"Explicit" Bargains are Essential to Forming Desired Norms in Cyberspace

Major Wonny K. Kim

ABSTRACT

As the United States endeavors to establish international norms in cyberspace, it is critical to delineate which behavioral norms it supports, how it plans to establish them, and to what ends the norms are to serve. Espionage does not violate any international norm; participants have tacitly agreed to undertake espionage and counterintelligence that fall below the "scale and effects" attributed to the "use of force"[1] and assume their associated costs in peacetime. Yet not all espionage in cyberspace below this threshold is considered acceptable. For example, the US desires to bar espionage conducted "with the intent of providing competitive advantages to companies or commercial sectors."[2]

Existing literature largely favors tacit bargaining to develop norms in cyberspace. However, the dynamics of the 2015 U.S.–China Cyber Agreement highlight the necessity of both explicit bargains and the prospect of cooperation to avoid costly escalatory spirals. The newly established position of Deputy National Security Advisor for Cyber and Emerging Technology and the formation of Department of State's Bureau of Cyberspace and Digital Policy offer a chance to develop a US-led multilateral whole-of-government approach for the formation of cyberspace norms. This approach is discussed here, using the the U.S.–China Cyber Agreement to illustrate how it would be preferable over simply relying on tacit bargaining.

Major Wonny K. Kim is an Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command and has served at various echelons in Europe, Africa, and the Middle-East. He holds a Master of International Affairs from Columbia University, a Master of Science in Technical Intelligence from National Intelligence University, and a B.A. in Philosophy and Psychology from Binghamton University.

INTRODUCTION

As the United States (US) endeavors to establish international norms in cyberspace, it is critical that it delineate which behavioral norms it supports, how it plans to establish them, and to what ends the norms serve. These considerations are particularly timely as the current US administration builds its cybersecurity team and considers pressing issues in cyberspace. In January 2021, President Joe Biden appointed National Security Agency Cybersecurity Director Anne Neuberger as Deputy National Security Advisor (DNSA) for Cyber and Emerging Technology in the National Security Council.[3] As reported then, "Neuberger will be responsible for coordinating the federal government's cybersecurity efforts, with a likely emphasis on responding to a massive cyberespionage campaign carried out last year by suspected Russian hackers [referencing SolarWinds], which the government is still struggling to unravel."[4] She has since been joined in the administration by Chris Inglis, National Cyber Director, and Jen Easterly, Director of Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).[5]

Although the SolarWinds breach was extensive, affecting roughly 100 companies and a dozen government agencies,[6] the breach itself was not a violation of international norms as the operation did not escalate beyond espionage.[7] As the US devises its cyber policy, it is imperative to distinguish between actions taken for counterintelligence purposes and actions taken to develop international norms in cyberspace. Espionage is not a violation of an international norm, and the US does not appear inclined to establish it as such. Espionage and counter-espionage are established behaviors that participants have tacitly agreed to undertake and assume their associated costs. Yet some espionage-associated behavior in cyberspace fall

outside these bounds; for example, the US takes exception to espionage conducted "with the intent of providing competitive advantages to companies or commercial sectors."[8]

Current literature advocates for tacit bargaining, that is, behavioral actions and counter-actions, in developing normative behavior in cyberspace.[9] The dynamics of the 2015 U.S.–China Cyber Agreement, however, indicate two important considerations: first, the necessity of explicit bargains, such as international agreements, to support the formation of desired norms that help avoid costly escalatory spirals. Second, how a viable prospect of cooperation underpins the success of norm development. Furthermore, the potential impact of actions taken outside of cyberspace must be taken into account as they did lead to the cyber accord and at least the temporary cessation of the People's Republic of China (PRC) offending activity in cyberspace.[10] These are critical considerations for the US cybersecurity team as they develop US cyber policy: ideally, one directed towards a robust US-led multilateral, whole-of-government approach to the development of norms in cyberspace.

THE SITUATION

The US National Cyber Strategy published in 2018 envisions an open, reliable, and secure cyberspace, one that supports American prosperity, liberty, and security.[11] The key to realizing this vision is accepting cyber norms that "define acceptable behavior to all states and promote greater predictability and stability in cyberspace"[12] and that "attribute and deter unacceptable behavior in cyberspace."[13] The accompanying 2018 Department of Defense (DoD) strategy emphasizes long-term strategic competition from the People's Republic of China (PRC), which has "expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners."[14] The DoD strategy further notes that, "China is eroding US military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from US public and private sector institutions."[15]

Aligning National Cyber Strategy goals with DoD's characterization of the threat requires an assessment of unacceptable PRC behavior. It is critical to note that DoD characterized PRC's espionage as the persistent exfiltration of sensitive information, which sought to damage US interests: through the erosion of US military overmatch and the erosion of US economic vitality.

