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 if 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 then 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 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 response 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 questions 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

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu