on cybercrime has since ground to a halt.[33]

Bilateral negotiation with China has not produced any meaningful progress for the United States.[34] This lack of progress

---

Council) (on file with the Washington and Lee Law Review).

31. *See* Bradley Klapper & Louise Watt, *U.S., China Talk Cyber Hacking Amid New Allegations,* HUFFINGTON POST (July 10, 2014), http://www.huffingtonpost.com/2014/07/10/us-china-cyberhacking_n_5574260.html (last visited Aug. 5, 2014) (discussing the "Strategic and Economic Dialogue" between the United States and China, in which the countries discussed cybercrime, but failed to come to a specific agreement on the issue) (on file with the Washington and Lee Law Review).

32. Rory Carroll, *Barack Obama and Xi Jinping Meet as Cyber-Scandals Swirl,* THE GUARDIAN (June 8, 2013), http://www.theguardian.com/world/2013/jun/08/obama-xi-jinping-meet-cyberscandals (last visited July 29, 2014) (on file with the Washington and Lee Law Review).

33. *See* Alina Selyukh & Doina Chiacu, *China Cyber Crime Cooperation Stalls After U.S. Hacking Charges*, REUTERS (June 26, 2014), http://www.reuters.com/article/2014/06/26/us-usa-cybersecurity-china-idUSKBN0F12OJ20140626 (last visited Aug. 5, 2014) (discussing how "cooperation has stopped" on combating cybercrime after the United States indicted Chinese officials for cyber-attacks) (on file with the Washington and Lee Law Review).

34. On the cybercrime issue and others. A promising bilateral investment treaty from the 2013 talks was said to be "facing big difficulties." *See* Kevin Yao & Nick Macfie, *China Says Investment Talks with U.S. Facing Difficulties*, REUTERS (July 10, 2014), http://www.reuters.com/article/2014/07/10/us-china-usa-talks-idUSKBN0FF17620140710 (last visited July 29, 2014) (providing that

is due to the President's misunderstanding of Chinese foreign policy, as evidenced by his calling for a single set of rules followed by all nations. Chinese foreign policy reserves "deep skepticism . . . about the liberal premises and basic concept of global governance, seeing it as the latest 'trap' laid by the West (primarily the United States) to 'bleed' China by getting it involved in crises and places where it does not have a direct national interest."[35] To succeed in negotiations with China, the United States must avoid global, collective goals, and speak in terms of national interest; and China has a strong national interest in continuing its cybercrime spree against the United States.

b. Bilateral Failures with Russia: Failing to Understand Russia's Pursuit of Its National Self-Interest

The United States is in even worse diplomatic straits with Russia. The United States has imposed sanctions against Russian businessmen in response to Russian action in the Ukraine.[36] Those sanctions have not been fully effective, as European sanctions have not dovetailed with the American sanctions, allowing a Russian end-run around the United States' sanctions.[37] Moreover, the United States has actually increased

---

"[n]egotiations between China and the United States on a bilateral investment treaty [were] facing big difficulties") (on file with the Washington and Lee Law Review).

35. David Shambaugh, *The Illusion of Chinese Power,* THE NAT'L INTEREST (June 25, 2014), http://nationalinterest.org/feature/the-illusion-chinese-power-10739?page=show (last visited July 29, 2014) (on file with the Washington and Lee Law Review).

36. *See* Julie Pace, *U.S. Preparing Unilateral Sanctions on Russia*, ASSOCIATED PRESS (July 16, 2014), http://news.yahoo.com/us-preparing-unilateral-sanctions-russia-193329225--politics.html (last visited July 29, 2014) (discussing the United States' imposition of economic sanctions against Russia in response to "its threatening moves in Ukraine") (on file with the Washington and Lee Law Review).

37. *See* Carol Matlack, *Russia Sanctions Lose Their Bite As U.S. and Europe Pull in Different Directions*, BLOOMBERG BUS. (July 2, 2014), http://www.businessweek.com/articles/2014-07-02/russia-sanctions-lose-their-bite-as-u-dot-s-dot-and-europe-pull-in-different-directions (last visited Aug. 5, 2014) (explaining that Western sanctions against Russia have "caused no more

trade with Russia since the sanctions were imposed.[38] Despite these ineffective sanctions—the diplomatic equivalent of an indictment that will go forever unserved—Russia's Deputy Foreign Minister, Sergei Ryabkov, stated that "the United States had wrapped up all tried and effective forms of cooperation and dialogue with Russia."[39] He compared current United States policy to the containment principle at the outset of the Cold War, and then taunted that: "These are methods of the past, the very old past. If they are using these methods[,] their foreign policy arsenal must . . . not [be] very rich."[40] Minister Ryabkov ultimately threatened that Russia would deploy a new weapon as retaliation for the sanctions.[41]

But, within Minister Ryabkov's taunts lies the United States' route toward successfully reducing adversarial cyber-activities. He stated: "In essence, they (the United States) reject the very possibility of us having any national interests. They reject the possibility of a model of values that is different from the one used by the [United States] and other Western countries."[42] If the United States is to make an effective effort against foreign cyber-attacks, it must pivot toward a foreign policy based on pursuing its national interest and allow Russia and China to pursue their national interests as well.

---

than moderate inconvenience to their targets" because sanctions "imposed by the U.S. and its European allies have been out of sync") (on file with the Washington and Lee Law Review).

