2017 9th International Conference on Cyber Conflict
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)

The Coming of Cyber Espionage Norms

Martin Libicki
Distinguished Visiting Professor
US Naval Academy

Abstract: The proposition that cyber espionage is acceptable state behavior, even as cyber attack is unacceptable, is in question. The United States has raised objections to certain types of cyber espionage activity, notably: (1) Chinese economically-motivated cyber espionage; (2) the (feared) transfer of data taken from the US Office of Personnel Management (OPM) and provided to criminals; and (3) Russian doxing attacks, particularly against the Democratic National Committee (DNC). In effect, the United States has been edging towards advocating a new class of norms for cyber espionage – countries may carry it out, but not use the results for other than traditional intelligence purposes, that is for informing national security decision-making. Other forms of cyber espionage may come to be viewed as unacceptable, notably the uses of cyber espionage to enable cyber attacks on critical infrastructure.

Establishing a norm that holds some forms of cyber espionage to be acceptable and others not would raise issues. First, can the United States and its friends define such norms in ways that render unacceptable (many of) those practices it finds objectionable, but do not prevent its own practices from being deemed unacceptable? In particular, can there be norms expressed in ways that allow all targets and methods to be used but restrict only what can be done with the information collected? Second, can monitoring regimes be developed to distinguish acceptable from unacceptable cyber espionage and attribute such actions – not only correctly, but in ways that are accepted widely enough to dissuade further such activity?

Keywords: *cyberspace, espionage, norms, cyber espionage*

1. INTRODUCTION

For hundreds of years, physical attacks by countries have been treated as unacceptable, and hence as reasonable pretext for a forceful response. Extending this principle, the United Nations Group of Governmental Experts declared in 2013 that existing international law (originally developed for conventional combat) also applies in cyberspace (United Nations 2013).

Conversely, espionage by countries has been treated as acceptable state behavior, hence not a reasonable pretext. This understanding has been carried over into cyberspace. Responsible nations may carry out cyber espionage (violating a system's confidentiality), but they may not carry out cyber attacks (operations that violate a system's integrity or availability).

In recent years, the United States, together with like-minded countries, has indicated that it does not feel that all cyber espionage is acceptable state behavior. It has complained about Chinese industrial cyber espionage since early 2010, winning a presidential-level agreement from China to ban such a practice (White House 2015b). It was considering declaring unacceptable the transfer of personally identifiable information harvested from the US Office of Personnel Management (OPM) hack into cybercrime markets (the issue had never been raised because there was scant evidence of any such transfer). In late 2016, President Obama argued that using stolen information to maliciously publish discrediting or private information on individuals (doxing) and thereby interfere with electioneering deserved and would get a response (Detrow 2016). Soon thereafter, he levied sanctions on Russia. This was after a great deal of urging by Congressman Schiff and many others for a strong response (Williams 2016). The United States is not alone in such sentiments. A G-20 communiqué extended the Xi-Obama agreement to 18 other countries (Poplin 2015). In looking at the potential for similar incidents affecting its politics, the UK has shown that it is similarly worried about Russian "cyber war" (Haynes 2016).

Perhaps needless to add, the tussle over cyberspace norms reflects not only the newness of the medium, but recent geostrategic realities in which the United States and like-minded allies contend with a rising great power (China) that seeks to maximize its national advantage within a broader international community, a declining great power (Russia) whose leaders are increasingly defining their legitimacy by opposition to the West, and several outliers (Iran and North Korea).

With that as background, this paper now intends to argue the following propositions:

First, the United States has been advocating what is, in effect, a new set of *peacetime* norms that limit what kind of cyber espionage countries can carry out. By norms, this paper means a set of understandings about what is or is not acceptable state behavior, whether or not such norms are codified by treaty.

Second, there may be other activities which may be deemed unacceptable, notably those that would help protect critical infrastructure.

Third, the United States (and its friends) should insist that such norms be shaped in terms of what countries do with the information they capture, rather than from which systems they are looking for such information, even if one is often a proxy for the other.

Fourth, while determining that state behavior violates norms is challenging if not impossible, several approaches are possible.

Although this essay is written from a US perspective (as per the author's experience), many of its basic assumptions, notably the distinctions between acceptable and unacceptable cyber espionage, are shared to a great extent among the other Five Eyes countries (Canada, the UK, Australia, New Zealand) and to a considerable extent by NATO members and other US allies.[1]

Consider, now, the three norms sketched below as exemplars of the shift in what can be considered acceptable state behavior.

2. NORM AGAINST ECONOMICALLY-MOTIVATED CYBER ESPIONAGE

The struggle between the United States and China over cyber espionage norms shows that creating them is no straightforward process. Starting in roughly 2009, US officials (as well those of allied countries) argued that while cyber espionage was acceptable state behavior if carried out to protect national security, it was not acceptable behavior if economically motivated – notably if the results were handed to corporations to give them an unfair trade advantage. As the Director of National Intelligence (DNI) said in 2013:

> What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of – or give intelligence we collect to – US companies to enhance their international competitiveness or increase their bottom line (Clapper 2013).

The absence of such a norm created the case for a new one.[2] To win Chinese accession to such a norm, or at least to modify China's behavior, the United States first tried cabinet-level admonitions and then moved onto presidential admonitions (the Sunnylands summit of June 2013), the May 2014 indictments of PLA officers (May 2014), and a March 2015 Executive Order that laid the groundwork for sanctions against companies (White House 2015a). By the summer of 2015 such sanctions had become a real possibility.