Eroding US military overmatch is obviously a serious concern, but espionage with the intent to understand and neutralize military advantages has been accepted normative behavior since at least as early as Sun Tzu in the 5th Century, BCE.[16]

It is not espionage itself that is the relevant issue here; rather, it is the intent to erode US economic vitality. This is precisely the issue that President Obama raised with President Xi in the 2015 agreement: espionage "with the intent of providing competitive advantages to companies or commercial sectors,"[17] hereafter referred to as intellectual property-theft (IP-theft).

The 2015 U.S.–China Cyber Agreement states that "the United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[18] The parties also pledged to investigate and mitigate malicious cyber activities emanating from their respective territories, and to support development of "appropriate norms of state behavior in cyberspace."[19] Post-accord, similar agreements were made between the PRC and other G-20 members.[20] Yet the PRC's active theft of IP have since continued.[21]

Continued IP theft has led Dr. Michael P. Fischerkeller of the Institute for Defense Analyses and Dr. Richard J. Harknett of the University of Cincinnati to argue that explicit bargaining, which involves "international conference or bilateral diplomacy and treaty negotiations,"[22] has significant limitations in the cyber domain because participants would not "trust the other to any agreement explicitly reached."[23] They write:

> Consider, for example, the 2015 agreement Presidents Obama and Xi, which committed that neither country would conduct or knowingly support cyber-enabled theft of intellectual property for commercial gain. ... This explicit agreement failed not because of any deficit in U.S. diplomatic bargaining skills, but because the bargaining process itself was not appropriate for the strategic competitive space to which it was applied.[24]

Instead, Fischerkeller and Harknett urge the use of tacit bargaining to develop normative behavior in cyberspace. Tacit bargains are defined by Schelling as "informal agreements.arrived at 'not by verbal bargaining, but by maneuver, by actions, and by statements and declarations that are not direct communication to the enemy.'"[25]

It is important to recognize that these two processes are not mutually exclusive. If the US had responded to violations of the U.S.–China Cyber Agreement[26] with more than mere words,[27],[28],[29] for example, with palpable actions against IP-theft recipients, the accord may have established an international norm and deterred future transgressions. Moreover, responses would not have had to be constrained to cyberspace: threat of economic sanctions is what compelled the PRC to enter into the accord in the first place.[30] Failure of the explicit bargain was not due to any structural realities of cyberspace, but, rather, to "Cheap Talk;"[31] the underlying potential payoffs for the PRC decision calculus ran counter to the explicit agreement. Xi had reason to convince Obama that it was in the PRC's interests and intentions to respect IP, yet the PRC's benefits from violating the agreement outweighed the prospective marginal cost, particularly if the prospect of US follow-through on the threat of sanctions diminished. As US enforcement of the agreement lagged,[32] the prospect of punishment diminished, and the calculus shifted in favor of IP-theft. Alternatively, the PRC may have perceived the prospective value of economic cooperation diminishing, given difficult trade negotiations throughout 2017-2018.[33] Either way, if actors are believed to be rational, trust in the agreement failed because interests were no longer aligned. The take away lesson should have been to enforce agreements, not necessarily that new interactions[34] in cyberspace are required to develop norms.

WHY EXPLICIT BARGAINING IN CYBERSPACE IS NECESSARY

These new interactions, in the form of tacit bargaining, have become embodied in DoD's 2018 Cyber Strategy as a way to contest malicious cyber activity. Countering "cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions."[35] As Fischerkeller and Harknett explain it:

> By describing *persistent engagement*, operationally, as continuously engaging and contesting adversaries and maneuvering for advantage below the threshold of armed conflict … it is reasonable to conclude that persistent engagement would support a strategic process of tacit bargaining adopted to develop mutual understandings with adversaries on acceptable/unacceptable behavior in agreed competition.[36]

Notionally, then, U.S Cyber Command (USCYBERCOM) would engage and contest adversaries conducting espionage in cyberspace for economic gain and thereby counter with consequences this unacceptable behavior. However, tacit bargaining in foreign networks, absent explicit bargains, risks establishing stable yet undesirable normative behavior.[37] Instead of the "open, reliable, and secure" cyberspace envisioned by the US strategy, this risks leaving the US vulnerable to costly escalatory spirals.

Escalatory Spirals

Escalatory spirals spawned by cyberspace actions have already occurred. Examples include Iran accelerating its cyber development and deployment following the attack on its uranium enrichment centrifuges (Stuxnet attack[38],[39]), and Russia's claim that it was simply responding in kind through cyber means to the Panama papers release.[40] Predicated on whether cyberspace becomes truly offense-dominant or defense-dominant as the domain matures,[41] two types of escalatory spirals may occur in cyberspace:

1) A spiral that leads to a standoff with the potential to breach the limits of "competition short of armed conflict"[42]
2) A spiral that stabilizes as marginal costs eventually match marginal gains in a costly competition.[43]

In either case, at least in regards to IP-theft, both of these options are less desirable than a US-PRC agreement to reciprocate on IP protection and cooperate on combating the economic threat of cyber-crime which was the envisioned state of relations in the 2015 accord.