38. *See* Kenneth Rapoza, *U.S. Exports to Russia Rise Despite Tensions, Minor Sanctions*, FORBES (July 4, 2014), http://www.forbes.com/sites/kenrapoza/2014/07/04/u-s-exports-to-russia-rise-despite-tensions-minor-sanctions/ (last visited Aug. 5, 2014) (noting that the United States "exported more good[s] and services to Russia" in May 2014 than any other month of 2014 despite sanctions "targeted towards a handful of Russian oligarchs") (on file with the Washington and Lee Law Review).

39. *US Sanctions Are New Type of Offensive Weapon—Russia's Deputy FM*, RT (July 4, 2014), http://rt.com/politics/170424-us-sanctions-weapon-russia/ (last visited July 29, 2014) (on file with the Washington and Lee Law Review).

40. *Id.*

41. *See id.* (explaining that Rayabkov "warned that Russia was preparing a response" to the United States' sanctions, noting that "[t]here must be a defensive weapon for every offensive weapon" and that Russia is "working on it now").

42. *Id.*

Minister Ryabkov's allusion to containment policy ("the very old past") begs comparison to a more recent and successful foreign policy strategy: that of triangulation. In the past, triangulation allowed the United States, the Soviet Union, and China to pursue their own national interests. This strategy ultimately hastened the collapse of the Soviet Union, and has the potential to assist the United States in challenging Chinese cyber-attacks.

2. Triangulation Between the United States, China, and Russia Provides the United States with the Greatest Number of Options and Highest Probability of Success

The concept of Cold War triangulation was first mentioned in the 1968 Republican presidential nomination contest. Governor Nelson Rockefeller had suggested that by forming "a subtle triangle of relations between [the United States, the Soviet Union, and China, the United States would] improve the possibilities of accommodations with each as [the United States] increas[ed its] options toward both."[43] Improving relations with China to achieve American interests adverse to the Soviet Union ultimately worked, hastening the collapse of the Soviet Union to end the Cold War. In a subtle reversal of influence, today the use of triangulation with Russia could exert influence upon China to modify its behavior and cool down the cyber-war.

a. How Triangulation Ended the Cold War

Prior to the exploration of diplomatic relations with China, the Soviet sphere of influence had expanded deep into Eastern Europe.[44] The United States' policy of containment, which effectively tried to stop Soviet expansion while awaiting the

43. KISSINGER, *supra* note 21, at 721.

44. The Soviets installed a Communist government in Hungary despite free election results that went against the Communists, and smashed the Czechoslovak uprising. *See generally The 1956 Hungarian Revolution: A History in Documents*, *supra* note 28 (discussing Soviet military intervention after the Hungarian Revolution of 1956).

internal collapse of the Soviet Union, at best produced a geopolitical stalemate between the two nations.[45] President Nixon's administration sought to reverse this course.

As Soviet influence spread west across Europe, the Soviet Union's relationship with China began to deteriorate. In 1962, Chinese immigrants began moving into the Soviet Union.[46] In 1964, Chairman Mao Zedong stated, amidst the rising tensions, "that Tsarist Russia had stripped China of vast territories in Siberia."[47] In 1969, small-scale combat erupted between the two nations, with both sides suffering casualties.[48] The Soviets had inadvertently opened a second front in the Cold War.

The United States sensed an opportunity to weaken the Soviet Union by supporting China.[49] The United States made unilateral advances toward China to signal to its erstwhile enemy that the United States would support its government. These minor gestures, such as allowing for small exports of goods,[50] opened the door to cooperation on major issues.[51]

---

45. *See* KISSINGER, *supra* note 21, at 482–90 (explaining that the application of containment theory in the Korean War resulted in a calculated stalemate because the United States miscalculated Soviet and Chinese power and resolve to support communist rule in Korea).

46. *See Sino-Soviet Border Conflict*, WIKIPEDIA, http://en.wikipedia.org/wiki/Sino-Soviet_border_conflict (last visited July 29, 2014) (discussing how the Sino-Soviet border conflict began when ethnic Uyghur refugees crossed into Soviet territory and China accused the Soviets of subverting the Uyghur population) (on file with the Washington and Lee Law Review).

47. *Id*.

48. *See id.* (discussing how Chinese troops "ambushed Soviet border guards on Zhenbao Island" on March 2, 1969).

49. *See* KISSINGER, *supra* note 21, at 722–23 (explaining that the United States aligned with China because it feared that the "application of the Brezhnev Doctrine to China would mean that Moscow would try to make the government in Beijing as submissive as Czechoslovakia's had been obliged to become").

50. *See id.* at 723 (noting that the "prohibition against Americans' traveling to [China] was eliminated," that "Americans were allowed to bring $100 worth of Chinese-made goods into the United States," and that "limited American grain shipments were permitted to China").

51. *See id.* (explaining that the United States' minor gestures toward China, "though insignificant in themselves, were designed to convey America's new approach").

The United States believed that triangulation would be effective because so long as the Soviet Union and China had more to fear from each other than from the United States, both nations would seek to grow closer to the United States to gain an advantage over the other.[52] To put it more constructively, both nations calculated that they either needed the United States' goodwill or feared that the United States would move toward its adversary, thereby providing an incentive to improve relations with the United States.[53] The Soviets acted on this incentive, leading to the eventual reforms sought by Mikhail Gorbachev and the ultimate collapse of the Soviet Union. Though the relative strength of China and Russia have since reversed, the United States remains the strongest party, and both nations are better off working with the United States than against it, which sets the stage for the Cyber Treaty.

b. Why Triangulation Can Work to End the Cyber-War

To negotiate a cyber treaty, each of the three nations must be convinced that the treaty is in its best national interest. This next section explores how each nation could benefit from entering into the Cyber Treaty.