One tool the United States did not and could not use was to threaten to act the same way by arguing that if economically-motivated cyber espionage is acceptable, then we will go ahead and do it ourselves. This threat would not have been credible. Not only does the US *Government* lack the apparatus to identify intellectual property in private Chinese corporations that US *firms* might profitably use, it would have been legally problematic to provide the information to one US competitor without providing it to them all. Furthermore, even if the United States did so, the Chinese would still come out well ahead, because US companies, at this stage, have considerably more intellectual property at risk than do Chinese companies; consider, for example, the great disparity between technology licensing revenues accruing to firms headquartered in each country.

1 There are differences between the US approach and those of many other NATO members, notably over mass surveillance and the right to privacy, but neither issue is discussed in this paper.

2 The consensus was that the Agreement on Trade-Related Aspects of Intellectual Property Rights amendments to the World Trade Organization, of which China is a member, enjoins signatories against stealing intellectual property, but did not itself provide sufficient support for a norm against economically-motivated cyber espionage.

The norm against cyber espionage was initially framed as a norm against going after certain targets. The US position was essentially that it did not spy on commercial enterprises and therefore it was not hypocritical to expect others to refrain. But the Snowden revelations made it difficult to deny that the United States did spy on commercial companies. Such cyber espionage was undertaken: (1) to look for weaknesses in commercial products, the knowledge of which would facilitate compromising the systems of their customers (who could well be legitimate national-security targets) (Sanger and Perlroth 2014); (2) to help track terrorists who used commercial systems (notably telecommunications) supplied by these companies (Schneier 2014); or (3) to aid the US negotiating position vis-à-vis foreign countries (Romero 2013). So, the US argument switched to: we do not spy on commercial companies *for the purposes of helping US companies compete*.[3] In other words, the US formulation was reframed from enjoining certain targets of cyber espionage to limiting what can be done with the results.

As it was, China never officially argued that economically-motivated cyber espionage was no worse than national-security cyber espionage. Instead it argued, with increasing implausibility, that the United States (or other accusers) had no proof that the Chinese had carried it out (Economist 2013). The February 2013 release of the Mandiant report, however, made that argument difficult to sustain; this was followed by an avalanche of similar revelations by other US cyber security companies. By May 2015, few in Beijing were trying to pretend that the Chinese did not carry out economically-motivated cyber espionage.[4]

Ultimately, the United States succeeded. In September 2015, President Xi Jinping promised that China would neither conduct nor tolerate such cyber espionage. Evidence to date (for instance, from Dilanian 2016) suggests that China has largely stuck by its promise (Nakashima 2016). Indeed, FireEye, the company that bought Mandiant, has reported that its monthly investigations into Chinese cyber espionage for corporate clients had fallen from 35 per month before the agreement to 3-to-10 per month afterwards (Marks 2016). Although the Chinese did react to the agreement by avoiding detection better, tradecraft simply does not improve fast enough to account for such a fall-off.

This introduces the first norm that the United States (successfully) fought for: cyber espionage is acceptable *unless* the results are used to help a country's firms compete.[5]

3. THE CYBERCRIME MARKETS NORM

As irritating as the hack on the US OPM was, in and of itself, it did not violate established cyber espionage norms. The then-Director of National Intelligence and a former head of the

3 Although foreign officials do not always believe that the United States actually follows such rules, proof that it has not has been difficult to come by.

4 As my colleague, Scott Harold, and I found when interviewing Chinese academics and government officials for the RAND Publication, *Getting to Yes with China in Cyberspace* (Harold, Libicki and Cevallos 2016).

5 China privately criticized the US position against intellectual property theft for its hypocrisy; after all, stealing technologies gave a push to US industrial development in the late 18th and early 19th century. Now that the United States is the global leader in licensing technology, it had more to lose than gain from such theft – hence its insistence on such norms. But perhaps the Chinese, themselves, were beginning to recognize that without respecting intellectual property – many thefts of which are internal – their own companies would not develop their own technology only to see it stolen.

Central Intelligence Agency (CIA) both indicated that they would have done the same had the opportunity presented itself.[6]

Nevertheless, the hack raised questions about what the Chinese would do with the information. They could use it themselves, perhaps to help focus their recruitment of US citizens as spies, or they could trade such information with Russia for similar purposes (see, for instance, Gallagher 2015). Both were acceptable acts of state. However, there were also fears that the Chinese would sell such data into the black market allowing criminals to use it for identity theft and other scams. Indeed, OPM reacted to the theft by offering 22 million individuals free access to credit monitoring services (Abel 2015).

To date, there is scant indication that the Chinese have handed such information over to cyber criminals, and no such information has been reported as found being traded within cybercrime markets. But whereas the Chinese government and Chinese cyber criminals are distinct, in other countries the division between national security and crime is gauzier. There is a constant exchange of information and perhaps other resources between the Russia's intelligence agencies and their cyber *mafiya* (see, for instance, Kramer 2017). And if reports are true that the theft of $81 million from the Bangladesh Bank was carried out by the government of the Democratic People's Republic of Korea, then at least one government is no stranger to cybercrime as such (Lyngaas 2016).

Russia may be the test case for such a norm, because of the difficulty that outsiders have in distinguishing the actions of official state intelligence organizations (the FSB and the GRU) from those of cyber criminals. Reportedly, the latter have avoided prosecution and extradition, so long as their victims are not Russian (Schwartz 2016), in part because they have been willing to lend their services to the state (Schwirtz 2017). The indictment of Russian FSB officials for the criminal hack of Yahoo is further indication of such entanglement (Nakashima 2017). In the end, there may be little valid distinction between state-paid cyber espionage in the service of crime and state-condoned hackers carrying out cyber espionage for criminal purposes.

The whole affair introduces a second norm on which US officials may have been prepared to act were their OPM fears founded: cyber espionage is acceptable *unless* the results are converted to criminal purposes.

