Strategy Research Project

International Law in Cyberspace Strategies: Formalizing Key Terrain

by

Ms. Alice Y. Goodson
United States Army

Under the Direction of:
Dr. Adrian Wolfberg

United States Army War College
Class of 2016

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*
01-04-2016

2. REPORT TYPE
STRATEGY RESEARCH PROJECT

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
International Law in Cyberspace Strategies: Formalizing Key Terrain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ms. Alice Y. Goodson
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Adrian Wolfberg

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

Please consider submitting to DTIC for worldwide availability? **YES: ☒ or NO: ☐** **(student check one)**

Project Adviser recommends DTIC submission? **YES: ☒ or NO: ☐** **(PA check one)**

13. SUPPLEMENTARY NOTES
Word Count: 6910

14. ABSTRACT

The use of cyberspace capabilities during peacetime by state and non-state actors is having a disruptive effect on the international system and the community has varying views on how to deal with these issues. The lack of technical and legal limitations threaten key cyberspace terrain and offers state actors with the political will and technical capability a way to achieve the strategic advantage against an adversary. Cyber operations conducted against a state's critical infrastructure could lead to misinterpretations that result in conflict escalation from the cyberspace domain to traditional air, land, or sea. This paper recommends the international community collaborate to define international characteristics for key cyberspace terrain; develop standards that ensure states provide timely technical attribution to states accused of cyberwarfare; and create guidelines to verify state intentions in order to increase understanding, promote fairness, and decrease the chances of conflict escalation.

15. SUBJECT TERMS
Cyberwarfare, Critical Infrastructure, Just War Theory, Law of Armed Conflict, Norms, Strategic Effects

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	34	**19b. TELEPHONE NUMBER** *(w/ area code)*

International Law in Cyberspace Strategies: Formalizing Key Terrain

(6910 words)

Abstract

The use of cyberspace capabilities during peacetime by state and non-state actors is having a disruptive effect on the international system and the community has varying views on how to deal with these issues. The lack of technical and legal limitations threaten key cyberspace terrain and offers state actors with the political will and technical capability a way to achieve the strategic advantage against an adversary. Cyber operations conducted against a state's critical infrastructure could lead to misinterpretations that result in conflict escalation from the cyberspace domain to traditional air, land, or sea. This paper recommends the international community collaborate to define international characteristics for key cyberspace terrain; develop standards that ensure states provide timely technical attribution to states accused of cyberwarfare; and create guidelines to verify state intentions in order to increase understanding, promote fairness, and decrease the chances of conflict escalation.

International Law in Cyberspace Strategies: Formalizing Key Terrain

> To talk much and arrive nowhere is the same as climbing a tree to catch a fish.
>
> —Chinese proverb[1]

The introduction of the cyberspace domain has had a disruptive effect on the international system. The use of cyberspace during peacetime is shaping the international political system and the community has varying views on how to deal with these issues.[2] Cyberspace, much like the other warfighting domains, supports both state and non-state actors' activities but the actors' objectives are often significantly different.[3] This paper focuses on international law thus, it excludes the discussion of non-state actor cyberspace activity for two reasons: the international system does not recognize non-state actors and non-state actors do not own critical infrastructure. Any attack against a state's infrastructure that results in conflict escalation would ultimately defer back to the state linked to the attack to seek resolutions.

This paper argues that ability of cyberspace to support a Range of Military Operations (ROMO)—defined as the use of the military instrument of power across defensive, offensive, and stability operations—and avoid detection through stealth capabilities offers state actors with the political will and technical capability a way to achieve the strategic advantage against an adversary.[4] Many states, including the United States, are taking advantage of cyberspace capabilities; however, technical limitations and the lack of norms and laws threaten key cyberspace terrain, critical infrastructure—United States defines as vital assets, systems, and networks whose disruption would debilitate the national security, economy, and public safety.[5]

Technologically advanced countries such as the United States, China, and Russia believe there are minimal concerns that an armed attack between states will occur in or through cyberspace. However, the recent U.S.-China bilateral agreement is a direct result of a state's concern for the strategic use of cyberspace ignored by the current norms and laws that fail to address non-kinetic cyberattacks below the threshold of armed conflict. The absence of non-kinetic warfare—warfare that threatens or destabilizes national security; harm economic interests; create political or cultural instability; or hurt individuals, devices or systems—guidance leaves individual states vulnerable to misinterpretations.[6] These misinterpretations can lead to conflicts that escalate non-kinetic warfare from the cyberspace domain to traditional air, land, or sea kinetic warfare between states. Thus, the international community can no longer afford to ignore the strategic implications of cyberwarfare non-kinetic "effects," or the ambiguity of international norms and laws to address such activity.

In May 2015, to address this gap the UN's Group of Governmental Experts proposed three recommendations to the General Assembly for adoption. The experts agreed that states should avoid intentionally damaging another state's critical infrastructure, avoid intentionally targeting another state's emergency responders, and actively assist other state's investigating cyberattacks and cybercrimes.[7] The success of these peacetime norms will require the international community expand this collaboration to include the following recommendations: (1) define clear international characteristics for key cyberspace terrain; (2) develop standards that ensure states provide timely technical attribution to states accused of cyberwarfare; and (3) create guidelines to verify state intentions. These recommendations will increase understanding, promote fairness, and decrease the chances of misinterpretations that may result in conflict escalation from the cyberspace domain to traditional air, land, or sea.

Cyberspace: Capabilities and Limitations

The ability of cyberspace to support the ROMO and decrease detection through stealth offer states a strategic advantage. Cyberwarfare "is well suited to all phases of operation, from shaping the environment through intense warfare through reconstruction.”[8] While ROMO is not a new concept, formally termed full-spectrum operations, the use of cyberspace changes the way actors conduct these operations. Today, the Department of Defense (DOD) is heavily reliant on cyberwarfare’s ROMO to protect and defend assets that control forces, coordinate fires, gather and distribute intelligence, surveillance, and reconnaissance, and generate knowledge. Cyberspace ROMO increases the likelihood of creating unintended consequences, while its stealth decreases the ability to identify the actor conducting the cyber event. These two factors combine to make it difficult to deter state actors from using cyberspace as a means to achieve national objectives.