(1) Issues Between Russia and China

Triangulation worked for the Nixon administration because China and Russia were heading toward a border war, and moving closer to the United States could provide a strategic advantage for each. The current context is a bit different for the United

52. *See id.* at 730 (explaining that triangulation succeeded because it created an incentive for the Soviet Union "to moderate existing crises and to avoid stirring up new ones while faced with resistance" from NATO and China, and China needed the United States' "goodwill in setting limits to Soviet adventurism").

53. *See id.* at 725 (noting that the "ostentatious renunciation of collusion with either of the communist giants served as an invitation to each to improve relations with Washington, and as a warning to each of the consequences of continued hostility").

States, as a Western-led push against Russia has in turn pushed Russia, which is economically heavily dependent upon energy exports,[54] into a thirty-year energy deal with China worth approximately $400 billion.[55] This deal secured China's long-term energy needs to fuel future economic growth and further increases China's influence over the Russian economy.[56] Though at first blush this deal appears to undo the basis for successful triangulation, further analysis shows that this is a positive factor for the United States as it appears that the balance of power between Russia and China is tilting continuously toward China.[57]

Russia and China have a long history of geopolitical tension. The Border Conflict of 1969 is replaying itself today. In June 2010, China leased 426,600 hectares of Russian land to Chinese farmers.[58] Russians have called Chinese immigration the "Chinese conquest of Siberia,"[59] while China has historically claimed Siberia as its own.[60] Siberia is rich in natural resources, such as copper and zinc. One scholar projects the Chinese

---

54. *See Russia GDP Growth Rate*, TRADING ECONOMICS, http://www.tradingeconomics.com/russia/gdp-growth (last visited Aug. 11, 2014) ("[The energy sector] contributes 20 [to] 25 percent of GDP, 65 percent of total exports and 30 percent of government budget revenue.") (on file with the Washington and Lee Law Review).

55. *See* Remi Piet, *Russia-China Energy Deal: Geopolitical Tectonic Shift: Can an Emerging China-Russia Axis Challenge US Hegemony?*, AL JAZEERA (June 17, 2014), http://www.aljazeera.com/indepth/opinion/2014/06/russia-china-energy-alliance-ge-201461765254926525.html (last visited July 29, 2014) (noting that Russia and China "agreed on an unprecedented 30-year energy agreement . . . firmly strengthen[ing] the strategic Russian-Chinese cooperation ties and guarantee[ing] a much needed source of income for an ailing Russian economy") (on file with the Washington and Lee Law Review).

56. *See id.* (explaining that the deal "secured essential natural gas supplies to fuel future Chinese economic growth and further increase[d] Beijing's influence on the Russian economy").

57. *See id.* (stating the details of the deal and illustrating the weakening Russian economic position and the shift of the balance of power toward China).

58. Richard Rousseau, *Will China Colonize and Incorporate Siberia?*, HARV. INT'L REV. (July 09, 2012), http://hir.harvard.edu/archives/2949 (last visited Aug. 14, 2014) (on file with the Washington and Lee Law Review).

59. *Id.*

60. *See supra* note 47 and accompanying text (discussing the Sino-Russian border dispute over Siberia, which involved isolated military action in 1969).

encroachment into Siberia could push Russia into the arms of the West.[61]

There is a cyber connection to this analysis. While the Russian economy has struggled,[62] the Chinese economy grows.[63] Part of the engine driving Chinese economic growth is the theft of American intellectual property. While the United States spends 2.9% of its GDP on research and development, China only spends 1.7%.[64] It stands to reason that some of the disparity is due to China's theft of American research and development, obviating the need for greater investment. Thus, as China steals American intellectual property, China's growth rate remains high, at the expense of the Russian balance of power with China. This puts Russia into a position where limiting China's growth rate, particularly the rate driven by stolen intellectual property, benefits Russia's national interest as well as the United States' national interest.[65]

(2) Why Should China Cooperate with the United States on Cyber-Attacks?

---

61. Rousseau, *supra* note 58.

62. *See China vs. Russia—Economy Comparison*, INDEXMUNDI, http://www.indexmundi.com/factbook/compare/china.russia/economy (last visited July 29, 2014) (noting that the Russian economy grew at an approximate rate of 3.4% in 2012) (on file with the Washington and Lee Law Review). Russia is currently in a recession. *See* Piet, *supra* note 55 (noting that the "Russian economy [is] currently experiencing the first signs of a recession worsened by US and European sanctions").

63. *See China vs. Russia—Economy Comparison*, *supra* note 62 (providing that the Chinese economy grew at an approximate rate of 7.8% in 2012).

64. *See* Shambaugh, *supra* note 35 (noting that "in 2009 China spent only 1.7 percent of its GDP on research and development, compared with 2.9 percent in the United States").

65. As a side note, China must maintain a 7% growth rate to maintain full employment. *See* Shambaugh, *supra* note 35 (noting that the Chinese "government is struggling to maintain the 7 percent annual growth rates deemed necessary to maintain reasonably full employment, absorb new entrants into the workforce and sustain social stability"). Thus, Russia preventing Chinese growth based on stolen IP would create internal problems in China, to its advantage.