4. THE NO-POLITICAL-DOXING NORM

The Russian hack of the Democratic National Committee (DNC) coupled with the delivery of such files to WikiLeaks for public posting embroiled the US presidential election and its aftermath. No serious individual in US public life has found this act to be acceptable, even if some argue that the content of the posted material deserved more attention than the question

6 "Don't blame the Chinese for the OPM hack," former NSA and CIA Director Michael Hayden said, arguing that he "would not have thought twice" about seizing similar information from China if he had the chance (Ferraro 2015). Director of National Intelligence James Clapper echoed the sentiment, saying at a recent conference: "You have to kind of salute the Chinese for what they did. [...] If we had the opportunity to do that [to them], I don't think we'd hesitate for a minute" (Sciutto 2015).

of how it was brought to attention. Many voices (even on the dovish half of the spectrum[7]) have argued in the subsequent months that the US failure to respond would only encourage the Russians to continue, referring to the several key European elections in 2017 subject to similar influence.

Distinctions have been drawn over how the take from the DNC hack can and cannot legitimately be used. John Brennan, the Director of Central Intelligence, has said that while spying on each other's political institutions is fair game, making data public – in true or altered form – to influence an election was a new level of malicious activity, far different from ordinary spy vs. spy maneuvers (Sanger 2016).

So, what exactly is it that is objectionable – and something that the United States, itself, would be willing to forego in the course of persuading others to do likewise?

To be clear, the DNC hack was *not* vote-tampering, even if it raised the odds that Russia, as a rogue player in the international system armed with first-rate hackers, might try its hand at the game. This was a real fear, given the pervasive use of potentially vulnerable electronic voting systems (Barrett 2016). President Obama warned Russia against tampering with voting systems in a private meeting with President Putin in September 2016 (Landler and Sanger 2016). That noted, vote-tampering is a cyber attack (in the sense that it could disrupt the voting practice or corrupt the results), while the DNC hack was an example of cyber espionage. No new norms were needed to warn Russia against vote-tampering. But new norms would be needed to properly condemn what happened to the DNC.

But what norm, exactly, would have been violated by the DNC hack and the DNC's subsequent doxing? Was it that countries should abjure from influencing elections in other countries? This precept is probably not the place to make a stand.[8] Perhaps prudence dictates that the United States not influence an electorate against voting for someone who then goes on to win anyway. Yet if intervention can make a difference, it may be a chance worth taking. President Obama did speak against both Brexit and Scottish independence. Other foreign leaders have expressed opinions about the US Presidential Election of 2016. One might propose a norm based on not breaking the laws of the country holding the election, but laws vary greatly between countries. Some of these laws (e.g. those restricting the freedom of expression) may strike the United States as illegitimate; breaking them is a good not a bad thing. A problem with limiting such a norm to political processes carried out by elections is a pronounced lack of appeal to countries that do not have elections, or those who maintain elections only for the sake of appearances.

7 "Any response from the Obama administration or the FBI will be viewed through this partisan lens, especially because the president is a Democrat. We need to rise above that. These threats are real and they affect us all, regardless of political affiliation. That this particular attack targeted the DNC is no indication of who the next attack might target. We need to make it clear to the world that we will not accept interference in our political process, whether by foreign countries or lone hackers" (Schneier 2016). "This is not just about the United States, it is not just about Trump or Clinton, or just about American democracy," said Thomas Rid, a professor of security studies at King's College London. "If they consider this a success, they may conclude that, 'Of course, we can do this elsewhere. We can do this again. We can probably also find things, *kompromat*, on the next president'" (Taub 2016).

8 "On the other hand, the United States has frequently and unapologetically intervened in other countries' elections. In Latin America, the Middle East, or Eastern Europe, this intervention has been open or covert, ranging from funding pro-democracy organizations and providing training to political leaders to handpicking candidates to install in power. In these interventions, the United States certainly uses products of the intelligence agencies" (Gessen 2016).

Perhaps the relevant norm is to not tamper with political processes in general. But the United States and its friends not only hold that elections have a legitimacy other processes may lack, but that their outcomes can be very sensitive to otherwise minor influences. Furthermore, such processes are subject to a myriad of influences. The revelation of the Panama papers – which Russians blame on the United States – shows how events in one country can affect the political processes of many distant countries (e.g., Iceland, Ukraine, Pakistan) (Rutinsky and Arkhipov 2016).[9]

Hence, if one would write a norm that makes the Russian DNC hack unacceptable, it cannot easily rest on a general prohibition against political interference, but against the yoking of a currently accepted practice (cyber espionage) to a problematic practice (unwarranted influence in another country's political processes). In other words, to be on safe ground, such a norm could be about the misuse of cyber espionage. Given the US discomfort with Russian operations on the Soros Foundation (Hattem 2016) or the World Anti-Doping Agency (WADA) (Goodin 2017) that resulted in the public release of thousands of documents, perhaps the norm could be generalized: it is unacceptable for states to acquire materials by cyber espionage and release them to the public for doxing.