Cyberspace operations offer states, with the political will and technical capability, an opportunity to seize control over a military or political situation with a minimal threat of detection. Some scholars and practitioners have posed the argument there is no threat of a “cyber doom” or “Armageddon” given the interconnected economic ties of the international world.[9] In this interconnected world, a cyberattack on one state’s financial system, such as the “global economic states” of U.S. or China, would have disastrous effects on all states.[10] Hence, the situation is not all or nothing, black or white. In fact, many nations are working diligently to create cyberwarfare capabilities that support their own strategic objectives and, while not intended to trigger a global meltdown, the capability can disrupt targeted, localized infrastructure functions. Whether an adversary could indeed limit such intended effects is a key research question.

An adversary's use of a range of military operations to invoke disruptive effects in or through cyberspace represents a credible threat to the security of the U.S. national interests. The United States should pay attention to these threats for two reasons. First, cyberspace operations use dual-use technologies—technologies that have commercial and military applications—to support a broad range of objectives, which creates significant ambiguity in identifying the cyber weapon; and second and perhaps more important, escalation of the intended disruptive effects can transition from the cyber domain into kinetic domains where physical violence affecting human life emerges.

Cyberspace: Capabilities

Cyberspace operations employ cyberspace capabilities for military, intelligence, and ordinary business operations where the primary purpose is to achieve objectives in or through cyberspace.[11] Joint Publication 3-12(R), the military doctrine publication discussing cyberwarfare, underscores three cyber capabilities that combine to support ROMO in cyberspace. First, Operational Preparation of the Environment (OPE) gathers information for intelligence analysis or sets the conditions for future operations; second, Offensive Cyberspace Operations (OCO) seeks to degrade or destroy adversary systems, and third, Defensive Cyberspace Operations (DCO) seeks to protect one's own systems against an attack.[12] The elements of OPE, OCO, and DCO work together against an enemy.

Military plans developed to engage an adversary consist of multiple phases from Phase 0 (shaping), Phase I (deterrence), Phase II (seizing initiative), Phase III (domination), Phase IV (stabilization), and Phase V (enabling civil authority).[13] Exploitation and espionage can occur in every phase of operations because the technology embedded to perform analysis is also capable of malicious behavior if necessary. The preparation of the environment enables offensive cyber while defensive cyber supports the ability to accomplish both exploitation and attack without increased exposure to a counterattack.

Cyberspace: Limitations

Cyberspace operations dual-use technologies limit the ability of states to prevent and detect the malicious activity in the domain. Dual-use technologies offer states an internationally accepted and legal way to maneuver seamlessly between exploitation and attack without major shifts in the technology employed.[14] Many global economic states, such as China, Russia, and the United States, have invested significant resources in the acquisition of these technologies in order to gain and maintain a strategic advantage.[15] Dual-use technologies in cyberspace pose a significant dilemma for lawmakers' because cyberspace operations that serve traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, are an accepted norm under international law.[16] Multiple states possess the destructive capability to conduct cyberwarfare against another state's critical infrastructure using these technologies but the peaceful uses of the technologies make it unrealistic to prohibit them within the global network.

The North Atlantic Treaty Organization (NATO)—an intergovernmental military alliance based on the North Atlantic Treaty—threshold for cyberwar requires effects similar to conventional attacks (e.g., physical destruction) to establish intent, but the lines for cyberwar are blurry. The problem is the NATO threshold does not consider the effects of terrorism, crime, and espionage. Powerful states in the international community are acknowledging the benefits of cyberspace and are taking advantage of all that the domain has to offer. For example, Russia's Ministry of Defense is establishing its own cyber command, which according to senior Russian military officials, will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and controls systems.[17] In addition, China's military strategists describe cyber capabilities as a powerful asymmetric opportunity in a deterrence strategy, while the state’s authoritative writings on cyberwarfare discuss the capability as an instrument for balancing overwhelming power during a conflict.[18] Cyberspace operations provide a versatile method to strategically engage the enemy and win without physical destruction.

Cyberspace Critical Infrastructure

States are taking full advantage of the characteristics of cyberspace as a force multiplier to gain the strategic advantage. Cyberattacks could disrupt, destroy, or exploit major financial centers or critical infrastructure (e.g., power generators; air traffic control systems). For example, in 2007, Estonia’s attempt to remove a Soviet-era grave marker resulted in a Russian cyberattack, which disrupted Estonian parliament, banks, ministries, newspapers, and broadcasters, paralyzing the country’s IT infrastructure over the dispute.[19] In late 2009, Iran accused the United States and Israel of conducting a cyberattack against Iranian centrifuges that resulted in the physical destruction of Iranian nuclear reactors.[20] Then, as recent as May 2015, a grand jury in the Western District of Pennsylvania indicted five members of the Chinese military on charges of economic espionage for hacking into critical private sector data supporting U.S. solar products, nuclear power, and the metals industry.[21] Despite the inherent risk of cyberattacks against critical assets, states continue to exploit the benefits (e.g., military or economic cyberespionage) that accompany the globally interconnected environment, which have become a necessary condition of conducting international business. At the strategic level, the implications of cyberwarfare are vast.

U.S. Exploitation

In 2009, U.S. national security officials reported successful penetrations of its critical infrastructure dating as far back as 2006. The report revealed the successful exploitation of the U.S. electrical grid by multiple countries to include China, Russia, and others that left behind software capable of disrupting the system during a crisis or war.[22] Soon after the report, President Obama made a speech expressing his concerns, "… we know that cyber intruders have probed our electrical grid and that in other countries cyberattacks have plunged entire cities into darkness."[23] The exploitation across the U.S. critical infrastructure could facilitate a cyber attacker's ability to take control of electrical facilities, nuclear power plants, or financial networks granting the perpetrator a strategic, operational, or even tactical advantage during a crisis or conflict.