In lieu of an explicit agreement, consider if USCYBERCOM had engaged in tacit actions to punish and thereby compel the PRC to cease its IP-theft. US experience with economic sanctions has proven the importance of focusing efforts on the appropriate targets and communicate the desired behavior change.[44] As such, USCYBERCOM's two likely targets would be

1) Those who authorize and conduct state espionage in cyberspace, as well as the abetting network infrastructure (PRC cyberspace state espionage)

2) Those that receive and exploit the stolen IP (IP-theft recipients).

Targeting PRC cyberspace state espionage

While disrupting or degrading the PRC's IP-theft enabling infrastructure is appealing, this approach is likely to be unhelpful for norm formation because the US is faced with a "Cheap Talk" dilemma of its own. This is because the US is motivated to disrupt or degrade this target for counterintelligence against espionage writ-large.[45] Even if explanatory communications accompany the counter-action and give IP-theft as the reason why it was imposed, there is no reason for the PRC to trust that these actions would end as the US benefits from the disruption. Furthermore, as the PRC would most likely not resume espionage from a network that is known to be compromised, there is no value proposition for the PRC to have the US cease its disruption or degradation activities. This is the antithesis for driving desired behavior change since it is necessary that the adversary sees both the prospect and value in the punishment ending when the egregious IP-theft behavior ends.[46] Tacit bargaining in this situation exacerbates the trust dilemma, not alleviates it. Instead, the US incurs ongoing manpower and resource costs to defend forward in order to suppress IP-theft, and the US and PRC are embroiled in an escalatory spiral in pursuit of marginal advantages over each other. As such, tacit bargaining, even with explanatory communications, contributes little to the development of the desired norm.

If the US could effectively disable all PRC espionage, that would eliminate IP-theft, but that is unrealistic. Again, the Iranian response to Stuxnet shows that an escalatory spiral is invariably in the offing given the low barrier to entry into cyberspace.[47] Even DoD acknowledges the futility of attempting to achieve total dominance.[48]

Targeting IP-theft recipients

Turning to the second set of targets, the *IP-theft recipients*, the US has followed "a two-pronged approach to combat economic espionage: (1) reducing theft by educating and training the private sector how to improve security and safeguard secrets,[49] and (2) federally prosecuting offenders."[50] This latter approach has yielded a mixed bag[51] with few convictions under the 1996 Economic Espionage Act,[52] none involving cyber espionage. Considering that IP-theft continues to plague the US at enormous scale,[53] prosecuting offenders does not seem to have effectively stemmed or deterred cyber-enabled IP-theft, anecdotal arguments to the contrary notwithstanding.[54] Whether US actions targeting non-cyber actors, including the Department of Justice's recently concluded China Initiative,[55] are successful at reducing espionage is outside the scope of this article.

A potential third US option is to threaten US cyberspace retaliation against businesses that exploit stolen US IP. This is likely to have some deterrent effect on IP-theft recipients' behavior. Examples of such potential punitive actions abound, from denial-of-service attacks against network infrastructure to malware akin to NotPetya[56] or high-profile ransomware attacks.[57] However, without an explicit bargain, these actions invite tit-for-tat reciprocal responses against US economic targets. Even if we assume that attribution for these actions makes them discernible from the background noise of cybercrime, without an explicit bargain, any US claim to legitimacy for its tacit actions is severely weakened, especially considering these actions would be conducted on foreign networks outside of US sovereignty. This greatly diminishes the value to normative behavior formation and lowers the barrier for retaliatory PRC action. Absent the explicit agreement, the PRC can simply claim the US violated their sovereign networks and reciprocate in kind. As such, prosecuting this target set with tacit actions in cyberspace also carries the potential for an escalatory spiral, not unlike the current US-PRC trade-war. The solution must include consideration for PRC domestic enforcement, which manifests in the prospect for cooperation discussed later herein.