But such a norm comes with costs to other US values. What differentiates doxing from whistle-blowing? The Russians could easily argue that activities of the Soros Foundation or WADA[10] which they considered anti-Russian were those that *should* have been brought to light (although inserting fake documents into the mix of released files hardly helps their case). The Snowden revelations – and more recently the Vault7 disclosures from WikiLeaks – are variously put in either basket. Furthermore, is it necessarily in the interests of the United States – which is largely an open society where certain types of disclosure are not only encouraged but mandated (see its Freedom of Information Act) – to press for norms that protect the leaders of closed societies from disclosures, particularly those with high levels of corruption that *ought* to be exposed?[11] The penetration of the *New York Times'* network by the Chinese in late 2012 was carried out because the newspaper had revealed the $2 billion dollar fortune of China's premier (Barboza 2012). In a slightly different universe where it was US government-conducted cyber espionage rather than journalistic "shoe-leather" that brought the information to the *New York Times*, which government would have been the more irresponsible: the United States for carrying out cyber espionage to gather the information, or the Chinese for carrying out cyber espionage to figure out where the information came from? Could a norm in which governments collectively pledge to keep everyone else's secrets be viewed as an international "conspiracy" to permit government corruption? So, while a norm against using cyber espionage to support doxing may nevertheless be worthwhile, it does have to be written carefully.

Many countries, especially those with limited cyber espionage capabilities, may well sign up to such a norm. Agreement may be possible even from China, whose willingness to curb economic cyber espionage suggests that they see valid limits to stealing information. Their assent is more likely if China gets to help write the norm – one of China's objections to the Budapest Convention is that it had no say in its drafting.

9 Perhaps the DNC hack was Putin's revenge for doing so (see Hamburger and Nakashima 2016; Golodryga 2016).

10 But the Russian tune has changed (see Ruiz 2016).

11 See, for instance, Thomas Friedman's fantasy of the CIA exposing Putin's corruptly-acquired billions (Friedman 2016).

Getting the assent of Russia, whose recent behavior is what has spurred such consideration, will be a major hurdle, unless its leadership signs up in the blithe belief that it can still do what it wants as long as it can deny having done so. Or Russia may realize it has more to fear from an aggressive use of cyber espionage-plus-doxing than it has to gain by doing it to others.[12] Russia, after all, is a country in which corruption and censorship are rife; for instance, its 2014 blogger law (Birmbaum 2014) is increasingly relied upon to forestall stories that the state does not want to see. Cyber espionage can reveal the former, and other cyber tricks can be used to move information into the flow of news accessible to Russians. Russia also has a long history of using *kompromat* to discredit (political) enemies. Because the legitimacy of Russia's government rests on popular approval of its leaders rather than popular approval of the process by which leaders are selected (a role, for instance, played by the US Constitution), it is far more open to question.

In any case, the US reaction to the DNC hack introduces a third norm: cyber espionage is acceptable *unless* the results are used publicly for political influence operations.

Put all three norms together, and the United States is edging towards a norms regime that allows countries to carry out cyber espionage *as long as* the results are used in a "professional" manner: that is, to foster a country's national security by influencing the decisions that the governments which collected the information make and facilitating their ability to carry them out. The results have to be kept in-house (or shared with allies to keep in-house), as US intelligence agencies do. They cannot be provided to commercial enterprises, criminals, or to the public.

But would the effort to sanction certain uses of cyber espionage be limited to those three categories? Perhaps not.

5. PEACETIME CYBER ESPIONAGE AGAINST CRITICAL INFRASTRUCTURE

Michael Hayden, formerly the NSA's director, said, "ideas have been raised about forming the cyber equivalent of demilitarized zones for sensitive networks, such as the power grid and financial networks, that would be off-limits to attack from nation states" (Zetter 2010). There are indications from the Chinese that they would be receptive to such a deal using the non-aggression pact in cyberspace that Russia and China inked in 2015 as precedent (see Ostroukh and Lyngaas 2015). Indeed, in late 2015, the UN Group of Governmental Experts (to which China belongs) agreed: "a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure" (United Nations 2015; see also Grigsby 2015). Unfortunately, as with any agreement not to engage in certain activities characteristic of war (as a serious attack on infrastructure could be considered), enforcement by punishment is unlikely to take place while war or warlike activities

12 And from the US perspective, Russia has made enough enemies to lift the burden of cyber espionage from its own shoulders. "Ukrainian hackers behind recent Kremlin email leaks said on Thursday they planned to release more information taken from accounts linked to senior Russian officials, including to President Vladimir Putin's chief spokesman. A network of Ukrainian hacking groups, called the Cyber Alliance, has been releasing emails they say were sent to one of Putin's top advisers - a bid to disprove Russia's denial it has stoked separatism in eastern Ukraine and played a direct role in the 2-1/2-year-old conflict there" (Prentice and Chornokondratenko 2016).

ensue. At that point, treaties would be less compelling and considerations of escalation control (if we do X, they might do X or even Y) would likely be the more relevant influence on each combatant's actions. Thus, the rules provide little real inhibition to bad behavior.

Yet, because cyber espionage is almost always a pre-requisite for cyber attack, particularly if implants are used, making it difficult to carry out *peacetime* cyber espionage can retard or inhibit wartime or warlike cyber attacks, at least in the first few weeks and months of conflict (that is, until new entryways into the target systems are found or developed). Even better, countries that abjured cyber espionage would have a hard time coercing others by threatening immediate cyber attacks on critical infrastructure without at the same time admitting that their word not to carry out (prefatory) cyber espionage on critical infrastructure was worthless. Thus, a serious norm (in the sense of a norm whose violation brings serious repercussions) prohibiting attacks on critical infrastructure or threats thereof could require banning cyber espionage on each other's infrastructure. This linkage is understood in both Washington DC and Beijing.

Because the aim is to ban activity *before* its consequences are manifest, this norm agreement requires some mechanism to find violations: to attribute as well as detect system intrusions, as well as to distinguish deliberate infection from random malware drift. Any such monitoring mechanism must pass three tests. One is getting attribution right. Two, more importantly, is to build a good case for what happened so that it can convince skeptics. Three, most importantly, is to present the case so that the accused accepts the results as fairly derived and not arbitrary (the process of attribution need not be resolved in every case as long as it resolves often enough to inhibit cheating[13]). Similarly, the process cannot be so stringent that victims of cyber espionage, who may have access to information that they will not or cannot pass forward, conclude that they need other ways to press the point with the accused.

