



March 1, 2017

Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities

Committee on Armed Services, United States House of Representatives,
One Hundred Fifteenth Congress, First Session

HEARING CONTENTS:

Witnesses

Jason Healey
Nonresident Senior Fellow, Cyber Statecraft Initiative
Atlantic Council
[View Testimony](#)

Martin C. Libicki
Adjunct Management Scientist
RAND Corporation
[View Testimony](#)

Peter Singer
Strategist and Senior Fellow
New America Foundation
[View Testimony](#)

Available Webcast(s)*:

[Full Hearing](#)

Compiled From*:

<https://armedservices.house.gov/legislation/hearings/cyber-warfare-21st-century-threats-challenges-and-opportunities>

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*

Healey – Testimony to HASC, 1 March 2017

Testimony of

Jason Healey

Columbia University's School Of International and Public Affairs

Saltzman Institute of War and Peace Studies

Before the

United States House of Representatives

Committee on Armed Services

Hearing on

“Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities”

1 March 2017

Testimony of Jason Healey

Chairman Thornberry, Ranking Member Smith, and distinguished Members of the Committee, thank you for the honor of testifying before you today on the topic of cyber conflict. I am humbled to be here before you today on a topic of such importance.

Our adversaries will continue to use cyber means to challenge American power and our citizens, as it offers significant opportunities for our adversaries, as will be clear from this selection of quotes.

A pioneering expert, Dr. Cliff Stoll, who started his cybersecurity work at one of our national labs, has noted that “[e]spionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations ... [while the perpetrators are] insulated from risks of internationally embarrassing incidents,” and “the almost obsessive persistence of serious penetrators is astonishing.”¹

This persistence has certainly been clear when it comes to cyber espionage. The National Counter Intelligence Center reported to Congress that “the largest portion of economic and industrial information lost by US corporations” is due to “computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses.”² Previous testimony to the House of Representatives has furthermore made it clear that “[g]overnment and commercial computer systems are so poorly protected today they can essentially be considered defenseless - an Electronic Pearl Harbor waiting to happen.”³

Cyber threats are real and getting worse every year, but they are not as new as we think. Each of the previous quotes were made about 25 years ago, if not longer. We have been warning about an electronic Pearl Harbor for 25 of the 75 years since the actual Pearl Harbor; there is a good chance we don’t understand the dynamics of cyber conflict as much as we think.

I was the action officer at Headquarters Air Force to help stand up the first joint cyber warfighting command, the Joint Task Force - Computer Network Defense in 1998 and was one of the initial cadre of twenty-five officers. In that time, the central questions and concerns have remained largely the same, even as the risks have grown immeasurably.

¹ Dr Cliff Stoll, “Stalking the Wily Hacker,” 1988, <http://pdf.textfiles.com/academics/wilyhacker.pdf>.

² NACIC Counterintelligence Report to Congress, July 1995, <https://fas.org/sgp/othergov/indust.html>.

³ Winn Schwartau, testimony to House Committee on Science, Space, and Technology, 27 June 1991, <https://babel.hathitrust.org/cgi/pt?id=pst.000018472172>.

Adversaries

America's adversaries in cyberspace and their motivations are no different than in the physical world: Russia acts because it *lost*, China because it is *behind*, Iran because it is *revolutionary*, North Korea because it is *starving*, and terrorists because they *hate*.

Russia to a large degree remains driven by having lost the Cold War, trying to carve out a sphere of influence in its near abroad and working to undermine the transatlantic victors, the United States, Europe, and the NATO structure that unites both. Since annexing Crimea, Russian cyber operations have gone from quiet, professional political and military espionage to far more aggressive and obvious intelligence and influence operations.

China feels preyed upon by Western powers since the unequal treaties of the mid-1800s. Because China has been unfairly kept down by the West, they believe, anything is permitted to catch back up. For most of the past fifteen years, this meant widespread and aggressive espionage for commercial purposes. It now seems that such espionage has fallen off dramatically, at least in part because of a 2015 agreement by President Obama and President Xi.⁴ Should relations with China become more troubled, such as over trade or the South China Sea, we should expect a fresh bout of troublemaking.

Iran continues to see itself as a revolutionary power and this extends into cyberspace as well. Of America's adversaries, Iran has been the most persistent conducting disruptive attacks meant to disrupt US companies and infrastructure, especially banks. Fortunately, as with China, the larger improving diplomatic situation with the United States has helped to throttle back the worst offenses. Since the nuclear agreement was signed, Iranian behavior is reported to be less disruptive, instead focusing on traditional political and military intelligence. Should the deal unwind, Iran would almost certainly act out using a wide range of means, including cyber disruption.

North Korea is starving, both in the literal sense of being poor as well as feeling starved of attention. Cyber capabilities, such that used against Sony Motion Pictures, is a way for the North Koreans to actualize their tantrums as well as have a direct, though limited, impact in South Korea and United States. North Korea knows it cannot keep pace with American and South Korean military capabilities, so cyber sabotage offers unique benefits, as does cybercrime to raise hard currency. Even so, their behavior often closely matches the overall diplomatic environment. Whenever Pyongyang walks away from Panmunjom or has fresh sanctions slapped on it, expect a cyber outburst.

Terrorists would not hesitate to use cyber capabilities if it offered an easy way to act out their hatred. Fortunately, terrorist groups have so far been more of a target of US cyber capabilities than a source of significant attacks. One reason is that it has been historically easy to take down

⁴ For example, see the FireEye report, "Red Line Drawn," June 2016, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf> and comments by John Carlin confirming the change in "U.S. Cyber Deal With China Is Reducing Hacking, Official Says," 28 June 2016, <https://www.bloomberg.com/news/articles/2016-06-28/u-s-cyber-deal-with-china-is-reducing-hacking-official-says>.

a target in cyberspace but hard to keep it down in the face of determined defenses which imposes a relatively high threshold which remain beyond what terrorists can build (or buy). A cyber takedown of France's TV5 appeared to be the beginning of serious cyber terrorism but was, in fact, Russian government hackers.⁵

Defense and Deterrence

With respect to traditional concepts of defense and deterrence, five issues stand out: what isn't a problem, how do we respond, what's most different, what we didn't see coming, and what we might most have wrong. I'm pleased to say that my colleague Professor Robert Jervis and I have been selected for a grant to further study these issues by the Minerva program of the Department of Defense.

What isn't a problem? Attribution is not nearly the challenge anymore that it used to be. Analysts at cybersecurity companies like CrowdStrike and FireEye as well in the US government have made tremendous gains in determining – relatively quickly and with high confidence – what nations are responsible for cyber attacks. As my colleague at Columbia University, Professor Steve Bellovin, points out, analysts have a deep “knowledge base and continuity of contact” spanning over a decade. The remaining challenge is having enough releasable information to convince a skeptical public and having an effective set of policy responses against the nation responsible.

How do we respond? I am also not terribly concerned that the US government has not stated more clearly what might constitute an act of war in cyberspace. Even though we have worried about a Pearl Harbor scenario for 25 years, no nations have used cyber capabilities to kill Americans or to cause destruction or more than even momentary disruption. It seems clear they understand that boundary. Moreover, since 2003, the last two administrations have used varying degrees of clarity to state that the President can respond to cyber incidents with any means of national power.⁶

Moreover, defining forbidden behavior is, in cyber conflict, often an unproductive errand as cyberspace offers adversaries so many possibilities. Neither the North Korean attack on Sony nor the Russian influencing of our elections crossed any of norms proposed, after much consideration, by Secretary of State John Kerry in 2015, nor those agreed to by the G-20 later that year. And unless the United States is unwilling to forego our own gray zone activities, adversaries will not be minded to back down.

We dithered for 10 years before even mentioning to the Chinese we were upset over their commercial cyber espionage. Without options for more effective and timely response, any definitions or red lines are perhaps beside the point. Response requires good enough attribution, which we have achieved, as well as the right policy tools, where more can be done. Most

⁵ Gordon Corera, “How France's TV5 was almost destroyed by 'Russian hackers',” BBC, 10 October 2016, <http://www.bbc.com/news/technology-37590375>.

⁶ Most notably, in the National Strategy to Secure Cyberspace (2003) and International Strategy for Cyberspace (2011) which both had declaratory statements.

importantly, we need to think more deeply about how our adversaries may try to attack us, develop response playbooks for such eventualities, and to create muscle memory by frequently exercising against these possibilities. Without this agility born of preparation, adversaries will bob and weave in and out of our definitions and red lines.

What's different compared to more conventional conflict? In other testimony, you have surely heard that cyber operations are different because they are at “network speed,” or operate across borders, or are so easily denied. Those things are all true, but as Putin showed us by suddenly seizing Crimea with his little green men, they are just as true in other kinds of modern warfare.

No, what is most different is in cyber defense, the private sector is the *supported* command, not the *supporting* command.

America's cyber power is not focused at Fort Meade with NSA and US Cyber Command. The center of US cyber power is instead in Silicon Valley, in Route 128 in Boston, in Redmond, Washington and in all of your districts where Americans are creating and maintain cyberspace and filling it with content the world is demanding. Our critical infrastructure companies are on the front lines of nation state attacks and our cybersecurity companies collectively have even more capabilities to defeat these threats than our military, and can do so at no cost to the public purse and with no arguments over Title 10 versus Title 50 authorities.

The government needs to better support the private sector, not try to force their compliance or deputize them to act out orders coming from the Department of Defense, Department of Homeland Security, or the White House.

Cybersecurity companies, key vendors, and many critical infrastructure companies have unique strengths: agility, subject matter expertise, and the ability to directly change cyberspace in the face of attack. These companies (as well as key non-profit and volunteer groups) are on the commanding heights of cyberspace and are already engaged in keeping it safe. Government bureaucracies cannot easily match any of these capabilities, but can bring massive resources, staying power, and additional authorities, from sanctions to arrest powers to kinetic response. The best hope for American cyber defense is to combine these strengths, not try to re-create them all at Fort Meade.