In response to the Pentagon's concerns about the hack, Congress proposed the Protecting Cyberspace as a National Asset Act of 2010, granting the President the authority to declare a national cyber emergency for critical infrastructure experiencing an ongoing or imminent threat by any individual or entity attempting to disrupt the reliable operation of covered critical infrastructure.[24] The President's controversial "kill switch" authority allowing the shutdown of commercial and government infrastructure in the event of an emergency was later removed, but the mere knowledge that Congress considered such a mechanism further supports the administration's exasperation about how to handle an attack by an adversary in or through cyberspace.[25]

Strategic Issues

There are two offensive issues to consider as well: a counter-response could lead to conflict escalation; and, the risk of engaging an adversary with a cyber advantage is much more complex than with kinetic weapons. Deputy Assistant Secretary of Defense for Cyber Policy, Aaron Hughes, issued specific guidance to U.S. private companies to avoid taking matters into their own hands, even to disrupt the theft of data. Per Hughes, hacking back may result in a misunderstanding by a foreign government and escalate the event from cyberespionage to a cyberattack making coordination for an appropriate response more difficult for the government.[26] In addition, the use of cyberspace, during phase 0 operations, becomes a game changer in risk management. The risk calculus, considering a U.S. intervention strategy into a Chinese-initiated conflict with Taiwan, can be quite complicated given the knowledge that China could potentially shut down key portions of the U.S. electrical grid whenever it desired.

So, if states remain undeterred and cyberespionage is an accepted practice, what would happen if state-on-state cyber operations resulted in an escalation to a kinetic air, land, and sea war? The United Nations (UN), the international organization responsible for development of international law, has engaged the international community to establish acceptable state behaviors based on customs, standards, or treaties; norms, state rights and obligations. The UN must develop regulations, or agreements that govern state relationships, and laws, that direct the use of cyberspace in order to reduce the chances of global disruption and answer the latter question.[27]

International Cyberspace

A cursory inquiry into cyber international law can lead to various perspectives. The international community agrees that while the domain is new, cyberspace is not a law-free zone or the “wild-wild west,” but there continues to be discourse about the ability of the existing laws and norms to adapt to the variety of effects the new domain introduces.[28] The Tallinn Manual on the International Law Applicable to Cyber Warfare, published in 2013, is a study on how the international law applies to the cyber domain.[29] There are also existing UN Charter laws and war theories interpreted by some states, for example the United States, as applicable to the new domain but each has its limitations.[30]

Tallinn Manual Limitations

The Tallinn Manual documents the results of a three-year non-binding academic study, conducted by an independent International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), located in Tallinn, Estonia, that examines how existing international legal norms, specifically *jus ad bellum*—the norms for justifying going to war—can apply to cyberwarfare.[31] The Manual only addresses prohibitions linked to armed conflict, and ignore cyber activities that occur below the defined use of force level—a cyberspace operation that constitutes a threat against territorial integrity or political independence of a state.[32] In addition, while the Tallinn Manual can indeed serve as a basis to establish norms, what the Tallinn Manual cannot do is serve as a law that requires international members to observe these norms. Thus, states are seeking to formalize the use of cyberspace with the existing UN Charter Articles and war theories.

UN Charter Limitations

Two particular UN Charter Articles present significant challenges to clarifying the use of cyberspace operations. First, Article 2(4) of UN Charter, which “prohibits the threat or use of force and calls on all Members to respect the sovereignty, territorial integrity, and political independence of other States," may require further clarification on the "use of force" in cyberspace. Article 2(4) focuses on direct physical injury and property damage, comparative to kinetic attacks, e.g. triggering a nuclear plant meltdown. Therefore, what happens if the results of a cyberattack are only for political purposes, and do not result in death, injury, or significant damage to property? For example, a state actor manipulates the upcoming U.S. election data to ensure a presidential candidate wins the 2016 elections to benefit the adversary's strategic goals. How should the United States respond? Can the United States respond? Second, UN Charter Article 51 affords each state the inherent right of individual or collective self-defense in response to an armed attack. However, what constitutes an armed attack in cyberspace? If the requirements of Article 51 are deferred back to Article 2(4) then a new lexicon is still required to define the more strategic effects that cyberspace offers. What is the appropriate response to the manipulation of data that misleads a State's diplomatic decision-making process?

Jus in Bello Limitations

Finally, and most problematic, are the issues of *jus in bello*—the norms for the conduct of war. *Jus in bello* is one of three just war theory concepts: *jus ad bellum*, *jus in bello* and *jus post bellum*.[33] While *jus ad* bellum, and *jus post bellum*—the norms for justice after war—may also pose issues in cyberspace, it is *jus in bello's* two principles—distinction and proportionality—that will face significant difficulties ensuring compliance in the new domain. The *jus in bello* principle of distinction requires state actors to establish military objectives that contribute to military actions whose targeted destruction would offer a military advantage.[34] *Jus in bello* generally protects civilian assets and herein lies the problem with cyberspace, the practical implications of dual-use technology. The civilian private sector owns most of the cyberspace critical infrastructure utilized by the military, making it nearly impossible to comply with the principle of distinction. So now, what constitutes a military target? For example, if the Army's Command and Control (C2) systems use the DOD's Global Information Grid (GIG), which operates via AT&T commercial leased telecommunications lines and Amazon's federally approved cloud-computing infrastructure, does an attack on the Army's C2 violate the *jus in bello* principle of distinction*?*

Complying with the *jus in bello* principle of proportionality, which prohibits attacks that may result in the incidental loss of civilian life, injury to civilians, or damage to civilian assets that would be excessive in retaliation to the concrete and direct military advantage anticipated by the action may also prove extremely difficult.[35] Proportionality requires states assess the potential harm to civilians prior to action and weigh the risk of collateral damage. In this globally interconnected world of shared infrastructures, this is an unrealistic expectation for two reasons. First, the lengthy reconnaissance required to map the entire network connectivity for an adversary is impractical. An attempt to comply with the principle of proportionality could severely degrade one of the greatest advantages of cyberwarfare, the swift no-warning attack.[36] Second, and perhaps more important, the uncertainty of knowing when, where and how the non-kinetic effects of cyberspace transition into the kinetic domain causing physical destruction and a threat to loss of life. For example, what if China's software code experiences an error or becomes corrupt and inadvertently shuts down portions of the U.S. electrical grid resulting in significant property damage or loss of life? How should the United States respond? A miscalculation by the United States of China’s intentions could result in crisis escalation.