Prospect of Punishment and Retaliation

Tacit bargains without explicit bargains risk escalatory spirals; explicit bargains need to be enforced. Had USCYBERCOM and other US agencies acted in defense of the 2015 U.S.–China Cyber Agreement by imposing punitive actions in response to PRC transgressions, this punishment would have helped to deter future transgressions.[58] Even Fischerkeller and Harknett support the dual importance of explicit and tacit bargains when they advocate for "an aligned application of them to the strategic realities the United States faces."[59] They write further:

> The success of a strategic framework for constructing cyber norms grounded in persistent engagement and tacit bargaining will depend, in part, on how well states communicate their national interests in cyberspace. Behavioral convergence around definable limitations is how sustainable cyber norms can be constructed.[60]

Those communicated defined limitations are the basis for explicit bargains, which confer legitimacy on retaliatory action; the prospect of retaliatory action and ensuing escalatory spirals supports behavioral convergence. This is where we see the convergence of explicit and tacit bargains. Even in the relatively benign costly competition scenario, the level of competition tacit bargaining will spawn will always be less desirable than a cyberspace characterized by cooperation. The US's failure to respond to PRC violations unfortunately, but predictably, emboldened PRC exploitation. However, while it becomes evident that explicit bargains and tacit enforcement are both necessary, this argument also leads to another question in the shadow of a potential escalatory spiral: what happens if the PRC reciprocates in kind against punishment, despite an explicit bargain? This question highlights the importance of the prospect of cooperation.

WHY CULTIVATING TRUE COOPERATION IS KEY

Criminal, non-state sponsored, activity withstanding, why would the PRC choose to violate an explicit bargain in the face of a credible threat of retaliation? Assuming a rational actor, it would be simply because the prospective marginal gains still outweigh the prospective marginal costs. Though explicit bargains set the conditions for avoiding escalatory spirals, there must exist a viable and mutually beneficial solution which is attainable through the prospect of cooperation. Otherwise, both sides would be resigned to a future of escalatory standoffs or costly competition. Notably, this is where the dynamics of counter-intelligence and norm development diverge. Namely, espionage and counterintelligence have no other prospective solutions outside of tacit bargaining, absent the possibility of an intelligence-sharing treaty like the United Kingdom – United States of America Agreement (UKUSA), also known as the "Five Eyes." Without such agreements, practitioners typically accept costly competition and retrospectively define the boundaries of acceptable action by triggering escalatory standoffs. Whether the SolarWinds hack is such a trigger or just becomes another aspect of costly competition remains to be seen. Either way, on norm development, it may be easier to build cooperation on economic issues as the market may have already provided the prospect for such regarding IP-theft.

In his seminal work, *The Evolution of Cooperation*, Robert Axelrod notes that the prospect of continued engagement enables cooperation to develop; inversely, a perception that the PRC or US would soon collapse undermines motivation for either party to cooperate. Instead, each would simply exploit the other for as much as it can steal from the other before the game ends. Assuming neither party is on the verge of collapse, in an environment in which continuous engagement is to be expected, for a strategy to be collectively stable—that is, able to resist the invasion of competing strategies—the strategy must offer a higher rate of return than a competing strategy. In other words, an international normative behavior must essentially be self-reinforcing. This requires two sequential conditions:

1) The reciprocal benefits of IP protections must be more beneficial amongst cooperating parties, e.g. the like-minded nations in the G-20, than for them to participate in IP-theft against each other

2) For (1) to be true, those who protect and respect IP must be prepared to retaliate collectively against those that adopt IP-theft, to deny, reduce, or otherwise render prohibitively costly the stolen IP.[61]

In essence, retaliation for violations of an international norm should be multilateral. Not only would a multilateral effort relieve the US of solely bearing the costs of enforcement, multilateral condemnation of IP-theft would provide even greater legitimacy to any punitive actions inside or outside cyberspace, raising the credibility and scope of potential punishment for violations while constraining the PRC's freedom of action to retaliate in kind.

While effective retaliation may deter future transgressions, the ability to return to a mutually cooperative state is as important.[62] Pundits may argue that communicating on such intentions

is impossible due to issues of trust, but the economic market for justice may well have already provided the tacit evidence necessary to move nations and other entities towards a cooperative cyberspace and away from IP-theft. As Fareed Zakaria put it,

> That China engages in rampant theft of intellectual property is a widely accepted fact—except among U.S. companies doing business in China. In a recent survey of such companies conducted by the U.S.-China Business Council, intellectual property protection ranked sixth on a list of pressing concerns, down from number two in 2014. ...Why this shift from 2014? That year, China created its first specialized courts to handle intellectual property cases. In 2015, foreign plaintiffs brought 63 cases in the Beijing Intellectual Property Court. The court ruled for the foreign firms in all 63.[63]

Since then, the IP caseload has grown rapidly. "In 2018 alone, Chinese courts received 301,278 new IP cases in the first instance, of which 287,795 were concluded. These figures represent an increase of 41 percent and 42 percent respectively compared to those for 2017."[64] These include cases involving myriad American, Chinese, and other international companies.[65] Interestingly, ~79% of the cases brought before the court were purely PRC domestic cases,[66] with the remainder having foreign interests represented. In those latter cases, the court ruled in civil cases ~68% of the time in favor of foreign interests over domestic parties.[67]

Historical evidence points towards potential cooperation on intellectual property rights as well. As Yukon Huang and Jeremy Smith from the Carnegie Endowment for International Peace argue,

> In terms of outright theft of IP, China's infractions are anything but unique: It is just one of 36 violators listed in the 2019 Special 301 Report by the Office of the U.S. Trade Representative (USTR). Historically, rapidly growing emerging market economies tend to be cited as they transition to higher income levels. For example, decades ago Japan, South Korea, and Taiwan were each perennial Section 301 violators until they reached a per capita GDP of about $20,000-$25,000.[68]

Given the PRC's per capita GDP is roughly $17,000 as of 2020,[69] this hypothesis will likely be tested in the near future.