What didn't we see coming? In the wake of the 1991 Gulf War, the armed services were eager to study and dominate influence operations, so we all studied OODA loops and looked for leverage across any and all information disciplines, from public affairs, civil affairs and counter propaganda to cyber operations and electronic warfare. Even weather prediction was folded into the information operations mix.

The Sony attack and Russian release of DNC documents, the incidents which have had the most immediate national impacts, were not “cyber” as such, but influence operations. Since 2003 or so, we have been so enamored of “cyber”, of sending bits and bytes downrange for espionage or to create military effects, we've largely forgotten how to respond to what is now our adversaries'

chief weapon. The US military would have been far better prepared to respond to these 20 years ago than today. Putin has not forgotten about information operations, much to the detriment of the United States, Ukraine, and the rest of Europe.

What we might most have wrong? Deterrence remains the most poorly understood dynamic of cyber conflict, with many practitioners and theorists arguing either that it is either not working or altogether impossible. Neither of those is a complete answer, but more worryingly deterrence may be the answer to the wrong question.

Remember that the cyber establishment has been fretting about an electronic Pearl Harbor for twenty-five years. That means for twenty-five years our throats have been strategically bare to our adversaries' attacks and, assumedly, their throats have been vulnerable to ours. Yet, to my research, no one has yet died from a cyber attack. This suggests that nations are in fact showing considerable restraint, at least above the threshold of attacks which might spark a devastating response.

Cyber deterrence, above the threshold of attacks that cause death or physical destruction, not just is working, but works just like more traditional deterrence. This situation might be quiet fragile, as I will explain shortly, and believe that maintaining *stability*, reinforce the threshold below death and destruction, ought to be a higher US priority than seeking deterrence.

Where deterrence is not working, is below that threshold of death and destruction. In this grey area between peace and war, all major cyber powers – the United States included – is enjoying a free-for-all which is getting worse every year. Developments in cyber conflict are driven less by new technologies than the increasing and incredible audacity of the major cyber powers to ever more escalatory activities.

Whenever you hear a US military or intelligence official discussing the need for deterrence, it turns out they often actually mean supremacy. We want to stop the Russians, Chinese, Iranians, and North Koreans from using their cyber capabilities against us, but do not want any notable restraints on use of our grey-zone capabilities against them. Compare this to the Cold War, where we wanted a nuclear edge against the Soviets, but not so that we could actually *use* those capabilities.

Indeed, I suspect cyberspace is the most escalatory kind of conflict that humanity has ever come across. My colleague, Professor Bob Jervis, argued many years ago that escalation was “doubly dangerous” if the offense is dominant over defense and it is hard to distinguish offense from defense.⁷ Arms races were especially likely and “incentives to strike first could turn crises into wars.”

Unfortunately, the cyber domain not only is distinguished by those two characteristics of offense dominance over defense and difficulty of distinguishing the two. Cyber conflict is far more

⁷ Robert Jervis, “Cooperation Under the Security Dilemma.” *World Politics*. 1978; 30(2): 167-214, https://www.jstor.org/stable/2009958?seq=1#page_scan_tab_contents.

escalatory as it is also hard to distinguish offense from either intelligence collection or intelligence preparation of the battlefield. Cyber conflict also has a low barrier to entry and capabilities are not just stockpiled (as with nuclear or conventional weapons) but actually *used* in unattributed, covert, grey-zone attacks. Cyberspace may not just be “doubly dangerous” but perhaps “quintuply dangerous” and ripe for escalation and miscalculation.

If the United States actively pursues cyber deterrence by ever-greater offensive capabilities and larger, more-capable organizations, other nations can easily respond. Our expenditures and attempts to prevail may only make us less secure.

Worse, there is actually very little evidence of adversaries being deterred by an opponent’s fearsome cyber capabilities. But there are many examples, especially between the United States and Iran, where capabilities and operations have led to escalation. Each nation experiences a cyber outrage from the other, which is then used to ratchet up capabilities and operations, which are then used by the other nation to itself ratchet up.

I do not mean to excuse their actions, but when you hear testimony from officials that they need more resources to deal with the Iranian cyber threat, please keep in mind that in cyberspace we threw the first punch. Deterrence works very differently if your adversary is certain they are striking back, not first.

Any exercise in US cyber deterrence is best thought of as an *experiment*. As it turns out, with China the experiment of indictments and threat of sanctions seems to have been more successful than anyone imagined. We cannot take as faith that if only the United States would act in a certain way, such as by pouring money into offensive capabilities or brandishing the awesome US cyber arsenal, that adversaries will be deterred on what, to them, may be a critical national interest.

Please be very skeptical in the face of certainty, even unanimity, of officers or officials about these points. Acting more forcefully, with escalating attacks, may just be pouring gas on a fire, which will affect our Internet-enabled economy far more than our adversaries. As the examples of China and Iran seem to show us, there are other options.

Recommendations

My first recommendation is that the United States takes further steps to deal with foreign influence. Treating these as “cyber” events misses what makes them unique and brings the wrong set of experts to the table. Frankly, we would have better equipped to handle these challenges in the 1990s when forward-looking officers created doctrines, organizations, and operating concepts around information operations, not just cyber.

Even though the military are not the best choice of government agency to respond to other nations seeking to influence or undermine the US system of government, their capabilities might be built up most quickly. The Cyber Mission Force already has area-studies specialists working alongside with cyber subject matter experts. A new set of Cyber Influence Teams could be trained

and folded into this structure to provide a more integrated capability to deal with influence events.

Second, I continue to advocate splitting the leadership of NSA and US Cyber Command as soon as possible. The most obvious reason is that two large bureaucracies is one too many for anyone, even our most senior officers to manage well. But other issues bother me even more deeply.

Having intelligence collection and offensive/defensive operations run by the same leader is certainly more efficient and undoubtedly leads to more success for each. Yet if cyber conflict is as escalatory I fear, then some friction between separate leaders is actually a good thing, tamping down escalatory pressures and furthering stability.

I am also concerned that the Pentagon's defensive experts are compromised by being so closely tied to offense and intelligence collection. Since our true cyber power is the private sector, America's defenses will be most effective and responsive not if we work to optimize the relationship between NSA and Cyber Command but rather between government and those key private sector firms. This means reducing classification, creating a clear dividing line between NSA and US Cyber Command, and within NSA, preserving the independence of the Information Assurance Division. The Department of Defense has some of the crown jewels of America's cyber defense, but without these steps like this, they will continue to be seen as compromised in the eyes of the technology community, just another part of the agencies "weaponizing" vulnerabilities in their software.

Perhaps an analogy can help. Imagine the commander of U.S. Pacific Command were the leading source of information on the Chinese military threat, was active in all NSC meetings on China policy, ran the best-funded China-oriented bureaucracies, was involved in covert military operations against China, and could decide what information on China was classified. Americans, with centuries-old traditions of mistrust, would never accept such a concentration of power and yet this is what we've intentionally constructed in the dual-hat arrangement. Two heads – and two hats – are better than one.

Third, since the private sector is the supported command, the best use of government resources is to reinforce those doing the best work. Cybersecurity companies and other key parts of the private sector are already fully engaged with America's adversaries in cyberspace, so the government should be hesitant to try to imitate their agility, subject matter expertise, or ability to directly measure and change and change cyberspace.

As another analogy, there are many, many players on the cyber ballfield. Odds are, the player most able to make the play is a private-sector entity. Cyber defense is weakened if one player, the government, constantly runs around the entire field, yelling "I've got it, I've got it!" Maybe those other players can't see the ball clearly, or need a better glove or need practice drills to get

better at playing their position. Maybe indeed they don't even know they are playing the game. But bringing them up to speed is far cheaper and more effective than hiring more bureaucrats or diverting an already limited number of military personnel.

Grants are perhaps the most obvious example of how this could be done. At one point, the non-profit Financial Services Information Sharing and Analysis Center, of which I used to be vice-chairman, would only share threat information and best practices with the 50 or so companies which were dues-paying members. The Department of the Treasury helped us out of this sub-optimal situation with a grant of \$2 million to upgrade the technology and expand sharing to all thirteen-thousand plus banks and credit unions in the nation. Now the FS-ISAC is widely recognized as the model for security and information sharing, making that perhaps the best spent \$2 million in US government cyber history. Though this example was for the finance sector, I'm sure examples abound for armed services and national security.

If I were back in the White House, this would be my top short-term project. The most comprehensive way to identify such groups is for the executive branch to conduct a review of one or two representative responses for each kind of major attack against the United States and the Internet. These could include major denial of service, malware spread (such as Conficker), critical infrastructure attack (such as Iran against the finance sector), botnet takedown, and release of emails (like the DNC or Sony). Such a review, which would only cost a few million dollars, would examine who took what decisions, based on what information, and leading to what actions to alleviate the crisis. This review then could be used to improve national incident response plans, drive information sharing requirements, identify promising partners for the Departments of Defense and Homeland Security, and identify promising new projects for the most national defense at least cost.

Lastly, I'd like to leave you with a question which I like to ask my colleagues, especially those still serving in uniform or elsewhere in government: *What do you believe will be the dominant form of cyber conflict will be in ten years?*

When, for example, the Air Force Chief of Staff appears before this committee on the need for a Long-Range Strike Bomber, it is because the Air Force's conviction that future air combat will be dominated by the need to operate across very long distances over denied airspace. Yet, in cyberspace the Pentagon seems to have a healthy set of requirements but not the same sense of what future conflict will be like.

Just to list one likely and disruptive possibility, what if in 10 years most cyber conflict is fought between intelligent software bots, constantly changing their forms and backed by powerful supercomputers? We've already tested a nascent version of supercomputer-driven malware, with DARPA's Cyber Grand Challenge. After all, trading in stocks is now dominated by algorithms and human floor traders are largely superfluous. Why is this not a likely future for cyber conflict

also and, if so, what are the implications for US Cyber Command staffing and projects and overall US cyber defenses?