Laws in Cyberspace

The lack of international consensus on accepted and enforceable laws, regulations, or norms of behavior specifically derived for cyberspace has left state actors undeterred from conducting cyberespionage or perpetrating cyberattacks. Not surprising, the permissive environment seems to encourage state actors to test their adversaries’ technical capabilities, political resolve, and thresholds with coercive low-level attacks short of war, with a relatively low risk of retaliation.[37] The distinct differences in states cyberspace values, customs, and standards, the inability of existing international laws to meet the needs of cyberspace, and the lack of common definitions and terms make it difficult to reach international consensus to support norms and laws in cyberspace.

Navigating Cyberspace

First, international norms require common values, customs, globally accepted standards, or an established treaty, a formally concluded and ratified agreement between countries, and some international cyber powers have different, and radically incompatible, values over how to protect cyberspace. States are legislating cyberspace within their sovereign territory based on state values, customs, and standards resulting in uneven enforcement, uncertainty, and fear in some cases for civil society.[38] Both democratic and authoritarian states have sought innovative technology and internal laws, policies, and regulations to address the issues introduced by cyberspace. But, authoritarian states have moved more aggressively to implement offensive techniques targeted against state citizens as a form of internal social control, and there are no norms or laws to prevent such behaviors.[39]

Next, global treaties are literally impossible to establish if states disagree on the definition of security. As mentioned above, UN Article 2(4), Article 51, and *jus bello* principles expose some structural limitations of the existing international laws and norms to support cyberspace security issues—effects unlike those in traditional warfare that result in physical destruction, loss of life, etc. Espionage is an accepted practice yet the United States found China's alleged economic cyberespionage pressing enough to create a unique agreement with them to decrease the negative effects of the cyberwarfare actions. The absence of an international cyber governance mechanism or common cyberspace norms make it difficult to respond to large-scale cyberattacks, such as China's 2015 theft of an estimated 100 million American Personally Identifiable Information (PII) profiles from government owned, contractor operated databases.[40] How many of these unique circumstances may arise? How many bilateral agreements may be necessary?

Finally, cyberspace raises far more questions than answers in the international community. What is a cyber weapon, given that dual-use technology—for example, one piece of software code—can support peace and war activities? How can technology be controlled, yet the internet remain free and open for every state? Even more important, what is the difference between cyberwarfare and cyberespionage? Per NATO, cyberespionage is inherent part of the ROMO in support of cyberwarfare, which makes them one in the same. Assistant Security of Defense for Cyber Policy, Aaron Hughes uses the term "squishy" to sum up the difficulty in delineating between the two.[41] The

United States admits to a struggle defining a cyberattack and its threshold; therefore, the Pentagon evaluates each event individually.[42] Given the latter issues, a more formalized norms and laws for cyberspace under the purview of the UN is a more prudent approach to create stability within international cyberspace.

Cyberspace Bilateral Agreements

Global powers have attempted to establish cyberspace bilateral agreements (e.g., Russia-U.S., Russia-China, and U.S.-China) in hopes that these pacts would decrease the threat of cyberwarfare and increase the cooperation between the nations, but maintaining these relationships has been complicated to say the least. In 2014, the United States froze the 2013 Russia-U.S cyberspace pact dialogue in response to Russian cyberattacks on Crimea and the Ukraine.[43] Apparently, the United States found Russia's use of cyber against Ukraine a violation of cyberspace norms and laws. The follow-on discussion of the U.S.-China bilateral agreement serves as a more recent example of two countries attempting to compensate for the limitations of existing international laws and norms for cyberspace with little consideration for the formal processes required to validate compliance.

U.S.-China Agreement

In September 2015, a visit from China's President Xi Jinping, in response to the exfiltration of millions of U.S. government employees' data, ended with rumors that the United States and China entered into the first cyberspace arms control accord treaty.[44] Immediately after that news report, the Department of State's Coordinator for Cyberspace Issues, Chris Painter, revealed that the report was an error. According to Mr. Painter, the United States did not and will not enter into a cyberspace treaty because; "I do not know what a cyberarm is."[45] The development of an arms control treaty requires a clear understanding of the weapons under control and UN engagement, so instead, the United States and China settled on a bilateral agreement that requires the states to discontinue the use of cyberespionage to support the theft of intellectual property. The agreement seems counter intuitive since industrial espionage, also coined economic espionage, has been a common government practice throughout history.[46]

United States analysts suspected that China would not honor the agreement since the state's official position is to deny carrying out espionage, and they were correct."[47] By December 2015, China re-categorized the incident as a criminal case instead of state-sponsored cyberespionage and there is no established process to determine otherwise.[48] Further, China's misinterpretation of U.S. Phase 0 operations, preparation of the environment, could lead to accusations that violate the bilateral treaty, but the international system has no formal jurisdiction over the dispute. So although well intended, the cyberspace bilateral agreement provides no mechanism to verify a State's objectives, no standard test criteria for attribution, and may simply restrict the U.S. ability to meet national interest and weaken the international system on matters in cyberspace.

National Security Objectives

The assumptions of the bilateral agreement rest on the ability of the states to separate private economic espionage from national security objectives. The U.S. complaint against China assumes that the economic espionage in question has no national security implications at all, but what if that is not the case. China's exploitation of solar product, nuclear power, metal industry, and federal personnel clearance data might support China's national security objectives. China's national cybersecurity strategy includes, “maintaining economic growth and stability, which involves industrial economic cyber espionage of U.S. and other foreign targets.”[49] Who has the last word on whether cyberespionage supports economic or national security goals? The mutually beneficial agreement seeks to solve a complex cyberwarfare issue, stop the use of cyberespionage to support the theft of intellectual property, but whether or not the states fully comply with the terms will depend on the state’s national objectives. After all, there are no international laws or norms in place to validate compliance or enforce penalties for this type of agreement. It is simply two states trying to resolve an international issue amongst them.

Attribution Testing

An analysis of China’ s national interest, national investments, and cyber doctrine supports a strong argument that the advantages of conducting cyberespionage far outweigh the disadvantages, which can make the state unwilling to restrict or give up its use in the U.S. private sector.[50] Included with the advantages are three characteristics of cyberwarfare that decrease the risk of escalation by the United States. First, a high percentage of the U.S. critical infrastructure and information resides in the realm of dual-use technologies owned and operated by the private sector, which blurs the lines between economic and military espionage and increases the odds to establish deniability.[51] Second, in cyberwarfare, espionage or OPE, is an accepted practice and a precursor to offensive operations; OCO is far more difficult to perform without conducting OPE first. Espionage is business as usual for state governments. Third, and most problematic to solve, is technical attribution—the ability to causally link a state government to espionage. Open source reporting suggests that the Chinese government maintains existing relationships with civilian freelance operators (elite hackers) and elicit their services at times.[52] Cyber proxies**,** private computer hacking experts, provide states the flexibility to deny any wrongdoing if the theft is detected. If the private sector shares the target infrastructure, espionage is an accepted practice, and the probability of detection is low, why should China deny themselves the strategic advantage?