Part of the political problem of enforcement from the perspective of China (and perhaps also Russia) is that the United States catches a much greater share of others' spying than the others catch of US government spying. Consider that all of the Snowden revelations about overseas cyber espionage were new, in that there was no example that *confirmed* a discovery of a specific cyber espionage case linked to the United States.[14] Putatively, any process that produces similar results may be viewed as deeply biased *even if accurate*. China's ability to detect and attribute cyber espionage from the United States, for instance, is far lower than the US ability to detect and attribute cyber espionage from China; there has simply been no equivalent of the 2013 Mandiant report. This arises from three differences. First, China's operational security lags behind US operational security, making Chinese spying easier to detect.[15] Second, China's ability to detect intrusions (especially from the US Government) lags behind the US ability

13 Not all attribution evidence is publicly releasable (see Sanger and Fackler 2015). This suggests an unbridgeable difference between the confidence that US officials place in attribution and the confidence felt by a fair-minded individual working from open sources, but unwilling to take the word of US sources at face value.

14 Since Snowden, one cyber security firm, Kaspersky, has uncovered what it called 'Regin' malware possibly linked to the United States (Kaspersky 2014) and the work of the Equation Group, probably linked to the United States (Kaspersky 2015).

15 From Segal (2016, p. 113): "Security analysts consider the Chinese particularly noisy in networks, especially compared to the Russians". Part of how one can tell good operational security is to see which intrusion sets attributed to each country have gone undetected for more than, say, five, years before being eventually detected.

to detect intrusions. Third, China's ability to attribute detected intrusions lags behind the US ability[16] to attribute detected intrusions.

As long as all three are true, will the Chinese (or, correspondingly, the Russians or Iranians) accept that compliance verification would be even-handed? Until the Chinese and others gain confidence in their own attribution capabilities, they may not even believe that US attribution capabilities are good enough; those caught spying may believe that they have been fairly caught but unless they tell others, China's policy-making community may retain their skepticism.

How might an attribution process merit trust? One could start with a multi-national body which, like the US National Transportation Safety Board (NTSB), focuses on characterizing a cyber espionage hack rather than assigning guilt for it. At the very least, such a body may permit examining evidence that a system's penetration was accidental (e.g., malware found in one system could have drifted over from another) or, if purposeful, may not have had prohibited intent. The International Atomic Energy Agency (IAEA) or the International Civil Aviation Organization (ICAO) may provide other models that can be used to build multi-lateral and highly technical examinations of norms violation. Microsoft has suggested that such a group be characterized by strong technical expertise, diverse geographic representation and peer review and the group should only undertake analyses for significant events (Charney et al. 2016). Since most cyberspace forensic authorities spend much of their career with their respective governments, it may be a challenge for professionals of one side to trust their foreign counterparts. Those from the West may consider Chinese or Russian representatives beholden to their governments and thus unlikely to be given enough latitude to offer an independent perspective. The Russians and the Chinese may, in turn, argue that US experts are comparably beholden themselves *and* would also have so much more background at making attribution as to reduce their own experts to spectators. Yet there are grounds for believing that working together for long enough can alleviate much of the unwarranted mistrust.

Conversely, might the Chinese and others be more forthcoming if they understood the mechanisms of attribution better?[17] If so, would the prospect of winning an agreement from the Chinese and others on norms be sufficiently attractive to justify the US teaching (or sending third parties to teach) others *some* of its forensic attribution techniques? Would the Chinese and others then be willing to credit such techniques as evidence of verification? An ancillary benefit is that stronger Chinese attribution capabilities could reduce the chances of a catalytic conflict in which China is attacked by someone masquerading as a US source. At first glance, this notion appears untenable: countries do not teach others such technology. Yet the United States encourages other countries to adopt permissive action links (PALs) for their nuclear weapons so that such weapons are not used accidentally or at the instigation of rogue nuclear warriors. There are also offsetting benefits when foes build enough surveillance capability to let them

16 In the United States, a large share of detection and intrusions are carried out by private companies (many of whom employ former NSA employees). China is only starting to develop its own cyber security companies. That noted, it can buy cyber security expertise: even if some US companies might refuse Chinese business, cyber security companies from beyond the United States (e.g., Israel) are for hire.

17 Richard Bejtlich (2015) has testified, "When either one, or both, opponents possess low attribution capabilities, it is a less stable situation. This could be a problem with the agreement between China and the United States. Private and public teams in the United States can perform high levels of attribution on Chinese activity. Private and public teams in China do not share the same capabilities at present. China could therefore suspect that the United States is behind certain hacks, although such activity could be caused by Russia or other actors. This is one reason to welcome the rise of private or nongovernment security companies in China, who may improve the country's attribution capabilities."

believe that the United States is adhering to arms deals in much the same way that aerial and later space surveillance technology assured the United States that it had little need to engage in a missile race with Russia (circa 1960). Furthermore, helping bring Chinese attribution capabilities closer to those available in the United States does not mean that the United States should be expected to teach others how to *detect* cyber espionage intrusions or how to keep their own penetrations from being *detected* by the United States.