The World Bank reports that 26% of China's GDP comes from exports,[66] and "[e]xport growth has been a major component supporting China's rapid economic expansion."[67] The United States is China's largest trading partner, receiving 17% of Chinese exports.[68] Thus, the Chinese economy would be particularly sensitive to a trade war with the United States, and that is precisely what is developing. The cyber-attacks have contributed to the circumstances that are pushing the two countries towards the "brink of a trade war."[69]

In early June 2014, the U.S. Department of Commerce imposed significant duties on Chinese solar products, such as solar panels.[70] SolarWorld AG's American subsidiaries were victims of the Chinese hacking that led to the Wang Dong indictment. The other victim companies in that indictment were Pittsburgh-based companies with connections to the steel industry. The PLA hacked into U.S. Steel to gain inside information about the trade dispute involving steel pipes and tubes.[71] Since the start of 2013, U.S. steelmakers have filed seven

---

66. *See Exports of Goods and Services (% of GDP)*, WORLD BANK, http://data.worldbank.org/indicator/NE.EXP.GNFS.ZS (last visited July 29, 2014) (providing that exports of goods and services accounted for about 26% of China's GDP in 2013) (on file with the Washington and Lee Law Review).

67. *China Exports*, TRADING ECONOMICS, http://www.tradingeconomics.com/china/exports (last visited July 29, 2014) (on file with the Washington and Lee Law Review).

68. *See id.* ("China's main export partners are the United States (17 percent), European Union (16 percent), ASEAN (10 percent),Japan (7 percent) and South Korea.").

69. *See* Trish Regan, *The NSA and Dangers of a Trade War with China*, USA TODAY (June 8, 2014), http://www.usatoday.com/story/money/business/2014/06/08/trish-regan-china-trade-war/10072969/ (last visited July 29, 2014) (noting that the "United States may be on the brink of a trade war with . . . China" because of "cyberspying") (on file with the Washington and Lee Law Review).

70. *See* Everett Rosenfeld, *Solar Shares Leap as US-China Trade War Escalates*, CNBC (June 4, 2014), http://www.cnbc.com/id/101731790# (last visited July 29, 2014) (explaining that the "U.S. Commerce Department announced a new set of duties on Chinese solar products . . . , sending American solar stocks like First Solar and SunPower skyrocketing, and China-based Trina Solar and JinkoSolar falling") (on file with the Washington and Lee Law Review).

71. *See id.* (providing that the cyber-attacks on U.S. Steel "were designed to extract sensitive information from U.S. Steel employees during a trade dispute

trade complaints against China, the most since tariffs were imposed in 2001.[72]

For its part, China does not think that the United States is blameless. In retaliation for the indictment, China accused Cisco Systems of spying on behalf of the United States, "bann[ed] the use of Microsoft's Windows 8 operating system," and accused "Apple, Google, and Facebook [of] cooperat[ing] in a secret U.S. program to monitor China."[73] The destructive consequences of a trade war would be felt by companies on both sides, as Cisco earned 15% of its revenue in a nine-month period from Asia, including China, while Chinese competitors have eroded its business.[74] This means that China's accusation of Cisco spying may have less to do with accuracy and more to do with weakening an American competitor to bolster Chinese companies.

Thus, the two nations stand at the precipice of a trade war, fueled by the winds of a cyber-war. The Cyber Treaty, between the United States, Russia, and China—three nations whose economies need to export to each other—may be the diplomatic option that cools down this cyber-war. In this way, a Cyber Treaty could avoid the destructive economic consequences of a trade war between these nations. The United States must revive its Cold War strategy of triangulation, and that strategy must result in a treaty that creates mutual responsibilities, cultivates trust, and provides punishment for violations of that trust.

III. The Framework for the Cyber Treaty

---

over imports of steel pipes and tubes for the U.S. oil and gas industry").

72. *See* Miller, *supra* note 3 (noting that "U.S.-based steelmakers, led by U.S. Steel, have filed [forty] trade complaints with the U.S. government, including seven against China, the most intense period of trade litigation since 2001").

73. Regan, *supra* note 69.

74. *See* Austin Ramzy, *China Pulls Cisco into Dispute on Cyberspying*, N.Y. TIMES (May 27, 2014), http://www.nytimes.com/2014/05/28/business/international/china-pulls-cisco-into-dispute-on-cyberspying.html (last visited July 29, 2014) (noting that "[a]bout 15 percent of Cisco's revenue of $35.8 billion for the nine-month period ended in April came from Asia, including China," and that "sales in China dropped 7 percent") (on file with the Washington and Lee Law Review).

A. Goals Underlying the Cyber Treaty

To fulfill the United States' national interests, the Cyber Treaty should accomplish the following goals: 1) reduce the theft of intellectual property from businesses; 2) hold violators of the Cyber Treaty responsible; 3) protect civilian populations from the results of cyber-attacks on critical infrastructure; 4) prevent military units from engaging in cyber economic espionage on behalf of corporate entities; and 5) professionalize cyber-attacks by reducing the use of "paramilitary" hacker groups and other unaffiliated hackers. The terms of the Cyber Treaty should be written to support those goals by including mechanisms for the enforcement of the law and promoting cooperation between the nations.

The next two subparts provide an overview of the Cyber Treaty's framework. The first subpart provides for a tribunal to resolve disputes arising under the Cyber Treaty and details the organizational structure of the tribunal and its powers. The second subpart provides the substantive and procedural laws to guide the outcome of disputes and set the rules of the road for cyberspace conduct between these three nations *vis-a-vis* each other.