Weakening the U.S. and the International System

The September 2015 U.S.-China bilateral agreement is unlikely to eliminate China's economic espionage activities, but it may restrict the United States ability to collect vital information in support of U.S. national interest and weaken the international system. The United States is pursuing dual paths to maintain a cooperative relationship with China. When U.S.-China interests converge, Washington works to expand their cooperation with Beijing and, when interests diverge, and China's actions result in a cost to the United States, Washington works to counter and deter those actions.[53] China also views a peaceful and cooperative relationship with the United States an important part of their foreign policy.[54] The intertwined economies create unique tensions when the United States and China's interest diverge because both sides must take actions to decrease the risk of conflict. The United States and China's willingness to enter into a bilateral agreement is simply an attempt to reduce the tensions between the states.

After the Edward Snowden intelligence leaks, the international community is demanding the United States practice what it preaches by adhering to international agreements and norms. China responded to the United States accusations of Chinese cyberespionage by calling Washington leadership hypocrites.[55] In response, President Obama has committed the United States to lead by example. The U.S.'s International Strategy for Cyberspace specifically calls for the United States to "….build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace" and the United States must work hard to ensure compliance with these guidelines in order to rebuild the trust of the international community.[56] The United States will work to fulfill its promise but the inherent assumptions behind the U.S.-China bilateral agreement will make compliance difficult.

In an effort to maintain a cooperative relationship with China, the United States is ignoring its own national security strategy to strengthen the multilateral institutions within international system—such as the United Nations, International Monetary Fund, World Bank, and World Health Organization. The Obama administration acknowledges that, as global powers, the United States and China must work together, but it must be through the international system to confront transnational threats.[57] That being said, why would China sign a cyber bilateral agreement with the United States? China may be seeking to devalue the UN, a multipolar international system of great powers and weak powers, in favor of a U.S.-China bipolar system of peers.

China's place in the multipolar international system is fraught with a destructive and hurtful history. Historically, the Chinese experience with western powers was one of inferiority. China never took part in the creation of the international system others now expect them to abide by.[58] Some view China as simply putting up with the existing system, created without their input, in order to gain or retain the benefits that come from membership.[59] Since 1978, when China began its modernization plans, the principle objective of the grand strategy has been to attain "comprehensive national power" in order to return to greatness.[60] China's cooperation with the international community buys them time to attain the necessary goals to accomplish their national interest. For example, as a strong trade partner with the United States China has benefited significantly with minimal compromise, hence the path towards a peer relationship with the United States.

The problem is cyberwarfare is not an issue limited to the U.S.-China relationship, and as such, neither the United States nor China can solve such a systemic problem without engaging the international community. At the end of the 2015 bilateral agreement, the only assured winner was China, who avoided sanctions for cyberespionage against the U.S. commercial sector.[61] The United States attempt to cooperate with, yet constrain China from conducting government-sponsored economic espionage through a bilateral agreement is unmanageable without the support of the international system. There is strength in numbers. Every developing and developed state interconnected in the global economy is subject to the threat of cyberwarfare. Multiple states are concerned about state sponsored cyberwarfare, particularly from China, and a bilateral agreement can set a precedence for independent negotiations vice international engagement to resolve cyberspace issues.[62]

As the debate about the necessity of cyber laws or norms continues, each bilateral agreement outside of UN purview may decrease the need and the desire of the international community to come together to create standards that are acceptable, and define violations that are punishable. While permanent United Nations Security Council members, which includes China and Russia, can veto UN efforts to create international laws and norms of behavior for cyberspace, the larger international community may question the countries sincerity to work within the international system and their desire to do what is best for the entire community. The other, more important point to understand from this discussion is the fact that none of the bilateral agreements focus on armed attacks. There is far more language about interfering in a state's internal affairs, economic damage, data breaches, and dissemination of information that threatens political and socio-economic systems, or spiritual, moral, and cultural aspects of a state's environment. So, why is the international community primarily focused on the applicability of just war theories and armed conflict? The UN must guide the international community to answer the more relevant questions about the use of cyberspace such as those contained in the language of bilateral agreements. How can the international community formally address the risks of unintended consequences and conflict escalation introduced by the ROMO in and through cyberspace?

Recommendation

The exploitative, offensive, and defensive characteristics of the ROMO leaves states vulnerable to unintended consequences and misinterpretations that arise from the ambiguities of cyberspace operations that may lead to conflict escalation. To decrease the risks of escalation the UN should implement three recommendations. First, develop an international classification system for critical infrastructure that creates a common language for the international community to define key terrain and promote a greater understanding of the strategic effects of cyberspace operations. Next, establish international standards for technical attribution and limit investigation timelines to promote feelings of fairness throughout the international community. Finally, establish international guidelines to assess the operational intentions of states performing the ROMO to decrease the chances of misinterpretations of unintended consequences that may result in conflict escalation.

International Critical Infrastructure Classification

A key shortfall of international cyberspace is the absence of understanding through accepted definitions for key terms. For example, the definitions of critical infrastructure are different in Russia, China, and the United States making it difficult to understand the potential effects of ROMO against individual states infrastructure.[63] There are three key tasks to increase international understanding and decrease the risks of unintended consequences for state's critical infrastructure. The international community must collaborate to identify and document (1) key characteristics of critical infrastructure sectors, (2) standard severity levels to meet *jus in bello* principles of proportionality, and (3) who and what are the potential effects of an attack to observe *jus in bello* principle of distinction. First, documented rules of behavior are typically the basis for punishment; then, it follows that states should have a fair understanding of punishable behaviors. Should something go dramatically wrong during Phase 0 operations, combatants must understand the implications and be prepared to face the scrutiny of the international community for its role in the event. The international community must embrace the difficult task of collaborating to attain consensus on the key characteristics for cyberspace critical infrastructure. The development of an international classification system will provide standardized characteristics of key cyberspace terrain for every nation, making it far more difficult to establish plausible deniability should unintended consequence result in an "armed attack" against a state.