6. PROHIBITING UNWELCOME USES OF STOLEN INFORMATION MAY MAKE CERTAIN TARGETS OFF-LIMITS

There is no clear line between prohibiting certain *targets* of cyber espionage and prohibiting specific *uses* of cyber espionage. Take the norm against industrial cyber espionage. Notionally, it would allow cyber espionage against companies for, say, purposes such as evaluating another country's capacity for developing dual-use technology (a national security rationale). In practice, it puts certain targets off-limits, because it creates a rebuttable presumption that the only good reason to spy on, say, automobile companies is to help someone compete in the automobile market. By contrast, US irritation at the threat that OPM data might find itself in criminal markets or the transfer of DNC data to WikiLeaks is *only* about the use of such data.

For some of the several potential norms discussed above, non-intelligence uses of captured data are strongly implied by the choice of targets: e.g., private corporations, or some critical infrastructure. Here, cyber espionage is indistinguishable from pre-cyber attack (and pre-coercion) preparations. As for critical infrastructure, while there seems little good reason to spy on electric grids, compromising communications nodes is almost *sine qua non* for wide-scale surveillance, while compromising financial systems helps in tracking financial crimes carried on with the connivance of unscrupulous bankers.

Nevertheless, from the perspective of the United States and its friends, the best strategy may be to insist that all prohibitions relate to post-cyber espionage uses of data rather than written as target-specific. This would foster the argument that such a form of professionalism differentiates cyber espionage carried out by the United States and its allies from the sort that should be prohibited. More importantly, if the collection of norms turns out to be a package deal, such a stance could inhibit this package from becoming a collection of unrelated items. Again, it would be understood, even if not stated outright, that evidence of cyber espionage within certain systems is a *prima facie* case of cyber espionage for the wrong reasons. So, in practice, there would essentially be a prohibition on spying on certain classes of target. But policy coherence helps in making the case for a broad set of prohibitions.

7. MAKING NORMS HAPPEN

Norms-setting is a deliberative process, but not necessarily multilateral. The United States, after all, could declare a set of red lines, call them norms if it pleases, and then warn others against

violating them lest they face punishment. Or, it could take the trouble to work out norms with other countries, which would be accepted as norms by others, not only because the United States says so but because other countries agree they merit approval and they have had a hand in the process by which norms were generated and agreed to.

Working from red lines and unilaterally calling them norms means that the United States recognizes the norms it wants and only those norms; no concessions are needed. Working with others offers two advantages, though. First, it forces the advocates of norms to be explicit about what behavior is proscribed, and why. Second, any result is more likely to get buy-in from other countries; the same benefit applies to getting buy-in for a US response to a violation of such norms. Conversely, the negotiations path is slower to finish than the unilateral route (which, in turn, is slower than the after-the-fact reaction route). And even negotiations exclusively with US friends may force the United States to make compromises over what is unacceptable behavior (European countries, for instance, tend to favor stronger privacy protections than those of US law) and perhaps even what criteria are used to determine that the behavior of a given country is unacceptable.

The process may not necessarily generate norms all of which the United States would feel totally comfortable with – although the package, on the whole, very well might (otherwise they will not gain US assent). The United States is likely to fight back against any package that goes beyond cyber espionage norms to include demands from other countries (e.g., on Internet governance or legitimizing censorship to "protect" cyberspace). The prospect that such a package is focused on cyber espionage alone rests on a reasonable presumption that some countries see value in constraining US cyber espionage operations, in large part because they fear that the United States is very good at carrying them out.

Finally, as far as norms without monitoring (let along consequences) are but sweet sentiments, the case for cyberspace norms has always been fraught (Roth 2016), although attribution has got better (Panetta 2012; Rid 2014 has a nice explanation of some of the techniques used). The Xi-Obama agreements appear to have worked so far without any formal compliance mechanism,[18] although as a rule multilateral agreements may require more compliance mechanisms than bilateral ones, in part because one side can quit the agreement if it deems it being violated by the other side, but in a multilateral agreement the party that leaves may be hurting itself more than it hurts the cheater. Yet foreign governments, which generally have weaker attribution capabilities than the United States does, may fear signing up to a cyber espionage norm that the United States, but only the United States, can police. In some cases, the *use* of the information gained from cyber espionage – e.g., a threat made against critical infrastructure – can provide sufficient evidence. Conversely, if attribution for cyber espionage is adequate, determining that data has been misused is often straightforward. For instance, if Chinese culpability for the OPM hack is certain, then finding this data on the black market means that China must have put it there, or managed it in ways that allowed it to get there. Similarly, if one knows for certain that Russia took the DNC's e-mails, then similar conclusions can be reached by observing that these e-mails ended up on WikiLeaks *even if* a transmission chain cannot be proven.

18 This is the consensus of many observers (see, for instance, Lynch 2016).

By focusing on what uses can properly be made of information acquired by cyber espionage, the United States and its friends can make progress on the challenging issues of developing a favorable package of norms and finding ways to monitor compliance.

8. CONCLUSIONS

The premise that cyber espionage (like physical espionage) is acceptable state activity has become increasingly untenable. The United States has won support for norms against economically-motivated cyber espionage, pushed back against the use of cyber espionage for political doxing, and was prepared to condemn the transfer of information from state-sponsored cyber espionage into cybercrime markets. These three examples suggest that countries look seriously at what sorts of cyber espionage should and should not be deemed acceptable. Further norms are possible, not least of which are those against cyber espionage for the purpose of implanting attacks into critical infrastructure, although the challenge of determining the *purpose* of an implant only adds to the challenges of determining who put them there.

This paper has suggested a normative framework in which cyber espionage is *unacceptable* unless the results are used *only* to inform national-security decision-making. Left open with this formulation is whether cyber espionage can be used to open the door for cyber attacks (e.g., via implants) – particularly cyber attacks on critical infrastructure. Further research can be used to refine the definitions of norms, explicate the interests of the various stakeholders in the norms formation process, and develop monitoring methods that can meet the twin tests of being accurate and accepted.