In closing, I'd like to address a small part of the cyber workforce talent gap. Five years ago, I helped create the Cyber 9/12 Student Challenge, for university students to tackle exactly the same sort of national security cyber challenges about which my colleagues and I are testifying before you today. The next competition will be held at American University on 16 and 17 March at American University with teams from many of your districts, including the US Air Force Academy, Brown University, the University of South Alabama, and the University of Maryland College Park. I've included the full list of 32 universities sending one of the 48 competing teams as an appendix to my written remarks. If you or your staff are available to observe, judge or provide remarks, I'm sure the student teams would benefit greatly.

Thank you for your time. Mr. Chairman and Members of the Committee, this concludes my testimony.

Appendix: Teams Competing in Cyber 9/12 Student Challenge

16 and 17 March 2017

Organized by the Atlantic Council and hosted at American University

1. Air University
2. American University
3. Arizona State University
4. Brown University
5. Carnegie Mellon University
6. Columbia University
7. Daniel Morgan Graduate School of National Security
8. Duke University
9. Georgetown University
10. Indiana University
11. John Hopkins University
12. Lewis University
13. Marymount University
14. Middlebury Institute of International Studies at Monterrey
15. National Defense University
16. National Intelligence University
17. Stanford University
18. Texas A&M University
19. The George Washington University
20. Tufts University
21. United States Air Force Academy
22. United States Military Academy
23. United States Naval Academy
24. United States Naval War College
25. University of Maine
26. University of Maryland, College Park
27. University of Maryland, Baltimore County
28. University of South Alabama
29. University of South Carolina
30. University of Texas Austin
31. University of Texas El Paso
32. University of Virginia

It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture
Dr. Martin C. Libicki

Testimony before the House Committee on Armed Services
Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities

01 March 2017

The views expressed here are those of the author alone. They do not represent the estimates or policies of the U.S. Navy or any other organization of the U.S. government.

Good morning, Chairman Thornberry, Ranking Member Smith, and distinguished members of the committee. My name is Martin Libicki; I hold the Maryellen and Richard Keyser Chair of Cybersecurity Studies at the U.S. Naval Academy, and am also adjunct management scientist at the non-partisan, non-profit RAND Corporation. The following represents my own viewpoint and not the viewpoint of the U.S. Naval Academy, the Federal Government, or the RAND Corporation.

I thank you for the opportunity to testify today about some issues associated with deterrence of cyberattacks.

Two years ago, the Commander of the US Cyber Command argued in Congressional testimony that he needed a greater ability to conduct offensive cyber operations, stating that its purpose was to be able to deter cyberattacks on the United States.¹

Clearly, greater capability would not hurt – but would it help much, must less suffice to achieve deterrence?

A successful posture of deterrence – that is, the use of threats to compel others to restrain themselves – has many prerequisites. Four of them merit note. First, the United States has to be able to *attribute* cyberattacks in order to punish the correct party and convince others that the United States is acting justifiably. Second, the United States needs to communicate its *thresholds* – that is, what actions will lead to reprisals. *Third*, U.S. promises to retaliate need *credibility* – so that others believe that punishment will, in fact, follow crossing such thresholds. *Fourth*, the United States needs the *capability* to carry out reprisals.

There are also other considerations but they are not prerequisites, as such. *One* is that carrying out reprisals affects the *broader* relationship between the United States and the attacking country; there may be larger issues in the ongoing relationship which may modulate or exacerbate the reprisal – which in turn affects the credibility and even legitimacy of the

¹ “How do we increase our capacity on the offensive side to get to that point of deterrence?”; Ellen Nakashima, “Cyber chief: Efforts to deter attacks against the U.S. are not working,” *Washington Post*, March 19, 2015, http://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html.

threat. For instance, however annoying the Iranian DDOS attacks on U.S. banks were in late 2012, efforts to halt Iran's nuclear program clearly had higher priority: thus, had reprisals been on the table, their impact on such efforts had to be taken into account. *Two* is the extent to which the attacker feels justified in its original cyberattack (which may have been prompted by something perceived in its past). This, in turn, will color its view of how legitimate the U.S. reprisal is – which, in turn, may influence the likelihood of its making counter-reprisals.

Returning to the prerequisites, the U.S. *capability* to retaliate in cyberspace is least in doubt amongst the four (even if United States need not respond in kind, Admiral Rogers' argument assumed that we needed to be able to do so). Any country credited with Stuxnet and the ability to penetrate systems using techniques described by Ed Snowden has demonstrated a very impressive capability. Whether or not the credit is deserved² is secondary. As long as other countries believe we can do magic, what we can *actually* do matters less for deterrence purposes. That noted, however, countries vary in their susceptibility to reprisals in cyberspace. North Korea is a good example because a combination of its economic primitiveness and paranoia about the outside world means that computers and connectivity are far less important to the national well-being than it is in other countries. Note that susceptibility consideration had only a modest effect on the efficacy of the nuclear deterrent. Furthermore, while the U.S. attention to the laws of armed conflict (specifically *jus in bello*) is laudable, the effect of following them is to take certain targets off the list. Such prohibitions are larger if people are worried that cyberattacks on some targets may yield unacceptable collateral damage. Lastly, for those who believe that reprisals delayed are reprisals denied, note that even a very capable United States is limited in its ability to respond from a cyberattack from a country that it did not previously consider a threat and thus whose systems it did not scope in advance. Otherwise, U.S. capability is more than sufficient for purposes of reprisals.

The other three prerequisites are what hobble the ability to develop a coherent deterrence policy.

Attribution, to be fair, has improved considerably over the past ten years. There are several reasons why. Roughly a decade ago, difficulties in attribution were recognized as an important barrier to establishing a deterrence posture. Considerable time and attention was therefore invested in improving the intelligence and science behind attribution; by late 2012, the Secretary of Defense was able to claim that two-thirds of all incidents could be traced back. Furthermore, several private cybersecurity companies – starting most publicly with Mandiant³ in early 2013 – started making their own attribution claims; this allowed the U.S. Government to make a case against other countries without having to reveal its own sources and methods

² In the last year, Israel has publicly declared that it and the United States together authored Stuxnet. "Deterring Terror: English Translation of the Official Strategy of the Israel Defense Forces," Belfer Center Special Report of August 2016; <http://www.belfercenter.org/publication/israeli-defense-forces-defense-doctrine-english-translation.p.48>.

³ Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*; sintelreport.mandiant.com/Mandiant_APT1_Report.pdf, March 2013

(even if some government officials believe private attribution claims force their hands when the evidence is less-than-overwhelming or decisions on reprisals need time to make correctly). Although the consonance between what the intelligence community knew and what the private cybersecurity claimed is less than perfect, the two efforts remain quite complementary. It is quite plausible that China's perception that the U.S. ability to attribute acts of economic cyberespionage to the Chinese was good enough sufficed to inhibit further economic espionage from that country after the Xi-Obama agreement to forswear such activity.

Nevertheless, a few cautions are in order.

First, the ability to attribute and the ability to evade attribution are a measure-countermeasure game. Until the consequences of being caught are severe enough, it may simply not pay for hackers to hide their origins (as opposed to their tracks) very well. Yet, if the point of having a deterrence policy is to inhibit cyberattacks, then presumably consequences have to be severe. If the prospects of reprisals are daunting enough, hackers can be expected to take pains to keep from getting *caught* carrying out cyberattacks. Hence countermeasures to attribution can be expected. Another way of putting it is that attribution will be good until it becomes useful at which point it will cease being good.

Second, the U.S. Government has made less progress in *explaining* why it believes its attribution is correct. After the Sony attack, the FBI's publicly released statement on North Korean attribution devoted just 140 words to justifying its conclusion.⁴ The public justification of Russian attribution for the DNC hack is even more problematic. The two public documents released on the matter – one by DHS⁵ and the other by the DNI⁶ – were generally deemed far from satisfactory. Granted, it may not be obvious why the United States has to convince others that it is right about attribution; by this argument, as long as the attacker knows that it could get caught and punished for what it did – and knows it did – then the opinion of third parties is irrelevant. But is it? To skeptics, U.S. retaliation against a country that could be innocent may strike them not as punishment but aggression. Worse, if potential attackers come to believe that innocence is no guarantee against reprisals, what is the point of being innocent? The accused country could easily maintain its innocence, and having done so credibly (for lack of a good case against it), could justify its responding to retaliation as if it were responding to unprovoked aggression. Thus, what started as an attempt to make other countries conform to standards of responsible behavior becomes an exchange of tit for tat where no one can easily claim the high ground.

⁴ FBI, "Update on Sony Investigation," December 17, 2014, <http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>

⁵ NCCIC, FBI, "GRIZZLY STEPPE – Russian Malicious Cyber Activity," December 29, 2016; https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

⁶ Office of the Director of National Intelligence, "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution," January 6, 2017; https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Credibility also remains an issue when it comes to *cyber* deterrence. Put simply, the United States has yet to retaliate to any cyberattack with any truly serious consequences of the sort that the rest of the world can see.

The U.S. retaliation against North Korea involved sanctions on a handful of individuals. The only quasi-serious response-like event was a DDOS attack on North Korea's thin Internet connection to the rest of the world – and, the United States, if anything, distanced itself from taking credit for that act.⁷ There are reports that the United States carried out reprisals against North Korea that did not make the news; although I have no way of evaluating that claim, suffice it to say that hidden reprisals lack effectiveness in persuading *other countries* of the folly of carrying out cyberattacks on the United States.