Second, *jus in bello* requires states to consider the proportionality, objectives that avoid loss of life, injury to civilian, and damage to civilian assets. A state's ability to meet the objectives of proportionality requires an understanding of the severity level and the effect of an attack created from intended or unintended consequences. Severity classifications should depict the impact of a cyberattack to the international and national community. For example, the degradation of assets directly linked to the loss of life or injuries to civilians are *vital* (V) and adversaries should avoid targeting these assets even during Phase 0, exploitation operations. Infrastructure attacks that result in the damage of civilian assets that affect international order or the global economy are *critical* (C), adversaries may be unable to avoid Phase 0 operations to support military objectives, but should proceed with caution with the understanding that an inadvertent attack could affect the international community. Infrastructure attacks that result in the disruption of assets that support essential functions at the national level are *important* (I); adversaries targeting these sectors should understand that attack may result in second and third order effects to sectors classified as vital or critical.

Third, *jus in* bello, principle of distinction requires states target military objectives that avoid civilian assets. To meet this objective the international community must have an understanding of who (e.g., international (I) or national (N) community) and what (e.g., military (M), government (G), or commercial (C) infrastructure) is affected by an attack. Shared infrastructure and dual-use technologies complicate the ROMO but the collaborative creation of an international critical infrastructure classification system will promote a greater understanding of the strategic effects of cyberspace operations (see Table 1).

Table 1. Example of International Critical Infrastructure Classifications

Sector	Characteristics	Severity	Effect	Infrastructure
Financial	Deposit funds and make payments; Provide credit and liquidity to customers; Invest funds for long and short periods; Transfer financial risks.	V	I, N	G, C

Defense Industrial Base (DIB)	Research and development;
	Design, production, delivery;
	System maintenance
		C	I, N	M, G, C

Emergency	Save lives; Protect property and the environment; Assist in community disasters; and Aid in recovery from emergencies	V	N	G, C
Manufacturing	Essential to other sectors	I	N	C

Note: Severity codes: (V) Vital linked to the loss of life or injuries to civilians, (C) Critical linked to international order or the global economy, and (I) Important linked to essential functions at the national level. Effect codes: (N) National and (I) International. Infrastructure codes: (M) Military, (G) Government, and (C) Commercial. Notional table based solely on U.S. Department of Homeland Security sector characteristics. International Critical Infrastructure Classifications should represent consensus among states.

Technical Attribution Standards

Next, are the questions of “who did it,” “how can we prove it,” and “how long does it take?” Technical attribution is not a new topic of discussion for cyberspace. States, including the United States, continue to explore technologies that can accurately attribute attacks to actors and enhance stealth capabilities to decrease detection during operations. There is no debate within the cyberspace community that actor attribution, who is responsible for a hostile cyber act, and act attribution, the relative severity of the act, are critical factors to determine the proper response.[64] What is new is the context in which this paper argues for standardized testing thresholds to support accusations of non-kinetic attack. An armed attack, covered by the Law of Armed Conflict, results in physical damage that; often supports, the forensics of the offline system to find technical traces of the attacker and their method. The problem is what if they system is not destroyed and the full forensics cannot be performed or it takes a lengthy amount of time to perform the test. Two questions require input from the international community: (1) what is the acceptable level of testing, burden of proof; and (2) how long is too long, or the statute of limitations, before a response to a cyberattack that did not result in destruction or loss of life is no longer actionable.

If the accusing state cannot provide evidence at the approved standard within a specified amount of time, it seems reasonable to draw a line that allows the accused to find a since of relief. For example, the United States grants a 7-year statute of limitation to individuals accused of "significant fraud of $1 million or more involving the U.S. government.[65] Despite the harm caused by the various types of cyberattacks, it is reasonable to limit a state's ability to seek retribution for unproven accusations after a reasonable amount of time. Today, these questions are not under consideration in the international community, but as cyberspace moves closer to a tool used to meet strategic objectives, the international community should consider the questions just as important to the security of cyberspace.

A Case for Operational Intent

Finally, it is impossible to ensure that Phase 0 operations, exploitation, will not result in Phase III operations, domination or offensive, due to software errors. The UN

Charter Article 51 affords each state, in response to an armed attack, the right of individual or collective self-defense. But, what if the attack was unintended? As a precaution, the international community should collaborate to establish guidelines to evaluate actor intent to decrease the chances of misinterpreting the actor's intentions and increase the likelihood that states will receive appropriate punishment for purposely attacking vital or critical infrastructure. State's response to a cyberattack must consider variables beyond the end state, the destruction of critical infrastructure. This recommendation correlates with the recommendation for technical attribution. States must be able to establish technical attribution prior to accusations that demand the intentions of the state actor. Realistically, no state would admit to cyberwarfare operations against a member state without substantial proof to support the accusation.

The use of dual-use technologies to conduct the ROMO in cyberspace is an important part of national security; therefore, the international community should expand their evaluation criteria to include inadvertent technical errors that may result in physical destruction or loss of life. This recommendation will face the scrutiny of states that lack trust amongst their international partners, but it could literally prove to be a lifesaver if a conflict is prevented after the internationally community comes together to assess the of state's operational intentions that resulted in the attack. After all, software errors are common and mistakes could happen to any state participating in ROMO in cyberspace.

Conclusion

States in the international community are utilizing the unique characteristics of cyberspace operations to achieve national objectives. Despite fifteen years of discourse, there remains disagreement on how the current international norms and laws apply in cyberspace. Of even greater concern should be the fact that the Law of Armed

Conflict and just war theories only support “armed attacks” or war activities and disregards the more popular gray area introduced by cyberspace’s strategic effects, such as the exfiltration of terabytes of U.S. citizens data. Cyberspace ROMO extend beyond the operational and tactical levels of conflict to allow states to gain a strategic advantage during the earlier phases of operations, but it also introduces the risks of misinterpretations and unintended consequences that may result in conflict escalation. To decrease the risks of escalation the UN should guide the international community to implement three recommendations. First, develop an international classification system for critical infrastructure that defines the characteristics, categorizes the severity level and effects, and identifies shared infrastructure sectors. Next, establish international standards for proof and prescribe time limits for legal action for cyberattacks below the level of “armed attack.” Finally, establish international guidelines that assess an actor’s operational intentions to decrease the chances of misinterpreting the act and increase the likelihood that states will receive the appropriate punishment for malicious behavior.

Endnotes

[1] Thinkexist.com, “Chinese Proverbs Quotes,” http://thinkexist.com/quotation/to_talk_much_and_arrive_nowhere_is_the_same_as/197226.html (accessed March 21, 2016).

[2] Andrea L. Limbago, "One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft," *Joint Forces Quarterly* 78 (2015): 84.

[3] Mark Pomerleau, "State vs. Non-state Hackers: Different Tactics, Equal Threat?” August 17, 2015, https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers-tactics.aspx (accessed March 10, 2016).

[4] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Chiefs of Staff, March 25, 2013), I-14.

[5] U.S. Department of Homeland Security, "What Is Critical Infrastructure?" January 8, 2016, https://www.dhs.gov/what-critical-infrastructure (accessed March 10, 2016).

[6] Michael Schmitt, "Armed Attacks in Cyberspace: A Reply to Admiral Stavridis," *Lawfare,* blog posted January 8, 2015, https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis (accessed February 24, 2016).

[7] Joseph Marks, "U.N. Body Agrees to U.S. Norms in Cyberspace," *POLITICO*, July 9, 2015, http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900 (accessed March 8, 2016).

[8] Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79 (2015): 49.

[9] Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable," *Strategic Studies Quarterly* 9, no. 2 (2015): 91; James R. Clapper, *Worldwide Threat Assessment of the Us Intelligence Community* (Washington, DC: U.S. Department of National Intelligence, 2015), 1; Ron Deibert, "Cyberspace under Seige," *Journal of Democracy* 26, no. 3 (July 2015): 71. Mazanec discusses one of the leading German academics, Thomas Rid, in his popular book *Cyber War Will Not Take Place*. In the December 2013 edition of *Foreign Affairs*, Rid argued that not only is cyberattack not a major threat but that it will in fact "diminish rather than accentuate political violence" by offering states and other actors a new mechanism to engage in aggression below the threshold of war. Erik Gartzke also argues that cyberwarfare is undergoing artificially hyped cyber threats of cyber doom in an effort to generate business but it is unlikely to prove as pivotal in world affairs as many observers seem to believe. The U.S. Intelligence community assesses that although the networks remain vulnerable to espionage and/or disruption the likelihood of a catastrophic attack from any particular actor is remote at this time.

[10] Global Economy defines countries intertwined by worldwide economic activity and thus can affect other countries negatively or positively. Businessdictionary.com, “Global Economy,” http://www.businessdictionary.com/definition /global-economy.html#ixzz3uQc5Yiub (accessed February 24, 2016).

[11] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 15; U.S. Joint Chiefs of Staff, *Cyber Operations*, Joint Publication 3-12 (Washington, DC: U.S. Chiefs of Staff, February 5, 2013), I-1; Stephen W. Preston, *Department of Defense Law of War Manual* (Washington, DC: U.S. Department of Defense, 2015), 995.

[12] U.S. Joint Chiefs of Staff, *Cyber Operations*, II-1.

[13] U.S. Joint Chiefs of Staff, *Joint Operations Planning*, Joint Publication 5-0 (Washington, DC: U.S. Chiefs of Staff, August 11, 2011), III-42.

[14] Deibert, "Cyberspace under Seige," 64; Barack Obama, “Remarks by the President on Securing Our Nation’s Cyber Infrastructure,”public speech, White House: Washington, DC*,* March 2009. Deibert suggest that the same technologies that many praise as the tools of freedom can also enable the control of society. In a 2009 speech, President Obama states, “the very technologies that empower us to create and to build also empower those who would disrupt and destroy.” Dual-use technologies are commercial/civil technologies with the potential for military or weapons applications (http://www.state.gov/strategictrade /resources/controllist/).

[15] Ash Carter, *The DOD Cyber Strategy* (Washington, DC: U.S. Department of Defense, 2015), 9.

[16] Stephen W. Preston, *Department of Defense Law of War Manual* (Washinton, DC: U.S. Department of Defense, 2015), 999.

[17] Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, 2.

[18] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (2011): 6.

[19] Ibid., 9.

[20] Mazanec, "Why International Order in Cyberspace Is Not Inevitable," 81; Andrea L. Limbago, "One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft," 90.

[21] David Geer, "Hackers inside Chinese Military Steal U.S. Corporate Trade Secrets," *CSO Online,* July 22, 2014, http://www.csoonline.com/article/2456610/data-protection/hackers-inside-chinese-military-steal-u-s-corporate-trade-secrets.html (accessed December 3, 2015).

[22] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal Online,* April 8, 2009, 1, http://www.wsj.com/articles/SB123914805204099085 (accessed December 5, 2015).

[23] Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure."

[24] Gorman, "Electricity Grid in U.S. Penetrated by Spies," 3; *Protecting Cyberspace as a National Asset Act of 2010,* Public Law, 111th Cong. (2009-2010), https://www.congress.gov/bill/111th-congress/senate-bill/3480 (accessed February 13, 2016).

[25] Gautham Nagesh, "Emergency Powers for President Dropped from Cybersecurity Bill," *TheHill*, February 14, 2012, http://thehill.com/policy/technology/210601-senate-cybersecurity-bill-drops-emergency-powers-for-president (accessed February 13, 2016).

[26] Anna Mulrine, "State Department Cyber Coordinator: We Don't Want a Cyberarms Treaty," *The Christian Science Monitor,* 2015, 2.

[27] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* 19.

[28] Koh, "International Law in Cyberspace," 1.

[29] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 4.

[30] Oleg V. Demidov, "Russia-China-United States: Setting the Global Rules of the Game in Cyberspace," September 29, 2015, 3, http://www.pircenter.org/media/content/files/13/14446 574000.pdf (accessed February 14, 2015).

[31] The NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) is an international military organization accredited in 2008 by NATO's North Atlantic Council as a "Centre of Excellence." Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands,

Poland, Slovakia, Spain, and the USA serve as sponsoring nations. The NATO CCD COE's mission is to enhance capability, cooperation, and information sharing between NATO, NATO Member States, and NATO's partner countries in the area of cyber defense by virtue of research, education, and consultation. The center is not part of NATO's command or force structure and there are no repercussions should a state chose to ignore the recommendations.