B. The Cyber Treaty's Framework: Enabling and Establishment Clauses

The subject of the Cyber Treaty is an amalgamation of different types of legal issues. Cyber law is not so much a body of law, such as torts or criminal law, but rather is a thread that weaves its way through the traditional bodies of law in search of the closest analogies. Thus, when cyber-attacks operate as cyber-warfare, the Cyber Treaty should look to guidance from the United Nations Charter provisions on kinetic warfare. When cyber-attacks operate as private cybercrime, the Cyber Treaty should borrow from American domestic criminal law and procedure, as well as look to the setup of the International Court of Justice and International Criminal Court for guidance. When cyber-attacks serve as cyber-espionage, particularly when the motive for the espionage is economic, the Cyber Treaty should

look to the dispute settlement process of the World Trade Organization.

The Cyber Treaty must provide a structure that organizes the tribunal, defines standing for parties, establishes jurisdiction, and has procedural rules for the operation of the tribunal. The following proposals rely heavily on treaties with dispute-resolution procedures, but are customized for the participation of only three nations, all of whom have demonstrated reluctance to concede sovereignty to international bodies. By borrowing from the most appropriate areas of extant multilateral organizations, familiarity with those processes will lead to a more effective treaty. The Cyber Treaty begins with establishing a tribunal to hear disputes.

1. Conceptual Framework of the Tribunal

Article 1 of the Cyber Treaty provides for the establishment of a tripartite tribunal with authority to resolve disputes and grievances arising under the treaty. Using common law distinctions, the tribunal should have civil law authority to hear disputes that are primarily economic in nature and also possess limited criminal jurisdiction. The criminal authority enables the court to act similarly to a magistrate court in the American federal judicial system, making probable cause determinations and extradition decisions.[75]

a. Organization of the Tribunal

The tribunal should consist of three judges. China, Russia, and the United States will each appoint one judge, qualified to practice law in his or her respective nation. The three judges form a panel, and the full panel should preside over each hearing. Though each judge is a national of a member party, the judges

75. *See* 18 U.S.C. § 3184 (2014) (providing magistrate judges with the authority to review extradition requests); Fed. R. Crim. P. Rule 5.1 (providing the procedure for and requiring a preliminary—probable cause—hearing when a defendant is charged with a crime).

shall be required to act impartially and conscientiously.[76] The court should not be seated in one fixed location, but rather should meet in the nation that is home to the aggrieved party.[77] The aggrieved party shall be the plaintiff in a civil case or the defendant in a criminal case.[78] The tribunal will decide cases based on a majority of votes.[79]

b. Competence of the Court

Competence of the court contemplates issues of jurisdiction, standing of the parties to participate, and applicable law. This Article recommends providing the court with both civil and criminal jurisdiction, addressing each separately.

(1) Who May Be a Party and How Matters are Referred

The World Trade Organization (WTO) and the International Court of Justice (ICJ) allow only member states to be parties to disputes before the court.[80] The International Criminal Court

---

76. *See* Statute of the International Court of Justice, art. 20, June 26, 1945, 59 Stat. 1031 [hereinafter ICJ Statute], T.S. 993, 39 AJIL Supp. 215 ("Every member of the Court shall, before taking up his duties, make a solemn declaration in open court that he will exercise his powers impartially and conscientiously.").

77. *See id.* art. 22 ("The seat of the court shall be established at The Hague. This, however, shall not prevent the Court from sitting and exercising its functions elsewhere whenever the Court considers it desirable."); Rome Statute of the International Criminal Court, art. 3, July 1, 2002, 2187 U.N.T.S. 90 [hereinafter Rome Statute] (fixing the seat of the court in the Hague, but allowing the court flexibility to determine appropriate seats when necessary).

78. *See* ICJ Statute, art. 34 (providing the court with jurisdiction to resolve disputes between states under international law); Rome Statute, art. 5 (providing the court with jurisdiction over prosecutions for genocide, war crimes, and crimes against humanity).

79. *See* ICJ Statute, art. 55 ("All questions shall be decided by a majority of the judges present."); Rome Statute, art. 54 ("The judges shall attempt to achieve unanimity in their decision, failing which the decision shall be taken by a majority of the judges.").

80. *See* ICJ Statute, art. 34(1) ("Only states may be parties in cases before the Court."); Marrakesh Agreement Establishing the World Trade Organization, Annex 2, art. 1, Apr. 15, 1994, 1867 U.N.T.S. 187 [hereinafter WTO Agreement]

(ICC) exercises jurisdiction over individuals or groups that have been accused of crimes.[81] The Cyber Treaty should provide the appropriate jurisdiction given the type of action before the tribunal and remedy sought by the aggrieved party.

(a) Civil Matters

In a civil case, only member parties may bring a complaint for a violation of the Cyber Treaty. Member parties may bring claims on behalf of the country, private parties, or both. Procedurally, when a company, public utility, or government agency has been the victim of a cyber-attack that can be attributed to a person or group within another signatory nation, the victim files a complaint with its national government. The national government will then formally file a complaint with the tribunal.[82] The government of the member nation will then represent the party or parties at the tribunal.

The rationale for this rule is judicial efficiency. Frequently cyber-attacks are bundled, and when one company or utility is a victim, other entities likely have been victimized in the same cyber-attack.[83] The evidence that supports a charge in one cyber-attack will frequently be the same evidence used to support allegations of another.[84] Thus, judicial economy is best served by allowing the court to hear related complaints in one hearing with plaintiffs and defendants acting through one counsel.