The United States also retaliated against Russia for the DNC hack by increasing some sanctions and throwing some Russian diplomats out of the country; there may have also been reprisals not visible to the public. Since the Russians probably believe that their contribution to defeating a presidential candidate they disliked exceeded the pain of having to replace a few diplomats, it is difficult to see how the consideration of future such punishment would deter them. Does anyone think the Russians will hereafter refrain from injecting itself into other countries' elections? And what does it say for the credibility of the U.S. Government when representatives of an incoming administration delegitimize the reprisals levied by an outgoing administration?

After two weak *public* responses, the credibility of U.S. reprisals cannot be ranked very high. Perhaps the failure to respond with anything harsher may have been wise given the relatively limited harm associated with both the Sony hack and the DNC hack – and the possibility that a major confrontation would have raised much higher levels of risk. But it would now take a serious response to raise the credibility of a *possible* U.S. response off the floor where it now sits – and several serious responses to convert the possibility into a likelihood. These hypothetical responses to as-yet-potential cyberattacks would carry their own risks. Put another way; if the United States wanted to achieve credibility for a cyberspace deterrence policy, the costs of doing so would not be small at this point.

That leaves *thresholds*, which I want to focus on in part because it seems to get the least attention. Here is the relevant question: what cyberattacks merit cranking up the machinery of U.S. retaliation for? The term, "machinery," is deliberately meant: the decision on whether and how to retaliate would certainly involve the President and the National Security Council, and would have to be followed up by policy adjustments throughout the bureaucracies to reconcile retaliation with whatever else is taking place vis-à-vis the attacking country. Retaliation, after

⁷ See Nicole Perlroth and David Sanger, "North Korea Loses Its Link to the Internet," December 22, 2014; <https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html>. But two weeks later, sanctions were described as a "first response" suggesting that the DDOS attack was not a U.S. response (BBC, "Sony cyber-attack: North Korea faces new US sanctions," January 3, 2015; <http://www.bbc.com/news/world-us-canada-30661973>).

all, is an unfriendly act. By contrast, foreign individuals can be indicted in U.S. court – as multiple cybercriminals are – based on decisions taken at the level of a U.S. district attorney and without much reference to the U.S. relationship with the country of their origin. Although the indictment of five members of China’s PLA and seven Iranian nationals doubtless required greater coordination, these moves were, at least, announced by someone no higher than an Assistant Attorney General.

The need for a threshold is obvious. Objectionable acts in cyberspace range greatly from a network hiccup to a major catastrophe. Not all of them merit Presidential attention. By contrast, in the nuclear realm, even the detonation of the smallest nuclear weapons on, say, U.S. soil was always going to be an enormous deal.

Finding a tractable and defensible threshold is, alas, a problem not easily solved. Let’s consider some candidates that have been bruited about.

Perhaps something is actionable if it violates the U.S. Computer Fraud and Abuse Act. Three problems arise. *First*, using a national law as a red line sets a precedent that can be easily abused by countries whose laws criminalize behavior that is acceptable, even normal, in the United States: e.g., posting on the Internet material critical of the government. In other words, if we use our domestic laws as a basis for international reprisals what keeps others from using their domestic laws in the same way? *Second*, the CFAA is being violated literally millions of times – notably every time a computer is infected as part of an effort to build a botnet, or every time some teenager wants to go exploring in someone else’s machine. *Third*, such a law makes cyberespionage generally actionable when the United States relies on such techniques to protect itself from terrorists and hostile countries. Another good reason not to establish a threshold that makes all cyber-espionage actionable is that penetrations can often go undetected for months or years and sometimes forever – whereas the effects of cyberattack in terms of the disruption of operations or the corruption of information is harder to hide. The less likely a violation is to be caught the more problematic it is to punish violations that are.

Another alternative threshold is to use some metric of size to determine whether something is actionable. As one Assistant Secretary of Defense has argued, the United States cares primarily about the top two percent of all cyberattacks.⁸ The problem with that formulation is that the criterion for membership in the set of cyberattacks has no obvious lower bound. Two percent of something unmeasurable is itself unmeasurable. Insofar as the effects of cyberattack can almost always be measured in terms of dollars, an economic threshold might make sense – until it comes time to measure impacts. If Sony’s statement to the SEC is indicative, the attack from North Korea cost only \$35 million (in the financial quarter that took place plus the quarter afterwards). Yet, there are reasons to believe that many intangible costs (e.g., to the reputation of Sony’s executives, the hassle of shifting communications from e-mail

⁸ David Sanger, “Pentagon Announces New Strategy for Cyberwarfare,” *New York Times*, April 23, 2015, <http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy>.

to phones, anxiety among employees) were not well captured by that metric. Furthermore, the Administration defended its decision to respond to the Sony attacks and the DNC attacks not by using economic criteria but because such cyberattacks violated transcendent values. That is, the attack on Sony contravened its freedom of speech, while the attack on the DNC contravened U.S. political sovereignty. Meanwhile, there was no U.S. response to the Iranian attack on Las Vegas Sands Corporation, which wreaked damage approximately as large as those suffered by Sony.

Another criterion for judging a cyberattack actionable is if it hurts some part of the U.S. critical infrastructure. One would think such a threshold had sufficient clarity, since the key elements of that infrastructure had been publicly enumerated by DHS (admittedly in response to physical terrorism, which generates a somewhat different list than a focus on cyberspace would). But following the attacks on Sony and the DNC, some have tried to stretch the definition to include such attacks. There were desultory attempts to note that, technically, Sony Entertainment was part of the U.S. critical infrastructure but they were not taken seriously.⁹ The DNC hack, however, did persuade the Government to declare the U.S. election system to be critical infrastructure, and properly so.

Perhaps a criterion is needed that offers a parallel with physical attack. Perhaps then, something is actionable if it violates the Laws of Armed Conflict (specifically *jus ad bellum*). LOAC has the benefit of being established international law. But the various laws of armed conflict, having been established for physical combat, focuses on destruction and injury. They do not cover economic loss from hostile activity (perhaps because one country can make many types of decisions that cost other countries money without using force at all). In the decades-long history of cyberwar physical destruction has occurred twice: Stuxnet, and a putative Russian cyberattack on a German blast furnace (in many other cases information was altered that resulted in making machines unusable until reformatted, but that is not physical destruction).¹⁰ No one has yet been harmed as a direct consequence of a cyberattack. Instead, the effects of cyberattacks are usually felt in terms of lost time, hence productivity: e.g., when systems are down or when the data they hold has to be recovered. It is unclear whether an attack that, say, bankrupts a trading house would be actionable by such criteria – and a willingness to declare it so after the fact is not a basis for deterrence.

To complicate matters further, the reliance on precedents such as LOAC fosters the notion that cyberattack, like physical attack, is actionable while cyber-espionage like pre-cyber espionage is acceptable behavior for countries. But accepting *all* cyberespionage as acceptable state behavior is *not* U.S. policy. The United States successfully pressed China to stop its economically-motivated cyberespionage – and by so doing established a norm that was

⁹ Kim Zetter, "Hacker Lexicon: What Counts as a Nation's Critical Infrastructure?," February 16, 2016; <https://www.wired.com/2016/02/hacker-lexicon-what-counts-as-a-nations-critical-infrastructure/>.

¹⁰ Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever" January 8, 2015; <http://www.wired.com/2015/01/german-steel-mill-hack-destruction/>.

adopted by the G20,¹¹ which, given the G20's membership, thereby makes it close to a universal norm. If the information taken from OPM had been sold into the black market – the possibility of which was implied by OPMs offering credit-monitoring services to potential victims – then it is quite plausible that the United States would have strongly objected that the acceptability of cyber-espionage did not imply the acceptability of every use of what was taken. Fortunately, there is scant evidence that such information was transferred to criminals. Lastly, it helps to remember that the DNC hack was actually cyberespionage – the results of which would not have led to a U.S. response if the Russians had kept what they took to themselves, rather than use it to influence the outcome of a Presidential election.

These three examples may not be the only occasions where cyberespionage rises to the point where it is as obnoxious as cyberattack. It is characteristic of cyberspace operations that it is very difficult to distinguish between cyberespionage against a system and the preparations made for a cyberattack on such systems. In some cases, the motivation for cyberespionage is so plausible, that countries caught penetrating systems with valuable information can be assumed to have done so out of interest in the information it held than in taking down the system that holds it. But it may be hard to give others the benefit of the doubt when they are caught carrying out cyberespionage against certain elements of a country's critical infrastructure – notably the machine control systems associated with transportation, energy production and distribution, or manufacturing in general – because the information such systems contain is of modest value while the potential for mischief is substantial. Here, too, certain types of cyberespionage may be plausibly deemed actionable if detected, characterized, and attributed.

In the face of these many issues, ensuring that countries do not convince themselves that there is a threshold below which that they can operate with impunity entails deliberately maintaining a threshold so low that the United States can afford to be indifferent to cyberattacks that fall beneath that level. This is hardly a panacea. First, it forces inordinate attention to above-threshold, even if low-level attacks, because the failure to respond to them erodes credibility associated with a U.S. promise to respond (although for some observers, the failure to respond will only erode their belief that the stated threshold is the real one). Second, if there is no difference between the responses to low-level and high-level attacks, potential attackers may reason that if they are going to get caught and punished (again, no sure prospect) they might as well try to achieve a greater rather than a lesser effect. Third, too low a threshold coupled with a fixed minimum cost associated with cranking up the retaliation machinery may strike others as disproportional, expensive, and even arbitrary.

A broader issue in all this is whether any country, even the world's most powerful, can arbitrarily establish redlines as opposed to first achieving some consensus on norms and then

¹¹ For a copy of the communique and a discussion thereof see Cody Poplin, "Cyber Sections of the Latest G20 Leaders' Communiqué," November 17, 2015; <https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communicé>.

using the violation of such norms as a basis for deterrence. To be fair, redlines are not the worst option; at least they have the advantage of needing to be declared beforehand. One of the problems with responding to the DNC hack – apart from its inherently political nature – was that few anticipated that the United States would need to declare against other countries hacking political organizations, extracting their contents of their e-mail, and posting them online. To react to injury solely after the fact assumes that a reasonable presumption could have been made by the attacker that something so injurious could not go unanswered. Such thinking is far from easy even in the physical domain where precedents to almost every conceivable action abound. In the cyber domain, such precedents are absent and the best one can resort to are inexact analogies between something that has merited objection in the past and some objectionable act in the present. Deterrence, after all, only works when the potential attacker knows *in advance* where the redlines are, at least approximately. A country's willingness to respond based on *post facto* redlines presupposes the willingness of others to give the aggrieved country a wide berth.