[32] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 4.

[33] Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," *Leading Issues in Information Warfare & Security Research* 1 (2011): 2. The just war theory is derived from the writings of Augustine, Aquinas, Grotius, Suarez, Vattel, Grotius and Waltzer and offers a framework for the ethics of war and peace. Just war theories attempt to add rules for the use of arms and answer complex questions such as when is it right to go to war, and how should war be conducted.

[34] Koh, "International Law in Cyberspace," 1-2.

[35] Ibid., 2.

[36] Martin C. Libicki, “Crisis and Escalation in Cyberspace,” in *Project Air Force* (Santa Monica, CA: RAND Corporation, 2012), 148.

[37] Clapper, *Worldwide Threat Assessment of the Us Intelligence Community*, 2.

[38] Deibert, "Cyberspace under Seige," 68.

[39] Ibid., 65.

[40] Melanie Hart, "Assessing American Foreign Policy toward China," *Center for American Progress*, 2015, 5.

[41] Mulrine, "State Department Cyber Coordinator: We Don't Want a Cyberarms Treaty," 1.

[42] Ibid., 2; Hart, "Assessing American Foreign Policy toward China," 6.

[43] Demidov, "Russia-China-United States: Setting the Global Rules of the Game in Cyberspace," 5.

[44] David E. Sanger, *U.S. And China Seek Arms Deal for Cyberspace* (New York: New York Times Company, 2015), 1.

[45] Mulrine, "State Department Cyber Coordinator: We Don't Want a Cyberarms Treaty," 1; Preston, *Department of Defense Law of War Manual*, 1003. There is no international consensus regarding the definition of a "cyber weapon." Most of the technology used is inherently dual-use, and even software can support for malicious actions.

[46] Geer, "Hackers inside Chinese Military Steal U.S. Corporate Trade Secrets." 2; Merriam-Webster online dictionary defines *espionage* as “the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company <industrial espionage>.” The history of espionage includes the theft of intellectual

property and the industrial community accepts the practice. The bilateral agreement, if adhered, limits the ability of China and the U.S. to utilize the practice to support national interests (http://www.merriam-webster.com/dictionary/espionage). The Federal Bureau of Investigations Economic Espionage Act of 1996 (EEA), 18 U.S.C. §§ 1831-1839 recoined and redefined the term “industrial espionage” to address the expansion of the practice to include more than defense-related and high-tech industries (https://www.fbi.gov/about-us/investigate/ counterintelligence/economic-espionage).

[47] Mulrine, "State Department Cyber Coordinator: We Don't Want a Cyberarms Treaty," 1; Gorman, "Electricity Grid in U.S. Penetrated by Spies," 2. A Chinese Embassy, said the Chinese government "resolutely opposes any crime, including hacking, that destroys the Internet or computer network and has laws barring the practice. China claims to be a part of the solution for cybercrime not the problem.

[48] Andrea Chen. “Positive Outcome in Cyber Talks with U.S: Public Security Chief Guo Shengkun and US Counterpart Jeh Johnson Reach Basic Deal on How to Handle Hacking and Theft Disputes,” *South China Morning Post*, 2015.

[49] Amy Chang, "Warring State: China’s Cybersecurity Strategy," *Center for New American Security*, December 2014, 8.

[50] Mazanec, "Why International Order in Cyberspace Is Not Inevitable," 85-86; Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," *International Journal of Computer Research* 21, no. 4 (2014): 15. Chinese doctrine and strategic writings emphasize the importance of seizing information dominance before or at the onset of hostilities and exploiting the use of IW tools for their potential deterrent effect.

[51] Obama, "Remarks by the President on Securing Our Nation’s Cyber Infrastructure"; Barack Obama, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, DC: The White House, 2013).

[52] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 21.

[53] Hart, "Assessing American Foreign Policy toward China," 6-7.

[54] Ibid., 2.

[55] David E. Sanger, "U.S. and China Seek Arms Deal for Cyberspace," *New York Times Online,* September 19, 2015, http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-forcyberspace.html?partner=bloomberg (accessed October 4, 2015); Josh Chin, "Cyber Sleuths Track Hacker to China's Military; the Story of a Chinese Military Staffer's Alleged Involvement in Hacking Provides a Detailed Look into Beijing's Sprawling State-Controlled Cyberespionage Machinery," *Wall Street Journal*, 2015, 2.

[56] U.S. Joint Chiefs of Staff, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: U.S. Joint Chiefs of Staff, 2011), 8.

[57] Barack Obama, “Remarks by the President at the US-China Strategic and Economic Dialogue,” speech, 2009; Robert D. Blackwill and Ashley J. Tellis, *Revising U.S. Grand Strategy toward China* (New York: Council on Foreign Relations, 2015), 14.

[58] Jacques DeLisle, "Politics, Law, and Resentment on the China Coast," *Foreign Policy Research Institute,* July 2001, http://www.fpri.org/articles/2001/07/politics-law-and-resentment-china-coast (accessed February 1, 2016).

[59] Blackwill and Tellis, *Revising U.S. Grand Strategy toward China*, 16.

[60] Ashley J. Tellis, “China’s Grand Strategy: The Quest for Comprehensive National Power and Its Consequences,” in *The Rise of China: Essays on the Future Competition,* ed. Gary J. Schmitt (New York: Encounter Books, 2009), 27.

[61] Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement," *Council on Foreign Relations*, January 4, 2016, http://blogs.cfr.org/cyber /2016/01/04/top-5-us-china-cyber-agreement/ (accessed January 16, 2016).

[62] Hart, "Assessing American Foreign Policy toward China," 9.

[63] Demidov, "Russia-China-United States: Setting the Global Rules of the Game in Cyberspace," 4.

[64] Eric F. Mejia, "Act and Actor Attribution in Cyberspace a Proposed Analytic Framework," *Strategic Studies Quarterly* 8, no. 1 (2014): 114.

[65] Geoffrey Nathan, "Federal Statutes of Limitations,” FederalCharges, http://www.federalcharges.com/federal-statutes-of-limitations/ (accessed February 15, 2016).