Others are less optimistic about China's IP-theft, noting that the US Trade Representative cites numerous cases and complaints in the office's 2018 report on PRC IP-theft.[70] And Zakaria does not consider that many affected US businesses may be unaware that they were victims of such theft.[71] However, Zakaria does highlight the convergence of PRC interests, US pressure, and desired normative behavior by stating that,

> reforms...are often undertaken only in the face of Western pressure and, even then, because they serve China's own competitive interests—the largest filer of patents worldwide last year was the Chinese telecommunications giant Huawei. But it is also true that many Chinese economists and senior policymakers have argued that the country will modernize and grow its economy only if it pursues further reform.[72]

While it may not be immediate, there certainly appears to be a prospect of cooperation that benefits both parties as the marginal gains from reciprocal IP protection outweigh the marginal gains from IP-theft as China's economy matures.

Some claim that this was a *fait accompli*, that the Chinese economy was essentially able to mature because of the IP-theft over these past decades. This is perhaps true and it may have been a strategic failure of the US for not timely countering. However, it was not a failure of the US to envision an operational approach to cyberspace; tacit bargains without explicit bargains are unlikely to have been helpful; and tacit bargains in support of the explicit bargain, though some may have been potentially successful, would still run the risk of an escalatory spiral absent a perceived prospect of cooperation. Additionally, a multilateral effort to collaborate on punishing IP-theft and protecting the value of cybersecurity cooperation is still lacking. How to resolve the issues of retribution for past transgressions is beyond the scope of this article, which seeks to highlight the dynamics at play and explain why explicit bargains, the prospect of cooperation, and multilateral coordination outside of the cyberspace domain are important keys to developing international norms within cyberspace.

CONCLUSION

The US government has an absolute obligation to keep its citizenry safe and uphold security commitments to allies and partners, and this article should not be read to suggest otherwise, or that the US should not contest espionage or protect sensitive technology that supports US security through military overmatch. However, in forming *desired* normative behavior, the focus is not the act of espionage itself, but the subsequent exploitation of the stolen IP. Tacit bargaining and actions alone are insufficient to develop this norm, and should be conducted in tandem with explicit bargains and a prospect of cooperation that is viable and desirable.

Following the 2015 U.S.–China Cyber Agreement, had USCYBERCOM imposed costs on PRC economic targets in response to transgressions, the explicit bargain might well have been saved through tacit enforcement, provided that prospective gains from cooperation and losses from a potential escalatory spiral were perceived as outweighing marginal gains from IP-theft. Given that the PRC is now exhibiting a willingness to retaliate against trade sanctions in a reciprocal manner, unfettered tacit actions in cyberspace seem more likely than ever to trigger a retaliation rather than establish deterrence. This is evidenced by the PRC's recent passage of its Anti-Foreign Sanctions Law which legalizes PRC retaliation against companies complying with US and EU sanctions.[73] Perhaps the most compelling, and ironic, example against the standalone use of tacit bargaining in cyberspace is the PRC actions following the 2015 accord. US officials were left befuddled as to why the PRC decided to renege on its commitments[74] and PRC actions have clearly provoked further US escalatory responses, leading to an escalatory spiral in the tit-for-tat trade war. Whether the trade war results in a stable costly competition centered on reciprocal tariffs, an escalatory standoff threatening military action, or a return to the liberalization of trade remains to be seen.

In addition to the appointments of the Deputy National Security Advisor for Cybersecurity to the National Security Council, the National Cyber Director, and the Director for CISA, the Department of State recently established the Bureau of Cyberspace and Digital Policy (CDP) to lead US government diplomatic efforts on: (1) International cybersecurity focusing on deterrence, negotiations and capacity building, (2) International digital policy for internet governance and trust in global telecom systems, and (3) Digital freedom in regards to human rights and engagement between the private sector and society.[75] This raises the prospect for coordinating a multilateral approach to dealing with IP-theft. As Axelrod's analysis suggests, all cooperating entities on a norm should retaliate against violators in support of collective stability.[76] Regarding IP-theft, as Richard McGregor writes, traditional US allies and partners like Europe, Australia, and Japan are eager to work more closely with the US on China trade policy.[77] The opportunity may be at hand, through multilateral collaboration, to enhance the legitimacy of any punitive actions for IP-theft while constraining the PRC's freedom of action for retaliatory actions in kind. This is particularly pertinent given that the PRC already has standing explicit agreements on IP-theft with G-20 countries.