Redlines have had their place in U.S. history; the Monroe Doctrine which stated the U.S. intolerance for any establishment of new colonies in the Americas could not possibly have been a norm. It was geographically delimited to one hemisphere and the prevailing norm in those days actually allowed colonization in general. Russia's concern over activities in its near abroad, or China's concern over activities within its self-defined first island chain, to use less justifiable examples, are also geographically defined. But cyberspace, as oft observed, does not have the same geography and, to an important extent, has no geography at all. Thus, redlines cannot be stated in geophysical terms very easily – and thus also, a major justification for redlines in order to defend the *physical* basis for a country's sovereignty does not apply.

Redlines and norms differ in several key respects. A country can establish redlines without having to abide by them; when a country establishes exclusion zones for others, it hardly signals its intention to exclude itself. But a norm implies mutual constraint. Every UN member, by dint of its membership, has pledged adherence to norms against carrying out an armed attack on others. Clearly, redlines are less constraining than norms – but that may be exactly why arbitrary redlines sit poorly with long-standing U.S. ideals.

At issue is how rules should govern the world. Until the mid-20th century, international relations could be said to be taken from Thucydides' Melian Dialogue: the strong do as they will and the weak suffer what they must. Redlines bespeak a world in which strong countries – and the United States is the strongest – can set the rules that they can compel others to live by even if they have no intention of living by such rules themselves. But U.S. leadership in the post-war era allowed a different notion to take root. International stability and world peace result when everyone follows the rules, just as domestic stability and safety follow when everyone obeys the law. To achieve legitimacy, that meant that the United States and its friends had to obey the same laws. And much of the history of the Cold War was an attempt – one that was largely successful – to define these laws and use the muscle of the United States and its allies to see

that such laws were largely obeyed. The end of the Cold War made that task easier and spread the rule of law wider, but the effort remains non-trivial.

This theoretical difference has a practical consideration. Reconsider the OPM hack. Should the United States have responded? The attack transferred information of great value to China. It embarrassed the U.S. Government. U.S. officials were angry at the Chinese, and there is evidence that Chinese officials were at least somewhat abashed at having been associated with the hack (they subsequently announced an arrest for having carried out the hack¹²). But the DNI and a former CIA director admitted that what the Chinese did was something that the United States would have done if it could have (and it may well have done similar things).¹³ The United States could easily declare that it would regard a repeat as having crossed a red line; it might even be able to enforce its dictum. But if the United States would not foreswear doing likewise, it could not argue that a repeat would have violated a norm. One of the reasons that the United States could persuade China to abjure economic cyber-espionage is that it could make a reasonable case that this was behavior that the United States would not conduct – and, indeed, had not conducted (or at least no one has proved the contrary). By the same token, one of the difficulties of dealing with Russia’s politically-motivated cyberespionage-cum-doxing was the lack of a norm that made it easy to argue that such activity was out of bounds. Because countries, even the United States, seek to influence the elections of other countries all the time, mere unwarranted influence is a poor guide to norms-writing – but a norm condemning the use of cyberespionage coupled with doxing (for political ends) would be more precise and consistent with U.S. behavior.

A norms-based deterrence posture has its issues. One is determining how much of a consensus is required to establish a norm. One advantage of working from the UN charter is that UN membership is universal – but the conversion from the words of the charter into the new fields of cyberspace is hardly obvious. The European Convention on Cybercrime (aka the Budapest Convention) counts almost every advanced country as a signatory, but Russia, for one, is not a signatory. Treating, say, the Russian’s providing sanctuary for major cybercriminals as an actionable violation of universal norms is an iffy proposition. Conversely, waiting until North Korea signs up to norms before deeming them universal means waiting indefinitely. A

¹² Ellen Nakashima, “Chinese government has arrested hackers it says breached OPM database” Washington Post, December 2, 2015; https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

¹³ “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. (Matthew Ferraro, “On the OPM Hack, Don’t Let China Off the Hook,” *The Diplomat*, July 14, 2015,). Director of National Intelligence James Clapper echoed the sentiment, saying at a 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.” (Jim Sciutto, “Director of National Intelligence blames China for OPM hack,” June 25, 2015; <http://www.cnn.com/2015/06/25/politics/james-clapper-china-opm-hacking/>).

best guess is that a norm can be deemed universal if it wins adherence from either Russia or China. The other issue is holding others to norms. A country that has declared a redline has put the onus on itself – and only itself – to respond to a redline’s violation. Responding to a norms violation, however, is a collective responsibility – which is both good and bad: good, because many countries joint together in responding, and bad because each country can shift the responsibility to the other. In the past, it has fallen to the United States to enforce norms of international behavior, picking up other countries as active allies or passive supporters as their politics dictated. But it is fair to note that despite the lip service that the United States pays to its mutual-defense alliances, it is more likely to react to a cyberattack on itself than to an ally. The best indicator comes from comparing its response to the Sony attack to its non-response to a longer series of more damaging incursions into South Korean systems.

Conclusions

Using the threat reprisals to dissuade cyberattacks introduces multiple issues that need far more careful attention than they have received to date. The notion that building an offensive capability second to none suffices for deterrence is simplistic, to say the least. Granted, weak countries cannot deter, and in there is a basis for Admiral Rogers’s argument. But the United States is by no means weak, especially in cyberspace. If the U.S. deterrence policy has problems they are not ones of weakness but wisdom, notably in determining where to draw the line between cyberattacks that are actionable at the national level and those that can either be ignored or responded to via judicial processes.

In the interim, we should understand that there are certain potential cyberattacks – e.g., one that plunges the country into a blackout – that clearly cannot go unanswered, while there are other ones that are simply too trivial to bother with. It is the in-between that is the problem. As a general rule, it would seem appropriate for the United States develop its thresholds by working towards a regime of norms with which the difference between the actions of foreign governments that are acceptable and those that are unacceptable and actionable can be made consistent.

I appreciate the opportunity to discuss this important topic, and I look forward to your questions.

Prepared Testimony and Statement for the Record of

**P.W. Singer
Strategist at New America**

At the

Hearing on “Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities”

Before the House Armed Services Committee

March 1, 2017

**Cyber-Deterrence And The Goal of Resilience:
30 New Actions That Congress Can Take To Improve U.S. Cybersecurity**

Hackers working on behalf of the Russian government have attacked a wide variety of American citizens and institutions. They include political targets of both parties, like the Democratic National Committee, and also the Republican National Committee, as well as prominent Democrat and Republican leaders, civil society groups like various American universities and academic research programs. These attacks started years back, but have continued after the 2016 election. They have hit clearly government sites, like the Pentagon’s email system, as well as clearly private networks, like US banks.

In addition to attacking this range of public and private American targets, over an extended period of time, this Russian campaign has also been reported as targeting a wide variety of American allies. These include government, military and civilian targets in the United Kingdom, Czech, and Norway, as well as now trying to influence upcoming elections in Germany, France and Netherlands. Overall, reports are that Russian cyber attacks on NATO targets are up 60%, against EU institutions up 20%, in the last year.

This is not the kind of “cyber war” often envisioned, with power grids going down in fiery “cyber Pearl Harbors.” Instead, it is a competition more akin to the Cold War’s pre-digital battles that crossed influence and subversion operations with espionage. Just as then, there is a new need for new approaches to deterrence, that must reflect a dual goal to defend the nation, as well as keep an ongoing conflict from escalating into physical damage and destruction.

While Vladimir Putin has denied the existence of this campaign, its activities have been identified by groups that include all the different agencies in the US intelligence community, the FBI, as well as multiple allied intelligence agencies, who have seen the very same Russian efforts hit their nations and various international organizations (most notably the World Anti-Doping Agency). This campaign has also been established by the marketplace; five different well-regarded cybersecurity firms (Crowdstrike, Mandiant, Fidelis, ThreatConnect and Secureworks) have identified it. This diversity of firms is notable, as such businesses are competitors and incentivized instead to debunk each other’s work. Indeed, even the most prominent individuals, who first denied the existence of the hacks and then the role of the Russian government in them, now acknowledge this campaign;

this now includes even the US president (“As far as hacking, I think it was Russia.” President Trump stated at his January press conference).

It is time to move past the debate that consumed us for the last year. The issue at hand is not whether Russia conducted a series of cyberattacks on the United States and its allies. Nor is cybersecurity a concern for only one political party. The real question now is whether and how should the United States respond?

A Wider Strategy for a Larger Problem

Russia’s attacks are the most notable events in cybersecurity, but they are only one aspect of a larger threat landscape. In cyberspace, the malevolent actors range from criminals stealing personal information or holding ransom valuable corporate data (though, here too there is a major Russian role, with over 75% of ransomware coming from Russian-speaking parts of the online criminal underground; and Russian criminal groups have repeatedly been used as an enabler for the Putin state) to governments like China, which have been accused of breaking into government databases like the OPM in a cyber version of traditional espionage, as well as largescale intellectual property theft.

Just like in the real world, in this online landscape, though, we must weight threats. And here too, the scale and power that states can bring to bear far outweighs that of non-state actors. For example, while “cyber-terrorism” and the activities of so-called “Cyber Caliphate” of ISIL sympathizers have garnered great media attention, their most noted exploits so far are mostly annoyances like hacking a US military command’s Twitter feed and posting pictures of a goat. By contrast, no single threat actor has brought malicious cyber activity together in the wide-ranging and brazen manner in which Russia has done, targeting not just individuals and organizations across our society, but the fabric of democracy itself.