(providing the World Trade Organization's dispute-resolution procedures only apply to member states).

81. *See* Rome Statute, art. 12–13 (providing jurisdiction over the prosecution of individuals for crimes committed in the territory of a signatory state or when the defendant is a national of a signatory state).

82. *See* ICJ Statute, art. 36(1) (providing jurisdiction through referral by the parties); Rome Statute, art. 14 (providing that a state party may refer a crime to the Prosecutor to request an investigation).

83. *See, e.g.*, Barrett & Gorman, *supra* note 2 (noting that the Wang Dong indictment alleged that the defendants "hack[ed] into five U.S. companies and a labor union").

84. *See* MANDIANT, *supra* note 7, at 41–50 (discussing how Mandiant traced cyber-attacks across countries and companies to various Internet Protocol addresses and then to servers at one origination point).

(b) Criminal Matters

Neither the United States, Russia, nor China has shown a willingness to enter into multilateral treaties that would allow international tribunals to try their citizens on criminal charges. This Article seeks to provide a framework that will work in the real world, and therefore this Article does not recommend providing the tribunal with authority to try criminal offenses. However, the United States has taken the step of indicting five Chinese military officials, an empty gesture that underscores the need for extradition for cyber-attacks.

Federal Bureau of Investigation Director James Comey stated upon the indictment of the PLA officers that: "This is thievery, so we're going to investigate it and seek to prosecute it the way we do when anyone kicks in your door and steals something from your house or business."[85] Director Comey is right, but the nature of cyber offenses is that the thievery seldom requires a physical presence in the location of the purloined material, seldom requires physical transportation of the material, and frequently originates and is carried out in another nation. Thus, for the United States to act on Director Comey's sentiments, the United States must find a way to gain jurisdiction over these cyber door-kickers.

The Cyber Treaty contemplates providing an extradition forum for the limited number of cybercrimes that will be discussed below. As the United States does not have an extradition treaty with China or Russia, this very limited extradition would be an effective first step toward resolving the need to hold people responsible for the damage done by cyber-attacks, balanced against the clear reluctance to allow any of the nations to try another nation's citizens for crimes.

Procedurally, if a country indicts a foreign national under any substantive criminal charge the Cyber Treaty specifically creates or incorporates, then the indicted defendants should be taken forthwith into custody by the national law enforcement agency of the host nation. Upon referral by the Attorney General

85. Barrett & Gorman, *supra* note 2 (internal quotation marks omitted).

(or equivalent) of any nation, and within a period of time to be determined, the panel should convene in a city in the nation where the defendant is being held. The three-judge panel should review the evidence against that person in an adversarial setting, and if a majority of the judges determine that the indictment is supported by probable cause, the defendant shall be extradited for trial in the charging nation. The hearing is designed to provide confidence in the validity of the charges. More importantly, the extradition provision forces all three nations into defining what conduct, committed by whom, is disallowed. The larger goal achieved by the extradition power is that the three nations must impose rules upon cyber-warfare, where none have previously existed.

(2) Jurisdiction

The tribunal should have jurisdiction in civil matters arising from violations of the substantive laws of the Cyber Treaty. In addition, the tribunal should have jurisdiction in criminal matters concerning violations of treaty provisions or violations of specific criminal provisions of the domestic laws of a nation that have been incorporated into the Cyber Treaty.

(a) Civil Jurisdiction

The primary basis for referred complaints falling under civil jurisdiction will concern the theft of intellectual property and research and development through cybercrime and cyber-espionage. These complaints will be akin to complaints referred to the WTO. Under the WTO Dispute Settlement Understanding (DSU), the basis or cause of action for a WTO dispute must be found in the "covered agreements" listed in Appendix 1 to the DSU.[86] Put another way, it is not the DSU that gives rise to the action, but the WTO Agreements that give parties their

86. *See* WTO Agreement, Annex 2, art. 1(1) (providing that the WTO dispute resolution system only applies to "the agreements listed in Appendix 1" to Annex 2 of the WTO Agreement).

substantive rights and obligations and determine the possible grounds for action.[87] Thus, the Cyber Treaty will have to provide the causes of action that the tribunal will ultimately hear.

The Cyber Treaty may include existing agreements, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights. However, such agreements contemplate disputes outside of the cyber realm, and the Cyber Treaty should be narrowly tailored to address cyber issues. Broader still is the Statute of the International Court of Justice, which will exercise jurisdiction on any matter referred to it concerning "the interpretation of a treaty;" "any question of international law;" "the existence of any fact which, if established, would be a breach of international obligation;" and "the nature or extent of reparations to be made for the breach of an international obligation."[88] Although this section covers civil jurisdiction, analogous international treaties for civil matters are too broad for the Cyber Treaty's purposes, and thus it is better to examine the jurisdiction method of the ICC.

Article 5 of the Rome Statute establishes the International Criminal Court's jurisdiction. It states that the court's jurisdiction is limited to "the most serious crimes," and then enumerates the four crimes as: genocide, crimes against humanity, war crimes, and the crime of aggression.[89] The subsequent Articles, six through eight, lay out the definitions and elements of the first three crimes.[90] The Cyber Treaty should exercise such precision in its jurisdiction over both civil and criminal matters. For the purposes of this section, such civil offenses should be drawn around specified actions. Though discussed later, the civil actions should include the cyber-theft of trade secrets, cyber-espionage of intellectual property, cyber-espionage of information for economic advantage, and identity theft with intent to gain economic advantage.