Rather than limiting itself to cyberspace alone, the US should also leverage tools and levers across the US government to change expected value propositions for PRC actions; a whole of government approach. Clearly, actions outside the cyberspace domain influence actions within it: note again that it was the prospect of economic sanctions that motivated the PRC to enter into the 2015 Accord in the first place. Much work remains to be done on formulating US cyber policy and how the US chooses to align interests and actions in cyberspace. However, we should hope that the prospect of cooperation remains viable, lest we resign ourselves to the constant risk of escalatory spirals. As the new US national cybersecurity leadership establishes themselves, the US has an opportunity to revisit explicit bargains and foster multilateral cooperation on tacit actions.

DISCLAIMER

The views expressed here are the author's and do not necessarily reflect the position of the National Intelligence University, the U.S. Army Reserve 75th Innovation Command, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government.

ACKNOWLEDGEMENTS

This article was based on my thesis at National Intelligence University, and I would like to thank my advisors, Professor Jason Healey, Columbia University, and Lieutenant Colonel John Duselis, U.S. Marine Corps. I would also like to thank Vivian Lei, my wife, for her enduring support.

NOTES

1. The broadest definition of an upper bound for acceptable behavior of operations in cyberspace in peacetime are those that fall short of the "scale and effects" attributed to the "use of force," drawing its verbiage from the UN Charter, Article 2(4). International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations,* Edited by Michael N. Schmitt and Liis Vihul, (New York: Cambridge University Press, 2017), 339.
2. Office of the Press Secretary, The White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, accessed on July 30, 2020.
3. William Turton, "The Former NSA Official Vying to Steer Biden's Cyber Policy, January 7, 2022, https://www.bloomberg.com/news/articles/2022-01-07/anne-neuberger-the-former-nsa-official-shaping-biden-s-cybersecurity-policy, accessed on January 17, 2022.
4. Natasha Bertrand, "Biden taps intelligence veteran for new White House cybersecurity role," *Politico,* January 6, 2021, https://www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508, accessed on January 18, 2021.
5. Ellen Nakashima, "Biden administration plans to name former senior NSA officials to White House cyber position and head of CISA," April 12, 2021, https://www.washingtonpost.com/national-security/former-senior-nsa-officials-named-to-white-house-cyber-position-and-head-of-dhs-cyber-agency/2021/04/11/b9d408cc-9b2d-11eb-8005-bffc3a39f6d3_story.html, accessed January 17, 2022.
6. Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack, accessed on September 9, 2021.
7. Michael Schmitt, "Top Expert Backgrounder: Russia's SolarWinds Operation and International Law," Just Security, December 21, 2020, https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/, accessed on January 17, 2022.
8. Office of the Press Secretary, The White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, accessed on July 30, 2020.
9. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Norms in Cyberspace," Lawfare, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace, accessed on July 20, 2020.
10. John P. Carlin and Garrett M. Graff, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat,* (New York, NY: PublicAffairs, 2018.)
11. The White House, "National Cyber Strategy," 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accessed on August 6, 2020.
12. Ibid, 20.
13. Ibid, 21.
14. Department of Defense, "Cyber Strategy Summary," 2018, 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed on July 30, 2020.
15. Ibid.
16. Mike Giglio, "China's Spies Are on the Offensive," *The Atlantic,* August 26, 2019, https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/, accessed on July 30, 2020.
17. Office of the Press Secretary, The White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, accessed on July 30, 2020.
18. Ibid.
19. Ibid.
20. Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," Council on Foreign Relations, September 28, 2016, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later, accessed on July 30, 2020.