So what can be done to defend America in this realm? The following is a strategy that, reflecting the nonpartisan nature of this realm, is able to be implemented with support from leaders of both parties.

1) Restore Deterrence

Cyberweapons have proven their value in espionage, sabotage, and conflict. And the digital domain will be as crucial to warfare in the 21st century as operations on land, air, and sea. Indeed, the cyber front of any war between the United States and China would feature not just military units like Cyber Command or the PLA’s Unit 61398, but also non-state actors that might range from Chinese university cyber militias to Anonymous hackers joining in the fight with their own goals and modes, much as what has happened in the online ISIS battles.

This is a good illustration of another misperception: Cyberweapons are increasingly useful tools of espionage and war, but they are not akin to “weapons of mass destruction.” The fear of a single big thermonuclear tit for tat maintained the nuclear balance; indeed, treating nuclear weapons as no different from conventional weapons is what many feared would unravel MAD. Offensive cyber capabilities, by contrast, are a key part of the toolkit to be used in both hot and cold conflicts. Indeed, the US has already crossed this line by openly admitting to conducting offensive cyber operations against ISIS.

Reflecting this dynamic, we should continue to build our offensive cyber capabilities and the deep investment we have made at organizations like Cyber Command. A key element to maintaining superiority will be to *invest deeply in game-changing technology breakthroughs in this space, most notably AI and quantum, to ensure a US lead is maintained. As such, congress should request classified briefings to assess where the US stands in this space in relationship to likely adversaries.*

As we move forward, though, we must recognize that, just as in the past, technology is not enough. The key to effectiveness will be in doctrine building and integration; i.e. how we meld technologies and activities in the cyber domain with conventional operations in the air, sea, land, and space. Indeed, if there is a historic parallel to worry about in a future conflict, it is not merely Pearl Harbor, but a digital version of the 1942 Battle of Kasserine Pass, where a US military failure to bring together technologies and units across domains helped contribute to the early losses of World War II. This points to how the time has come to *establish Cyber Command's long-term status and disentangle the "dual hat" leadership structure with the National Security Agency.* These two valuable organizations work in the same realm, but they must reflect different organizational culture, goals, and processes. Of note, among the original rationale for this "dual" structure was concern that the leadership of Cyber Command would not have enough stature with Congress; instead, the post-Snowden debates have meant that Congress has more often become interested in their NSA role.

Building deterrence, however, is not merely about military capability. We must have a unified strategy that cuts across agencies and is willing to understand and use all the tools of power and policy, not just those that encompass the zeroes and ones of software or malware. In these, we should seek to leverage our strengths against others' weaknesses.

The Obama administration moves in late December to sanction Russia for targeting US democracy are a good start, albeit too little and too late, criticism that the congressional leadership was quick and correct to make. It is thus equally correct for the legislative branch to back these words with action, *by turning the sanctions against Russia for its 2016 elections interference into law and strengthening them further.* This will make it harder for any moves by the Executive Branch to set them aside (as both White House aides have noted in press conferences and Mr. Trump has hinted would be the case at his press conferences). Instead, strengthened sanctions would show Mr. Putin that the nation of Truman, Eisenhower, and Reagan is still willing to stand up to Moscow, rather than shower it with praise.

Deterrence is not about punishment for punishment's sake, though, but seeking to find pressure points to influence future actions, both by that actor and others looking to its example. Here the overall weakness of the Russian economy and its oligarchic structure are choice leverage points (indeed, it is sad that the US is being bullied about by the 13th largest economy in the world). In thinking through targeting for cyber deterrence, we can sometimes see what regimes fear most by what they try to ban discussion of. This points to a particular focus to expand: *targeting financial assets of Mr. Putin and his allies, especially those held outside the country in real estate and tax shelters*, even those with US and Western business partners. Sanctions, especially tying up oligarch money/visas, to Russian cyber interferences are valuable in two ways. The first is to shift malicious cyber activity from being low cost-high gain to the attacker, changing Russia's calculus, as well as a signal to future attackers. IE, we should want it 'on-the-record' that this kind of action crosses the line and warrants retaliation, which would also be useful for a rapidly forming body of international law and norms that are in flux.

Outing these assets should also be the target of any covert cyber action (the Russian regime's outsized anger at the publication of the Panama Papers, showing where just a small portion of its money was hidden around the world, reveals an area to exploit further). The same twin goal of outing and defanging networks should also be placed on enablers of the attacks, focusing on *revealing to the wider community the digital and financial infrastructure that has been used to conduct the attacks themselves*, which would reduce their utility for future attacks.

The point is that, unlike in the Cold War, there is no need to hit back within the limited time window of the other side's missiles in flight. Cyber deterrence building can come after the fact of an attack and in other realms. The defender can go after the structure used in the attack, other assets valued by the attacker in other realms, or even those assets valued by third party actors that have influence on the attacker. Thus, the response to a cyber attack can range from hitting back with a like cyber attack to alternative pathways like sanctioning companies benefiting from stolen fruit to personal level actions like threatening to revoke valued visas or business deals for regime leader or oligarch family members, etc. Indictments of individuals involved in hacking might also serve a purpose not of actual prosecution and punishment, but as a different means of surfacing data about attribution, or to make access to the global financial system more difficult. The goal is a wide dynamism that complicates attackers' calculation that they will make any clear gains.

So too must our deterrence building goal align with the building of global norms, through activities that range from international treaty negotiation to the use of sanctions.

This leads to a fundamental change from the typical discussion of deterrence. In the Cold War, everything was targeted, from military bases to cities full of civilians, but outright attacks crossed the line. Today, the situation is inverted. While unwanted, some cyberattacks will have to be allowed, while certain targets must be made anathema.

Not all 'cyberattacks' are formal acts of war. No one wants their state secrets stolen, for example, but it is part of the expected dance of great powers in competition. Hence while the theft of secrets from the OPM was a clear loss to US security, it was not an attack that was beyond the pale. As former NSA and CIA directors have explained, the breach at the OPM was more a "shame on us" than "shame on them" situation. By contrast, there are other cyber attacks that may not be clear acts of traditional war, but they should be a focus on norm building to prohibit. For instance, introducing the digital equivalent of a dormant Tasmanian devil into a nuclear power facility's operating system or other major civilian infrastructure should be off limits to both sides, not merely because it would be disproportional if actually used, but because simply the act of deploying it risks accident or even interpretation as an incredibly escalatory step of preparing for war.

Continuing to set and reinforce these guardrails has to be one of the key activities in the various bilateral and multilateral efforts that the US government makes in this space on norm and law building. These extend from the webwork of agreements on cybersecurity that we are building with our allies to the two U.N. General Assembly resolutions that call for respect of the laws of war in cyberspace, to the Tallinn Manual process. In order to ensure this track is not abandoned in the upcoming administration, *the Congress should hold hearings on what US norm-building strategy in global cybersecurity will be moving forward, with a special focus on actions that can be taken to support the Tallinn Manual 2.0.*

Yet, for all the laudable work in building norms, what threatens to undermine any guidance of behavior is inaction when acts clearly violate the norms. One of the consistently agreed upon norms across global and US discussions is not to target clear civilian infrastructure with the intent to cause widespread damage (as opposed to a goal of monitoring or stealing information), even more so outside of a context of a declared war. Such attacks are viewed as violating the norms of necessity and proportionality that underpin the internationally agreed upon laws of war.

Yet, in December of 2015, this line was clearly crossed in an attack on the Ukrainian power grid. More than 230,000 civilians lost power, in what has been positively identified as a cyber attack by both local authorities and international experts, and US officials have identified Russia as the attacker. It was the first proven takedown of a power grid, the long discussed nightmare scenario. Yet, in the story of action and consequence that is the key to maintaining norms, we had clear action, but as yet no clear consequence. Just as with the attacks on our political system, a pattern of not responding builds a different kind of norm and incentive. *The Congress should hold hearings on what US strategy is in response to this new realm of attack, both in how we plan to aid Ukraine and foreign partners from suffering such attacks in the future and how we plan to better defend the US system*, to ensure this act is not swept under the table.

2) Build Resilience

This strategy to influence attackers should be joined with an effort to build our own resilience to their influence. “Resilience” is the ability to power through an attack and shake it off, thereby limiting the gains to the attacker and recovering rapidly from any losses. It is also known as “deterrence by denial.” The idea here is, by making attacks less beneficial to the attacker, you make them less likely. Most importantly to the problem that we face in the diversity of cyber threats, it is useful for responding to them all. The great value of building resilience is that it applies not just to Russia, but to any kind of cyber attacker and any kind of cyber attack.

Unfortunately, despite the attention, rhetoric, and money the United States government spends on cybersecurity, it is still far from resilient against cyber attack. For every gain, there is still a major gap to be closed. In the military, the construction budget alone for Fort Meade, the combined headquarters of the NSA and Cyber Command, reached \$2 billion by the end of 2016, and the force will add another 4,000 personnel. Yet, the Pentagon’s own tester still found “significant vulnerabilities” in nearly every major weapons program, that extended from breaches of operational systems all the way back to the original design process. The multiple reported breaches of the F-35 program and the “interesting” similarities between the next US strike fighter and its Chinese twin the J-31 is an example of changed dynamics: It will be hard for the US to win any arms race if we are paying the research and development cost for the other side.

The Pentagon leadership is aware of these vulnerabilities, but the overall implementation of resilience measures is still uneven, especially within the DoD and federal government acquisitions process. *A focus on building resilience, establishing metrics, and determining where progress towards them is not being met, should be a key oversight priority for Congress.* Among the measures needed is to *determine where if any, changes are needed in either law or Pentagon buying processes to bolster resilience to cyberattack.*

In the broader federal government, the cybersecurity budget for 2016 was 35 percent higher than it was just two years ago. Yet half of security professionals in these agencies think cybersecurity did not improve over that same period. The reasons range from continued failure to follow basic

measures – the requirement for personal identification verification cards dates back to 2004 but still is not fully implemented -- to a failure to take seriously the long-term nature of the threats we face, most importantly in a world of renewed geopolitical competition. The exemplar of these failures was the OPM, which dealt with some of the most sensitive government information, and yet outsourced IT work to contractors in China -- despite warnings going back to 2009.