REFERENCES

Abel, Jennifer, "OPM hack fallout: feds pay $133 million for (largely useless) ID theft monitoring services," *Consumer Affairs*, September 9, 2015. https://www.consumeraffairs.com/news/opm-hack-fallout-feds-pay-133-million-for-largely-useless-id-theft-monitoring-services-090915.html.

Barboza, David, "Billions in Hidden Riches for Family of Chinese Leader," *New York Times*, October 25, 2012. http://www.nytimes.com/2012/10/26/busainess/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html.

Barrett, Brian, "America's Electronic Voting Machines are Scarily Easy Targets," *Wired*, August 2, 2016. https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

Bejtlich, Richard, "Outside perspectives on the Department of Defense cyber strategy," Testimony before the US House of Representatives Committee on Armed Services on September 29, 2015.

Birmbaum, Michael, "Russian blogger law puts new restrictions on Internet freedoms," *Washington Post*, July 31, 2014. https://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html?utm_term=.c2501c618038.

Charney, Scott, Erin English, Aaron Kleiner, Angela McKay, Nemenja Malisevic, Jan Neutze, and Paul Nicholas, 2017. *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*. https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf.

Clapper, James R., Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, September 8, 2013. https://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economicespionage.

Detrow, Scott, "Obama on Russian Hacking: 'We Need to Take Action. And We Will'," *NPR News*. December 15, 2016. http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will.

Dilanian, Ken, "Russia May Be Hacking Us More, But China Is Hacking Us Much Less," *NBC News*, October 12, 2016. http://www.nbcnews.com/news/us-news/russia-may-be-hacking-us-more-china-hacking-us-much-n664836.

Economist, "Admit nothing and deny everything," June 8, 2013. http://www.economist.com/news/china/21579044-barack-obama-says-he-ready-talk-xi-jinping-about-chinese-cyberattacks-makes-one.

Ferraro, Matthew F., "On the OPM Hack, Don't Let China Off the Hook," *The Diplomat*, July 14, 2015. http://thediplomat.com/2015/07/on-the-opm-hack-dont-let-china-off-the-hook/.

Friedman, Thomas, "Let's Get Putin's Attention," *New York Times*, October 5, 2016. http://www.nytimes.com/2016/10/05/opinion/lets-get-putins-attention.html.

Gallagher, Sean, "China and Russia cross-referencing OPM data, other hacks to out US spies," *Ars Technica*, August 31, 2015. http://arstechnica.com/security/2015/08/china-and-russia-cross-referencing-opm-data-other-hacks-to-out-us-spies/.

Gessen, Masha, "Arguing the Truth with Trump and Putin," *New York Times*, December 17, 2016. http://www.nytimes.com/2016/12/17/opinion/sunday/arguingthetruthwithtrumpandputin.html.

Goodin, Dan, "US athletes' doping tests published by Russian hackers, agency says," *Ars Technica*, September 13, 2016. http://arstechnica.com/security/2016/09/anti-doping-agency-pins-leak-of-us-gold-medalists-data-on-russian-hackers/.

Golodryga, Bianna. "3 Major Implications of the Panama Papers Leak," *Huffington Post*, April 21, 2016. http://www.huffingtonpost.com/bianna-golodryga/3-major-implications-of-t_b_9748512.html.

Grigsby, Alex, "The 2015 GGE Report: Breaking New Ground, Ever So Slowly," *Council on Foreign Relations Guest Blog*, September 8, 2015. http://blogs.cfr.org/cyber /2015/09/08/the-2015-gge-report-breaking-new-ground-ever-so-slowly/.

Hamburger, Tom and Ellen Nakashima, "Clinton campaign — and some cyber experts — say Russia is behind email release," *Washington Post*, July 24, 2016. https://www.washingtonpost.com/politics/clinton-campaign--and-some-cyber-experts--say-russia-is-behind-email-release/2016/07/24/5b5428e6-51a8-11e6-bbf5-957ad17b4385_story.html.

Harold, Scott, Martin Libicki, and Astrid Cevallos, 2016, *Getting to Yes with China in Cyberspace*, Santa Monica CA (RAND).

Hattem, Julian, "Thousands of Soros docs released by alleged Russian-backed hackers," *The Hill*, August 15, 2016. http://thehill.com/policy/national-security/291486-thousands-of-soros-docs-released-by-alleged-russia-backed-hackers.

Haynes, Deborah, "Russia waging cyberwar against Britain," *The Times*, December 17, 2016. http://www.thetimes.co.uk/edition/news/russiathreattobritaingpd98bz83.

Kaspersky Lab, "Regin: a malicious platform capable of spying on GSM networks," November 24, 2014. http://www.kaspersky.com/about/news/virus/2014/Regin-a-malicious-platform-capable-of-spying-on-GSM-networks.

Kaspersky Lab, "Equation Group: The Crown Creator of Cyber-Espionage," February 16, 2015. http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber espionage.

Kramer, Andrew, "Top Russian Cybercrimes Agent Arrested on Charges of Treason," *New York Times*, January 25, 2017. https://www.nytimes.com/2017/01/25/world/europe/sergei-mikhailov-russian-cybercrimes-agent-arrested.html.

Landler, Mark, and David Sanger, "Obama Says He Told Putin: 'Cut It Out' on Hacking," *New York Times*, December 26, 2016. https://www.nytimes.com/2016/12/16/us/politics/obama-putin-hacking-news-conference.html.

Lynch, David, and Geoff Dyer, "Chinese Hacking of US Companies Declines," *Financial Times*, April 13, 2016. http://www.ft.com/cms/s/0/d81e30de-00e4-11e6-99cb-83242733f755.html.