NOTES

21. National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf, accessed on July 30, 2020.
22. Fischerkeller and Harknett, "Persistent Engagement and Tacit Bargaining."
23. Ibid.
24. Ibid.
25. Ibid.
26. Fireeye, "Redline Drawn: China Recalculates its use of Cyber Espionage," June 2016, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf, accessed on August 6, 2020.
27. Cory Bennett, "Why Trump is sticking with Obama's China hacking deal," *Politico,* November 8, 2017, https://www.politico.com/story/2017/11/08/trump-obama-china-hacking-deal-244658, accessed on July 20, 2020.
28. Chris Bing, "Trump administration says China broke Obama-Xi hacking agreement," cyberscoop, March 22, 2018, https://www.cyberscoop.com/trump-china-hacking-obama-xi-agreement/, accessed on August 6, 2020.
29. Department of Homeland Security, "First U.S.-China Law Enforcement and Cybersecurity Dialogue," October 6, 2017, https://www.dhs.gov/news/2017/10/06/first-us-china-law-enforcement-and-cybersecurity-dialogue, accessed on August 6, 2020.
30. Carlin and Graff, *Dawn of the Code War,* 366-367.
31. Joseph Farrell and Matthew Rabin, "Cheap Talk," *Journal of Economic Perspectives,* Vol. 10.3 (1996), 103-118.
32. Carlin notes that there was a "new norm" that had broken down by 2018. He does not detail any US response except that of Jeff Session's China Initiative starting in 2018. John P. Carlin and Garrett M. Graff, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat,* (New York: PublicAffairs, 2018), 370.
33. Heather Timmons, "Timeline: Key dates in the U.S.-China trade war," Reuters, January 15, 2020, https://www.reuters.com/article/us-usa-trade-china-timeline/timeline-key-dates-in-the-u-s-china-trade-war-idUSKBN1ZE1AA, accessed on August 6, 2020.
34. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation," Institute for Defense Analysis, May 2018, 9, https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx, accessed on July 30, 2020.
35. Department of Defense, "Cyber Strategy Summary," 2018, 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed on July 30, 2020.
36. Fischerkeller and Harknett, "Persistent Engagement and Tacit Bargaining."
37. Akin to a suboptimal Nash equilibrium in a continuous Prisoner's Dilemma - Pareto efficient outcomes that are undesirable compared to other pareto efficient outcomes that have higher payoffs; Colin F. Camerer, *Behavioral Game Theory: Experiments in Strategic Interaction* (Princeton, New Jersey: Princeton University Press, 2003).
38. Following the 2010 Stuxnet attack against Iran's uranium enrichment centrifuges, Iran has since developed and employed offensive cyber attack capabilities. Andrea Shalal-Esa, "Iran strengthened cyber capabilities after Stuxnet: U.S. general," Reuters, January 17, 2013, https://www.reuters.com/article/us-iran-usa-cyber-idUSBRE90G1C420130118, accessed on July 30, 2020.
39. Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities," January 13, 2020, https://sgp.fas.org/crs/mideast/IF11406.pdf, accessed on September 9, 2021.
40. "Putin publicly pointed to the Panama Papers disclosure…as US-directed efforts to defame Russia…" and is assessed to be a potential driver for Russia's interference in the 2016 US Presidential Election. Office of the Director of National Intelligence, "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf, accessed on July 30, 2020.
41. Concepts of offense- and defense-dominant from Robert Jervis; Robert Jervis, "Cooperation under the Security Dilemma," from *Conflict After the Cold War: Arguments on Causes of War and Peace, 5th Edition* edited by Richard Betts, (New York, NY: Routledge 2017).
42. Fischerkeller and Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation," 9.