---

87. *See id.* app. 1 (providing that the covered agreements are the Agreement Establishing the WTO and various multilateral and plurilateral trade agreements).

88. ICJ Statute, art. 36(2).

89. Rome Statute, art. 5.

90. *See id.* art. 6–8 (defining the crimes of genocide, crimes against humanity, and war crimes).

(b) Criminal Jurisdiction

Article 1 of the Rome Statute invests the ICC with "the power to exercise its jurisdiction over persons for the most serious crimes of international concern, as referred to in th[e] Statute, and shall be complementary to national criminal jurisdictions."[91] This co-linear jurisdiction works perfectly for the Cyber Treaty, particularly given the court's limited powers to function as a court that conducts probable cause hearings to determine extradition for specific crimes. The specific crimes, detailed in a subsequent section, should include crimes specifically written into the Cyber Treaty and domestic criminal offenses that are unanimously adopted by the three member nations and incorporated by reference into the treaty.

As with the ICC, the Cyber Treaty tribunal should acquire jurisdiction through referral by a member party.[92] Jurisdiction of the Cyber Treaty tribunal diverges from ICC jurisdiction at this point. The ICC has its own Prosecutor,[93] while prosecution under the Cyber Treaty shall be handled by the member nation's jurisdiction wherein the victims reside. As explained previously, the Attorney General (or equivalent) must refer the charging document to the tribunal.[94] Once extradition has been granted upon probable cause the nation that indicted the defendant will try the case. The criminal jurisdiction of the court is therefore limited in scope—probable cause and extradition—and temporary, lasting only from referral of the charging document until extradition has been accomplished through the transfer of custody.

Once the procedural matters for the operation of the tribunal have been established, the negotiators can address the substantive and procedural laws the court will follow. The next subpart discusses a framework for substantive laws.

---

91. *Id.* art. 1.

92. *See id.* art. 13(a) (allowing the court jurisdiction through referral to the Prosecutor of the ICC by a member nation).

93. *See id.* art. 15 (prescribing the role and responsibilities of the Prosecutor).

94. *See infra* Part III.B.1.b(1)(b) (proposing procedures for extraditing individual defendants for prosecution in the victim-nation).

C. Substantive and Procedural Laws

The Cyber Treaty should provide for carefully drafted laws to clearly articulate the substantive crimes and procedural rules to be followed by the tribunal. That drafting is beyond the scope of this Article. However, this Article does provide a conceptual framework for crafting such laws. The following sections prioritize the considerations for the drafters, beginning with the substantive laws.

1. Assets to Be Protected

Hackers commit sophisticated cyber-attacks for two reasons: to steal information or to disrupt services. Nations should therefore identify what assets they seek to protect under the Cyber Treaty, and from that point work backward to circumscribe which acts may be committed by which actors. Using this framework will allow for the narrow tailoring of laws to precisely achieve the desired goals.

The two most prized assets subject to cyber-attack are critical infrastructure systems and intellectual property, particularly trade secrets and research to be patented. The goals of cyber-attacks on critical infrastructure are primarily disruption of service and gathering intelligence. Critical infrastructure systems[95] often have a cyber-backbone. Energy production is often operated and monitored by supervisory control and data acquisition systems that rely upon properly operating computers and network connections. Banking systems rely upon the security of online login credentials and the storage of transactions and account balances. Though the functions of these two types of infrastructure are entirely different, their commonality is that they allow for the day-to-day living of the

95. Critical infrastructure systems include power grids and their operating systems, water distribution centers, transportation systems, financial systems, etc. *See Critical Infrastructure*, WIKIPEDIA, http://en.wikipedia.org/wiki/Critical_infrastructure (last visited July 29, 2014) (describing "assets that are essential for the functioning of a society and economy" and regional critical infrastructure protection programs) (on file with the Washington and Lee Law Review).

civilian population. A disruption of electricity service, or locking people out of the financial system, can grind economic activity to a halt, which can paralyze a nation.[96]

International law purports to protect civilians from military attack.[97] This protection specifically includes acts that have a "primary purpose of . . . spread[ing] terror among the civilian population."[98] This guideline should be analogized to prohibit using cyber-attacks to *shutdown* of the operation of critical infrastructure that provides services to a civilian population.

Cyber-thieves frequently target private businesses to steal intellectual property. Much of the value of intellectual property is in the exclusivity of knowledge by the owner. Once the exclusivity is lost, competitors can use that knowledge to produce the same items for significantly less cost, eroding the profits of the inventor. The United States—and most of the American states—has laws protecting trade secrets.[99] The unfortunate reality is that many developing nations rely on economic espionage to bolster their economic growth,[100] and once exclusivity of

---

96. *See* Jason Richards, *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security,* 18 G.W. INT'L AFF. REV. (2009), *available at* http://www.iar-gwu.org/node/65 (noting that a "sustained attack" on Supervisory Control and Data Acquisition systems that "run much of U.S. [critical infrastructure], including those sectors that regulate water and electricity distribution, and mass transit" could "bring about disastrous consequences for the quality of American life").

97. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, art. 51, 1125 U.N.T.S. 3 [hereinafter Protocol 1] (providing that the "civilian population and individual civilians shall enjoy general protection against dangers arising from military operations").

98. *Id.* art. 51(2).