There have been various drafts of new Trump administration Executive Orders on floating about online, so it is preliminary to comment on them, other than to say that they seem focused on initiating a series of evaluations and reviews. For the new team to further study the problem and how we are organized is perfectly sensible; but it is well past time that we begin to act on areas where there is general agreement across political lines.

One of the lesser noticed studies of the last administration was to identify a series of best practices that the top firms in private industry use in cybersecurity that could be brought into government, as well as create a bipartisan commission of experts, which issued its own set of recommendations during the transition period of Dec. 2016. These range from identifying high-value assets that need to be better protected and recruiting top human talent to accelerating the deployment of detection systems. *Ensuring the implementation of these measures to raise federal agency cybersecurity could be one of the most important things that the new Congress could do to limit our insecurity in cybersecurity.* And the fact that they originate from market lessons and bipartisan advice should make them politically doable for leaders of both parties. *The Congress should request of the new administration a yearly report on its progress on meeting these metrics, and use them to identify any key funding or programmatic gaps.*

As information systems ubiquitously underlie key governing functions, states and localities are increasingly critical to the nation's cybersecurity. Investing in robust relations between the federal government and state and local actors is essential to (cyber)securing the nation. Recognizing the essential role played by non-federal government actors on the 'front lines', *the Congress should identify where the federal government can better coordinate with and aid local authorities. This includes efforts to clarify the respective roles of and responsibilities for federal and state entities, as well as disseminating the many existing and helpful resources to state and local actors, who are currently operating in relatively resource-starved environments.*

This same uneven implementation plays out across industry. While corporate boards are now talking far more about the problem, cybersecurity spending as a portion of IT budgets is still roughly a quarter of the rate within government IT budgets, while only 25% of key industry players, for example, participated last year in Information Sharing and Analysis Centers (ISACs), which share needed cyber threat data -- the same percentage as in 2014. The outcome is that some sectors, like banking, take cybersecurity seriously, while others, like health care, manufacturing, and infrastructure, remain behind the curve. Of note to the concerns over Ukraine power grid attack is that despite this real demonstration of the risks, experts worry that US companies have not implemented key steps to better protect themselves, not just against the tactics used in December, but how they will naturally evolve in the future. *Congressional action is needed to establish whether critical infrastructure firms, most especially in the power sector, actually have implemented needed measures.*

This concern extends down to the personal level. Unlike in the Cold War, individuals both face personalized cyber threats, but also can contribute more to national security. During the Cold War, "duck and cover" was about all that a population could do when it came to nuclear deterrence. Today, the vast majority of Americans use the Internet, and they can actually make a difference in its defense. Whether we are talking about career civil servant or a citizen trying to secure sensitive

information, the human is an incredibly important part of the system of defense, if not the most important. Over 90% of cyber attacks would be stopped by basic measures of cyber hygiene, from two factor authentication on accounts to using different passwords for their bank accounts and fantasy football teams. *Increased congressional support for cyber hygiene efforts, including in our schools, would be a valuable aid to national security.* Just as we should seek the latest technology, a truly robust government approach would include the latest innovations from behavioral science to improve cybersecurity. Reflecting this, *Congress should also include support for programs that support social and behavioral science insights to improve cybersecurity policy outcomes, specifically in the creation and improvement of cyber hygiene-related policies to boost adoption.*

How this all ties together into one strategy is that we have to rethink the role that government can play in linking cybersecurity policy, markets, and citizenry behavior. In other words, government can and should play the role it plays in cybersecurity that it does in other realms, from health to transportation.

Sometimes government can be a trusted provider of useful information to both business and the wider public. And sometimes it can go further to help shape individual and market incentives. For instance, the government created Center for Disease Control (CDC) to fill key gaps in fighting disease, funding research on under-studied diseases, and serving as a trusted exchange for information provided by groups ranging from universities to drug companies. *The creation of an equivalent cyber CDC could meet some of the same needs in cybersecurity.* This track will also build upon how the question in cybersecurity is no longer the debate of public sector vs private sector response, but rather which part of the public sector should companies turn to for what aid? The last administration's PPD41 started this clarification, but there is more required; it should not be for the private sector to have to navigate which part of the government to call in each circumstance.

Similarly, U.S. buildings are filled with "EXIT" signs and fire extinguishers, while cars have seatbelts and crash bags. These demonstrate the efficacy of government in creating *both* voluntary standards and actual regulations to increase security. These regulations are then bolstered by insurance laws and markets that use the combined power of the public and private sector to incentivize good behavior and best practices. Such a system has positively shaped everything from building construction to driving habits.

So too, the government should support not merely research on the basic standards of Internet security, like the laudable NIST process, but now work to backstop them with the nascent cybersecurity insurance market. Like many other new insurance markets, cyber-insurance certainly has a long way to go and key questions to figure out, but we can't let its growing pains now keep us from reaching for a system that would make our industry, as well as citizens, consumers and the entire nation, more secure. If Congress can aid in spurring that market to further develop, it can potentially have a massively positive effect on national security.

Last year, the cybersecurity marketplace collected \$1.6 billion in premiums. It sounds like much, but is a drop in the bucket compared to the overall scale of the insurance industry (which collected over a trillion dollars comparatively), the scale of our digital economy, and the scale of cybersecurity risk at both a personal, business, and national security level. Less than half of the Fortune 500 have insurance protecting them against cyber incidents (and, in turn, incentivizing and guiding them to undertake best practices to avoid and mitigate these risks), while among mid-sized firms, some 18,000 firms are not yet insured. The protections are also varied across sectors. Much as how banks

were among the first to information share and adapt other best cybersecurity practices, so too here are other sectors behind; only 5% of US manufacturing firms have cyber insurance.

As Elana Broitman explores in her New America report on the needs of a cyber-legislative agenda, Congress can aid in building personal, corporate and national cybersecurity by injecting more life into this marketplace. We are certainly not at the point yet in the debate to where such insurance should be required of all firms, the way fire insurance or car insurance is. However, in lieu of regulation, Congress can push forward key measures to enable better and more flexible market solutions for cybersecurity. It should 1) *hold a series of hearings to better understand the cyber insurance field and its relationship to US national security* 2) *commission a study to explore how DoD buying power and partnerships with the corporate sector, not just in the traditional Defense Industrial Base, but also through Transportation Commands' relationships with broader parts of the economy, can incentivize or require the spread of cyber insurance that would bolster market solutions to raising US national cybersecurity* 3) *help establish an Insurance Laboratory within the National Institute of Standards and Technology (NIST) cybersecurity process,* 4) *work with the industry and state partners to build legislation that would aid in the building of common cybersecurity insurance industry terms and language, something that requires regulatory cooperation across states, thus fitting with Congress's constitutional role;* and 5) *explore the passage of a Cybersecurity equivalent to the Terrorism Risk Insurance cap (TRIA).* Just as such legislation was designed to encourage best practices in protecting infrastructure from conventional terrorism threats post 9-11, the same kind of back stop against catastrophic cyber attacks against critical infrastructure sector (particularly from states in the event of war) would help encourage the spread of insurance that would, not so ironically, help make cyber attacks both less painful and less likely.

The challenge in building true cybersecurity resilience is not only about software and legal code, however, but also about people. This is where there is concern on the new administration's cybersecurity executive order draft. The question is not just what is in it, but what is not; the last drafts to circulate online were lacking any strategic effort to solve our cybersecurity workforce challenges.

Across government and industry, there is a growing lack of cybersecurity professionals; the consultancy Frost and Sullivan estimates that the global gap between security openings and skilled people to fill them will reach 1.5 million by 2020. Thus, even when positions are created and funded, they are difficult to fill, both in private industry and in government. For example, at last report, 40% of the cybersecurity positions at the Federal Bureau of Investigation (FBI) remained unfilled, leaving many field offices without expertise. Diversity is also a problem; less than 10 percent of cybersecurity professionals are women, lower than the already dismal rates in the broader IT world. How can we fill key gaps if we are only recruiting well from less than half the population?

The prior administration created a "Cybersecurity Human Resources Strategy," that should serve as the basis of a move forward. *Congress should oversight implementation of (or not) of the strategy's identifying human resources milestones and aid in building greater resilience by targeting any gaps with scholarship programs and other incentives. The Congress should also task the Department of Education to report on where it can best aid states and cities (where education policy sits in the US) to start to develop genuinely effective cybersecurity education and workforce strategies to fill needed national, state, and local gaps, as well as steer students towards this valuable and well-paying field.*

Filling the human resources pipeline to aiding our cybersecurity is a long term challenge. Of immediate concern, though, is the impact of the Executive Branch's federal hiring freeze on filling

needed cybersecurity positions. This has been described as causing “disarray” in areas that range from the US CyberCorps, the scholarship program that serves as a ROTC like feeder for cybersecurity positions (Students are unclear if they can no longer be hired and meet their scholarship obligations) to filling needed IT/cybersecurity positions at agencies that range across the government, from OPM to Treasury (one official said there will soon be “hell to pay” in its near and longterm effect). *Congress should make clear to the Executive branch that cybersecurity related positions, across the federal government, should be excluded from the hiring freeze, given the critical nature of the field and the higher costs that would come from security breaches, nullifying any purported budget savings.*

Any human resources strategy, however, will fail if it only puts new people in old organizational boxes, using the same pipelines.