Lyngaas, Sean, "Debating the Sino-Russian cyber pact," *Federal Computer Week*, May 12, 2015. http://fcw.com/articles/2015/05/12/russian-chinese-cyber.aspx.

Lyngaas, Sean, "Symantec traces Swift banking hacks to North Korea," *Federal Computer Week*, May 31, 2016. https://fcw.com/articles/2016/05/31/swift-hack-dprk.aspx.

Mandiant, APT1, *Exposing One of China's Cyber Espionage Units*, March 2013. sintelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Marks, Joseph, "US-China Cyber Dialogue to Continue Under Trump," *Nextgov*, December 9, 2016. http://www.nextgov.com/cybersecurity/2016/12/us-china-cyber-dialogue-continue-under-trump/133782/.

Nakashima, Ellen, "Treasury and Justice officials pushed for economic sanctions on China over commercial cybertheft," *Washington Post*, December 27, 2016. https://www.washingtonpost.com/world/national-security/2016/12/27/fc93ae12-c925-11e6-8bee-54e800ef2a63_story.html.

Nakashima, Ellen, "Justice Department charging Russian spies and criminal hackers in Yahoo intrusion," *Washington Post*, March 15, 2017. https://www.washingtonpost.com/world/national-security/justice-department-charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html.

Ostroukh, Andrey. "Russia, China Forge Closer Ties With New Economic, Financing Accords: Moscow turns to Asian investors to reduce reliance on Europe and the U.S. amid standoff over Ukraine," *Wall Street Journal*, May 8, 2015. http://www.wsj.com/articles/russia-china-forge-closer-ties-with-new-economic-financing-accords-1431099095.

Panetta, Leon E., "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," October 11, 2012; http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Poplin, Cody, "Cyber Sections of the Latest G20 Leaders' Communiqué," *Lawfare Blog*, November 17, 2015. https://www.lawfareblog.com/cyber -sections-latest-g20-leaders-communiqué.

Prentice, Alessandra and Margaryta Chornokondratenko, "Ukrainian Hackers Promise Leaks on Putin Spokesman," *Reuters*, November 4, 2016. http://in.reuters.com/article/ukraine-crisis-cyber -russia-idINKBN12Y2P5.

Rid, Tomas and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, 2014.

Romero, Simon, "N.S.A. Spied on Brazilian Oil Company, Report Says," *New York Times*, September 9, 2013. http://www.nytimes.com/2013/09/09/world/americas/nsa-spied-on-brazilian-oil-company-report-says.html.

Roth, Andrew, "How the Kremlin is sure to keep its fingerprints off any cyberattack," *Washington Post*, August 2, 2016. https://www.washingtonpost.com/world/europe/how-the-kremlin-is-sure-to-keep-its-fingerprints-off-any-cyberattack/2016/08/02/26144a76-5829-11e6-8b48-0cb344221131_story.html.

Ruiz, Rebecca, "Russians No Longer Dispute Olympic Doping Operation," *New York Times*, December 27, 2016. http://www.nytimes.com/2016/12/27/sports/olympics/russia-doping.html.

Rudnitsky, Jake and Ilya Arkhipov, "Putin Sees US, Goldman Sachs Behind Leak of Panama Papers," *Bloomberg.com*, April 14, 2016. https://www.bloomberg.com/news/articles/2016-04-14/putin-sees-u-s-goldman-sachs-behind-leak-of-panama-papers.

Sanger, David, "U.S. wrestles with how to fight back against cyberattacks," *New York Times*, July 31, 2016. http://www.nytimes.com/2016/07/31/us/politics/us-wrestles-with-how-to-fight-back-against-cyber attacks.html.

Sanger, David and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *New York Times*, January 19, 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

Sanger, David and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2014. http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

Schneier, Bruce, "NSA Hacking of Cell Phone Networks," *Lawfare Blog*, December 8, 2014. https://www.lawfareblog.com/nsa-hacking-cell-phone-networks.

Schneier, Bruce, "Hacking the Vote," *Schneier on Security*, August 1, 2016. https://www.schneier.com/blog/archives/2016/08/hacking_the_vot.html.

Schwartz, Matthew, "Russia: 7-Year Sentence for Blackhole Mastermind (Jail Time for Russian Cybercriminals is Rare)," Bankinfosecurity.com, April 15, 2016. http://www.bankinfosecurity.com/notorious-blackhole-exploit-kit-author-sentenced-a-9048.

Schwirtz, Michael and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," *New York Times*, March 12, 2017. https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.

Sciutto, Jim, "Director of National Intelligence blames China for OPM hack," *CNN*, June 25, 2015. http://www.cnn.com/2015/06/25/politics/james-clapper-china-opm-hacking/.

Segal, Adam, *The Hacked World Order*, 2016. New York NY (Public Affairs).

Taub, Amanda, "D.N.C. Hack Raises a Frightening Question: What's Next?" *New York Times*, July 29, 2016. http://www.nytimes.com/2016/07/30/world/europe/dnc-hack-russia.html.

United Nations, General Assembly, A/68/98, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

United Nations, General Assembly, A/70/174, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, July 22 2015 p. 2. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

White House (2015a), Executive order, April 2, 2015. https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

White House (2015b), "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.

Williams, Katie Bo, "Dems urge Obama to release info on Russian links to DNC hack," *The Hill*, July 27 2016. http://thehill.com/policy/national-security/289485-intel-dems-urge-obama-to-release-info-on-russian-involvement-in-dnc.

Zetter, Kim. “Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible,” *Wired*, July 29, 2010. http://www.wired.com/2010/07/hayden-at-blackhat/.