NOTES

43. Readers familiar with economic theory may recognize the similarity of this concept to suboptimal Pareto efficiencies derived from participants pursuing dominant strategies in a Prisoner's Dilemma game.
44. Richard Nephew, *The Art of Sanctions: A View from the Field.* (New York: Columbia University Press, 2018).
45. National Counterintelligence and Security Center, "National Counterintelligence Strategy of the United States of America 2020-2022," January 7, 2020, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf, accessed on August 6th, 2020.
46. Richard Nephew, *The Art of Sanctions: A View from the Field.* (New York: Columbia University Press, 2018).
47. Robert Jervis and Jason Healey, "The Dynamics of Cyber Conflict," Columbia University, SIPA, August 2, 2019, https://sipa.columbia.edu/sites/default/files/embedded-media/Brochure%20on%20the%20Dynamics%20of%20Cyber%20Conflict.pdf, accessed on July 30, 2020.
48. USCYBERCOM, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, accessed on July 30, 2020.
49. Passive defensive actions to "harden" potential economic targets of IP-theft are out of scope for this paper; however, there is evidence that such efforts have not been effective at stemming cyber-crime, let alone state-sponsored cyber espionage. Coveware, "Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound," April 26, 2021, https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound, accessed on September 9, 2021.
50. Melanie Reid, "A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with This Global Threat?" *University of Miami Law Review*, Vol. 70, No. 1 (2016), 58.
51. Andrew Boutros, David Kelley, and Jay Schleppenbach, " Department of Justice Year-End Update Shows 'China Initiative' Prosecutions Are Alive and Well," Dechert LLP, December 7, 2021, https://www.jdsupra.com/legalnews/department-of-justice-year-end-update-2087556/, accessed on January 17, 2022.
52. Eileen Guo, Jess Aloe, and Karen Hao, "The US crackdown on Chinese economic espionage is a mess. We have the data to show it," MIT Technology Review, December 2, 2021, https://www.technologyreview.com/2021/12/02/1040656/china-initative-us-justice-department/, accessed on January 17, 2022.
53. The Commission on the Theft of American Intellectual Property, "Update to the IP Commission Report," The National Bureau of Asian Research, 2017, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf, accessed on July 30, 2020.
54. Neal Pollard et. al., "Named But Hardly Shamed: The Impact of Information Disclosures on APT Operations," Columbia University, SIPA Capstone Project, Spring 2020.
55. Department of Justice, "Attorney General Jeff Session's China Initiative Fact Sheet," November 1st, 2018, https://www.justice.gov/opa/speech/file/1107256/download, sccessed on January 17, 2022. Steve Kwok, "DOJ Steps Back From China Initiative But Remains Focused On China-Related Enforcement," Coventus Law, April 1, 2022, https://conventuslaw.com/report/doj-steps-back-from-china-initiative-but-remains-focused-on-china-related-enforcement/, accessed on April 15, 2022.
56. NotPetya was a high-profile malware attack that crippled infrastructure and organizations around the world that is assessed to have been originally directed at Ukraine by Russia, but went awry due to poor safeguards in the coding. Mike McQuade, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, accessed on July 30, 2020.
57. Matt Stieb, "What's Driving the Surge in Ransomware Attacks?" *Intelligencer, New York Magazine,* June 11, 2021, https://nymag.com/intelligencer/article/ransomware-attacks-2021.html, accessed on June 13, 2021.
58. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security,* Vol. 41, No. 3, Winter 2016/2017, 44-71.
59. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining."
60. Ibid.
61. Robert Axelrod, *The Evolution of Cooperation:* rev. ed. (New York: Basic Books, 2009).
62. Ibid.
63. Fareed Zakaria, "The New China Scare: Why America Shouldn't Panic About Its Latest Challenger," *Foreign Affairs,* Vol. 99, No. 1, 2020, 59.

NOTES

64. Tao Kaiyuan, "China's commitment to strengthening IP judicial protection and creating a bright future for IP rights," *WIPO Magazine*, World Intellectual Property Organization, June 2019, https://www.wipo.int/wipo_magazine/en/2019/03/article_0004.html, accessed on July 30, 2020.
65. Aaron Wininger, "China's Supreme People's Procuratorate Issues Top Example Cases of Criminal Intellectual Property Rights Infringement in 2019," *The National Law Review,* Vol X. No. 212, April 26, 2020, https://www.natlawreview.com/article/china-s-supreme-people-s-procuratorate-issues-top-example-cases-criminal, accessed on July 30, 2020.
66. DEQI Intellectual Property Law Corporation, "Beijing Intellectual Property Court: Foreign-related Intellectual Property Cases Increasing Year by Year," https://www.lexology.com/library/detail.aspx?g=62f25070-8679-4b84-bf67-202b3109e949, accessed on September 9, 2021.
67. Ibid.
68. Yukon Huang and Jeremy Smith, "China's Record on Intellectual Property Rights Is Getting Better and Better," October 16, 2019, https://carnegieendowment.org/2019/10/16/china-s-record-on-intellectual-property-rights-is-getting-better-and-better-pub-80098, accessed on September 9, 2020.
69. World Bank, "GDP per capita, PPP (current international $) – China" Most recent year 2020, https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?end=2020&locations=CN&start=1990, accessed on September 9, 2020.
70. Office of the United States Trade Representative, Executive Office of the President, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," March 22, 2018. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF, accessed on July 30, 2020.
71. Megan Reiss, "Counting Cybercrimes," *The American Interest* February 27, 2018, https://www.the-american-interest.com/2018/02/27/counting-cybercrimes/, accessed on July 30, 2020.
72. Zakaria, "The New China Scare: Why America Shouldn't Panic About Its Latest Challenger," 59.
73. Chun Hanong, "China Passes Law to Counter Foreign Sanctions," *The Wall Street Journal,* June 10, 2021, https://www.wsj.com/articles/china-passes-law-to-counter-foreign-sanctions-11623327432, accessed on June 13, 2021.
74. David E. Sanger and Steven Lee Myers, "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology," *The New York Times,* November 29, 2018, https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html, accessed on August 6, 2020.
75. Samantha Schwartz, "State Department to add cyber bureay, tackle tech diplomacy," November 9, 2021, https://www.cybersecuritydive.com/news/state-department-blinken-cyber-bureau-diplomacy/609697/, accessed on January 17, 2022.
76. Robert Axelrod, *The Evolution of Cooperation, rev. ed.* (New York: Basic Books, 2009).
77. Richard McGregor, *Xi Jinping: The Backlash,* Lowy Institute for International Policy, (Docklands, Australia: Penguin Books, 2019).