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 the 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 though 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 ranged 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 helped 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

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