Attracting more talented civilian expertise into the government through new channels will be a key to supporting a “deterrence by denial” strategy across our broader networks. Consider, for instance, that after the embarrassment of the healthcare.gov rollout, the government created a Digital Service to bring young Silicon Valley innovators into government to do things like fix the federal health care website design and aid the VA in building user-friendly apps. Even after the OPM debacle, however, there is still not a parallel one to shore up cybersecurity. One approach is to simply *expand the USDS to include cybersecurity recruiting as part of a larger extension of the program to 2026*. Additionally, as Adam Segal of the Council on Foreign Relations has recommended, *a cyber version of the Epidemic Intelligence Service (EIS) at the Center for Disease Control and Prevention (CDC) should be established*. The goal in both would be to provide government with a flexible pool of in-house talent and expertise that can aid in training, preventing, and mitigating breaches.

Another area where Congress can aid, importantly in a manner that cuts across traditional partisan lines, is to jumpstart more best practices that bring together the public and private sector. A good illustration is the Pentagon’s adaption of a “bug bounty” program. This is a program used by many top companies that offers small rewards to encourage a “crowd sourced” solution to cybersecurity; in essence, it enlists the ingenuity of citizens in the open marketplace to find the holes in our security before the bad guys do. The Pentagon’s pilot program offered rewards ranging from \$100 to \$15,000 for a person that identified multiple security gaps. The experiment with this approach has been a success. Its first bug reports came in just 13 minutes after the contest started. After just 1 month, 1410 outside hackers had submitted 1189 reports to help to spot and fix vulnerabilities in the Pentagon’s websites.

The cost was \$150,000, an order of magnitude at least cheaper than if the task had been contracted out. But the gains of the program were also about identifying and building out ties to cybersecurity talent beyond government. For example, one of the hackers who helped defend our military’s IT systems via this program was a teenager who did help protect the Pentagon during his high school AP exams. *Congress could play a powerful role in aiding and encouraging the spread of such “bug bounty” programs to each DoD agency, as well as to other federal government agencies. It should also create incentives for similar programs across state and local government partners and private industry.*

Similarly, innovations are needed in our military organizational models. Several National Guard units have been retasked to focus on cybersecurity. They have performed admirably, even besting some active duty Cyber Command units in wargames. But the new units are not enough, nor can they ever be enough. They only serve as a means to organize talent *already* serving in the military. There is a far deeper and wider pool of talent outside the military that is simply not going to be accessed by this

effort, either because the individuals are unwilling to meet the various obligations that come with military service (an IT tech in the National Guard, for example, is still legally obligated to serve in any mission they are ordered to, whether it be a cyber 911, Haiti Earthquake response, or Iraq war) or because they are unable to meet the various physical or legal requirements for joining the military.

Here again, there are lessons to be learned from the past that are not usually part of our present day cyber deterrence discussions. During the Cold War, nations like Switzerland or China chose an “active defense” model that was based on deterring attack not by massive retaliation but by mobilizing their citizenry for broader national defense. The United States was in a far different position in the Cold War and so this model was not an apt one for us in the nuclear age.

Today, in the new issue of cybersecurity, there is much to learn from others, past and present, as they wrestle with similar problems. Estonia’s Cyber Defense League, for example, is a particularly good model. Rather than a traditional military reserve, it is a mechanism for Estonian citizens to volunteer their expertise for cybersecurity. It is made up of a security-vetted volunteers, who aid the government in everything from “red teaming” --finding vulnerabilities in systems and activities before the bad guys can exploit them-- to serving as rapid response teams to cyberattacks. Notably, the members are not just technical experts, as the needed expertise that lies outside of government is about far more than just computer coding. For example, to defend the national banking system from cyberattack, a mix of hackers and bankers is better than just bankers or hackers.

These efforts have helped turn Estonia from one of the first victims of a state-level cyberattack, when Russian hackers partially shut down the country in 2007, to now being perhaps the best-equipped nation in the world to weather cyber threats. Estonia may not have the same capabilities as the NSA and Cyber Command, but it does have deterrence by denial and an involved populace -- giving it arguably better cybersecurity than the United States.

While the “Minutemen” from the Revolutionary Era is the historic US parallel to Estonia’s approach, today, the most apt parallel today would be the U.S. Civil Air Patrol-Air Force Auxiliary, where citizens can build up their own aviation skills, but also volunteer to aid government in anything from aviation-related emergencies to training exercises. The CAP also serves as a useful recruitment and feeder program for future US military pilots. *The Congress should establish a US cybersecurity parallel program to the Estonia’s Cyber Defense League and U.S. Civil Air Patrol-Air Force Auxiliary, designed to draw upon our nation’s wider technology talent and sense of volunteerism.*

The Special Cases of Elections and Social Media

The success of Russia’s attacks on the 2016 election are dangerous not just because of their past impact, but also how they will serve as a guidepost to others in the future. Contrary to the approach so far, however, we must recognize that the critical infrastructure of elections is not just the voting machines, but also the wider ecosystem, including national parties and campaigns. Notably, these groups began to physical security protection from the Secret Service after threats to candidates had both national political relevance and were beyond the private resources of the day (Pinkertons and friends).

Much as banks compete, but still share threat information, our election systems and political organizations, including even both the RNC and DNC, should have had the structures to cooperate in this space; indeed, all that would have been needed to stop the entire DNC hack was a better line

of communication with the FBI agents who had been tracking the Russian hacking for years. *Beyond just voting machines and voter databases, Congress should redefine the institutions involved in our democracy as a whole as critical infrastructure, in order to provide higher levels of resourcing and support from the federal government and enable better information sharing.*

More broadly, the 2016 elections point to how we need to understand that the internet is changing. The rise of social media has turned any user into both a collector and sharer of information. It has provided more transparency and engagement, but also means that cyber attacks have pivoted from being merely about controlling computer networks to enabling information warfare. The hacking of a computer system is often now merely the entry point to hacking hearts and minds. A way to think about it is that the Russian efforts to influence the 2016 US election were less like past state-linked hacks of political campaigns in 2008 and 2012, or attacks like those on the OPM. Instead, their parallels were more like the attacks on Sony or the cheaters' website AshleyMadison. These attacks involved not merely the stealing of information, but the outing of it in a manner designed to influence.

Thus, our need for resilience also must extend beyond bits and bytes to building up better political resistance to the influence and information warfare operations that allows Russia and other future attackers to exploit such cyber attacks. We must continue to uphold our freedom of speech, but ensure that authoritarian leaders don't take advantage of it. *Congress should recreate the Active Measures Working Group, an interagency effort during the Cold War that debunked the worst of Soviet misinformation. In addition, as Secretary Mattis recently noted at the NATO conference, there is "very little doubt" that Russia is targeting for interference "a number of elections in the democracies." It should also *hold hearings on how the United States can better work in cohesion with our NATO allies to help identify and counter Russia's election influence campaigns* (many of which have just pivoted from targeting US to European voters). Importantly, these lines of activity to identify and push back against such campaigns will not just counter outside influencers, but also help in debunking the individuals and outlets who have chosen to become either willing partners or полезные дураки, "useful idiots," for spreading conspiracy theories and foreign government propaganda.*

The shift towards social media also connects to a broader lesson: information is being weaponized in new ways. In warfare, social media is not merely an issue for public affairs officers. Just as political campaigns have shifted to reflect the new landscape in their voter outreach, many of our armed adversaries have radically reoriented how they use and integrate social media into everything from their recruiting and propaganda to their intelligence and even conventional military operations. The rise of ISIS and the Russian military operations in Ukraine are exemplars, but the model is now global. In turn, it points to how we have to integrate the same. *Congress should request a report on how the Department of Defense can better utilize and integrate social media into our own training environments, intelligence gathering, and operational planning.*

We also need to better understand not just how social media is being used in conflict, but how it contributes to the very risks of conflict. The change dynamics here range from leader statements that reveal negotiating psychology to those that inflame relations with either adversaries or even with longstanding allies.

This is not just about understanding leaders' personal social media use, but how it shapes the environment around them. Just as newspapers and television once shaped public opinion, and

governments had to understand this dynamic, so now does social media. It can empower leaders, but maybe box them in, including even in authoritarian states, such as high levels of nationalism and social media use in China.

It has become a cliché among international-relations scholars to draw parallels to 1914 Europe, but the potential challenges posed by social media make the comparison apt. Then, as now, regimes toyed with the new communications mediums, in order to bolster their standing, which had the effect of amplifying the power of nationalism. These leaders discovered too late that the popular forces they sought to manipulate were beyond their control. *The Congress should request of the intelligence community a briefing on how social media is shaping conflict likelihood and where the Congress can aid in better US capability to understand and monitor this changing force.*

Conclusions

History will record that in 2016 the United States was the victim of the most important cyber attack so far in history. It will judge us by whether and how we respond.

Akin to the Cold War, we face a long-term challenge that has to be managed and mitigated. For as long as we use the Internet, adversaries like Putin's Russia and many others will seek to exploit this technology and our dependence on it in realms that range from politics and business to warfare itself. In response, the United States can build a new set of approaches designed to deliver true cybersecurity, aiming to protect ourselves better, while reshaping adversary attitudes and options. Or, we can keep on talking tough and simple, and continue to be a victim.

Biography

Peter Warren Singer is Strategist and Senior Fellow at New America, a nonpartisan thinktank based in Washington DC. New America's funding, including full list of donors and amounts, can be found at: <https://www.newamerica.org/contribute/#our-funding-section>

Singer is also the author of multiple bestselling and award-winning books, including Cybersecurity and Cyberwar: What Everyone Needs to Know and Ghost Fleet: A Novel of the Next World War, an editor at *Popular Science*, where he runs the "Eastern Arsenal" reporting on Chinese military technology, and a consultant for the US military, intelligence community, and tech and entertainment industry. Further background at www.pwsinger.com.

Note: If the website or PDF this statement is posted on restricts rollover links to the references embedded in the text for any sources, quotes or statistics, they will available at the posting on www.NewAmerica.org