99. *See* 18 U.S.C. § 1832 (2014) (criminalizing the intentional conversion of a trade secret for "the economic benefit of anyone other than the owner thereof," and with the intent or knowledge that the act will "injure any owner of that trade secret"). Forty-eight states have enacted the Uniform Trade Secrets Act. Bradley E. Chambers, *Texas Joins 47 Other States to Adopt the Uniform Trade Secrets Act*, BAKER DONELSON (May 30, 2013), http://www.bakerdonelson.com/texas-joins-47-other-states-to-adopt-the-uniform-trade-secrets-act-05-30-2013/ (last visited Sept. 21, 2014) (on file with the Washington and Lee Law Review).

100. *See* James Surowiecki, *Spy vs. Spy,* THE NEW YORKER (June 9, 2014), http://www.newyorker.com/magazine/2014/06/09/spy-vs-spy-3 (last visited Aug. 6, 2014) (noting that "engaging in economic espionage is something developing

intellectual property is lost it is generally lost for all time. The legal interest in this treaty is reduction, not elimination, of economic espionage. The threat of a civil cause of action to provide compensation to the victims, and extradition to resolve criminal charges against the perpetrators, should deter some cyber-thieves.

2. Prohibited Acts

The Cyber Treaty should break down prohibited acts into three groups, allowing for a degree of overlap. The classifications are cybercrimes, cyber-espionage, and cyber-warfare. Cybercrimes should focus on acts directed at individuals and interrupting transactions for businesses. Cybercrimes would include the theft of login credentials in furtherance of larceny, theft of payment card information, denial of service attacks aimed at commercial websites, and the like. Losses should be aggregated to promote judicial economy. The rationale for the prosecution of cybercrime is to prevent large-scale capital outflow and lost profits.

Cyber-espionage is the middle ground bridging cybercrime and cyber-warfare. Cyber-espionage has a similar economic motive to cybercrime, but is tied into the theft of intellectual property, and when completed, causes massive financial losses. It may also serve as the precursor to cyber-warfare: for instance, mapping a power grid and planting logic bombs in the event of launching a cyber-attack. The Cyber Treaty must differentiate between the valid role of cyber-espionage for intelligence agencies—gathering intelligence—and acts that can harm civilians.

Cyber-warfare may be the most critical section to negotiate. The rules should specifically delineate what cyber-attacks military cyber-units may carry out and against whom. The intent of this section of the treaty should be nothing less than to civilize

---

countries do. When you're not yet generating a lot of intellectual property on your own, you imitate") (on file with the Washington and Lee Law Review).

cyber-warfare through the protection of civilian populations while still recognizing the proper military uses of these tactics.

3. Actors

Cyber-attackers can fall into one of three groups: citizens, military, and "paramilitary," meaning private citizens working under the direction of the military. The goal of the Cyber Treaty should be to maintain order in hacking by way of discouraging citizen hackers from committing acts that bring about serious detrimental consequences. This goal can be achieved by squeezing from two directions. First, military cyber-units should be given more latitude to commit acts, since chains of command and state sponsorship bring oversight and responsibility to actions. Second, military members could be given extraterritorial immunity from treaty violations under certain circumstances,[101] while civilian hackers could face both civil damages and criminal extradition. The aspirational goal is to deter citizen hackers from attacking the networks of other member nations in violation of the treaty by providing a punishment mechanism.

4. Procedure: Attribution

The single most difficult element of an offense to prove in a cybercrime will always be attribution. Attribution relies heavily on circumstantial evidence, much of which, though scientific, can be called into doubt through the actions of the attackers.[102] The Cyber Treaty must allow for the admission of circumstantial evidence to substantiate attribution, and should set a legal standard of "clear and convincing evidence" to satisfactorily attribute an attack to an individual or group.

---

101. Cyber-attacks that cause civilian death would be an example of something that could not carry immunity.

102. Hackers seek to mask the IP addresses through techniques like hopping. *See* MANDIANT, *supra* note 7, at 39–42 (explaining how hackers can "bounce or 'hop' through intermediary systems such that they almost never connect to a victim network directly from their systems").

The Cyber Treaty drafters will have to work with corporations and intelligence agencies to understand attacks and their consequences. From that point they can move toward assigning obligations and responsibilities, and proscribing actions, to bring about the goals addressed at the outset of this Part.

IV. Conclusion

The concept of linkage in international relations means that statesmen find relationships in different issues to reinforce each other by "creat[ing] a network of incentives and penalties to produce the most favorable outcome."[103] Put more simply, linkage is finding a way to use progress made in one area to build toward progress in an ultimate area.

This Article has taken a successful Cold War theory, triangulation, and applied it to the first link in the diplomatic chain, cyber-attacks. The United States needs to prevent economic losses from cybercrimes for its own economic health, but Russia and China need a strong United States for their own economic health and internal stability. The United States can pursue its national interests—a stronger economy and reduced cyber-attacks—by incentivizing Russia and China to pursue their own national interests in stronger economies. By triangulating the two nations, the United States will move each nation closer to it, producing the desired results. More importantly, the negotiating points to bring about the Cyber Treaty will link the goals of each nation with each other. Knowing that ultimately cyber-attacks are as economically motivated as investment treaties and export contracts, negotiating the Cyber Treaty will allow for progress to wind down the U.S.–China trade war, and may free Russia to expand energy exports in ways that do not involve external regime change.

The current posture of bilateral talks has failed, and the parties are advancing towards economic bellicosity. Cooler heads

---

103. KISSINGER, *supra* note 21, at 717.

must prevail. The successful conclusion of this Cyber Treaty will be the prevailing force.