Prepared Testimony and Statement for the Record of

P.W. Singer
Strategist at New America

At the

Hearing on "Digital Acts of War."

Before the House Committee on Oversight and Government Reform
Joint IT and National Security Subcommittee

July 13, 2016

Chairmen Hurd and DeSantis, Ranking Members Kelly and Lynch, and Members of the Subcommittees, thank you for the opportunity to testify before the committee today.

My name is Peter W. Singer. I am Strategist at New America, a non-partisan thinktank with a goal of preparing the US for the new digital age; the author of a variety of books on security, including Cybersecurity and Cyberwar: What Everyone Needs to Know, a primer on cybersecurity issues, and Ghost Fleet, which is a look at the future of war; and the co-host of the Cybersecurity podcast, which Chairman Hurd was kind enough to join us for an interview last year. It is an honor to speak at this important discussion today, designed to reboot the cybersecurity conversation.

There is perhaps no national security problem more 21st century in both its definition and form than cybersecurity. And yet to solve it, the ready solution in nearly every U.S. national security conversation today is the 20th-century framework of Cold War style deterrence. It argues that the best way to stop the frustrating array of cyberattacks on the United States -- ranging from credit card theft, to emails stolen from Hollywood studios, to the millions of security clearance records lifted from the Office of Personnel Management (OPM), to not yet realized fears of a national power grid collapses or devastating military defeat through digital means-- is to demonstrate the capability and willingness to hit back just as hard.

This rhetoric of achieving Cold War deterrence by retaliation is appealing. It offers both simplicity, an easy answer that echoes back to a time of familiarity, and the allure of a rhetoric that seemingly demonstrates strength and resolve.

There is just one problem: Any cybersecurity strategy based on merely whacking back to end hacking is not going to work. This is a new technology and a new era, and U.S. deterrence thinking needs to reflect our new needs.

Not Your Grandfather's Deterrence: Why the Cold War Parallels Fail

In the Cold War, the challenge was huge, but the problem was relatively simple. The opposing sides possessed roughly the same type and number of weapons, and these weapons affected them both in roughly the same way. The attack to be deterred was a clear and obvious one, with clear attribution that assured mutual and equal destruction in a massive mushroom cloud. Thus, building up a potent offense, and being willing and able to use it, translated directly into deterrence.

Today, though, there are seven key differences that mean the Cold War model of deterrence is not an apt one to deal with the threats of a new digital world.

First is the different civilian versus military makeup of the issue. In the Cold War, while support of the population mattered, the basic competition of deterrence came down to the two sides' defense and strategic nuclear establishments. Today, the domain in question is civilian-owned and operated (even 98% of US military communications go over civilian systems), meaning everything from the technology itself is to many of the most important players are civilian, from the protectors (civilian government agencies like the FBI and DHS to cybersecurity firms) to the targets themselves (civilian agencies like the OPM or NASA to the individual victims of over $1 Trillion in cybercrime).

The relative position of the military and civilian world is also reversed. In the Cold War, the military led the way, including even funding the creation of the Internet itself. Today, it is the civilian world that is often doing cutting-edge work in everything from finding new zero days to building new means of encryption. This applies even to the human resources side. There was no private market in the Cold War for missileers in the same way that there is a booming cybersecurity industry that rivals and sometimes surpasses talent inside of the military, as well as makes it harder to retain.

Second, today, there is no "mutual" to balance, let alone "assured" nature of any action, nor "destruction" of the same scale. The United States is arguably more vulnerable to cyberattack than any of its adversaries, largely because of its wide commercial, military, and cultural dependence on the Internet. This feels daunting, but is, on balance, a good thing. North Korea, for instance, may be in the seemingly enviable position of being the world's least vulnerable nation to cyberattack. But this seeming strength comes at the cost of global isolation, dictatorship, and an economy that relies on military-run pig farms.

Likewise, while conventional and nuclear weapons have highly predictable, i.e. "assured," consequences, cyber attacks are uncertain by their very nature. Their impact depends on multiple, often unpredictable actions, and often have second and third orders effects unanticipated by their designers. The (at the time) covert operation to deploy Stuxnet in 2009-2010, for instance, was arguably one of the most successful digital attacks in history, as it successfully sabotaged Iranian nuclear research equipment. Yet, the software was discovered as it popped up in some 25,000 other computers located around the world, from Belarus to India, contrary to the operational plan.

Finally, while there are great threats and costs from cyber attack, no human has yet been directly hurt or killed by one. Of the very few attacks that have caused physical impact (three are most commonly recognized at this time: Stuxnet, the 2015 Ukrainian power grid hack, and a suspected attack in 2014 at a German steel factory), the actual destructive damage has so far been limited to less than a grenade could do, let alone the Hiroshima device. Looking forward, we can envision cyber attacks that would cause great physical damage and even death, such as the take down of a city or even entire region's power grid. Yet, even in such worst fears, the death toll would still be orders of magnitude smaller than the toll of a single nuclear bomb, let alone the all out thermonuclear war between the US and USSR that threatened human existence and thus was truly MAD.

Third, there is an inverse relationship to conventional military strengths and weaknesses that guided us in the past. Underpinning Cold War deterrence strategy was that the United States perceived itself weaker than the Soviet Union in conventional warfighting, worrying about a quick takeover of Western Europe by a larger Red Army. Thus, it relied on the threat of nuclear response to avoid an unequal conventional war. Today, we face an opposite dilemma. It is the United States that has the conventional edge on its adversaries and our attackers see cyberattacks as their asymmetric way to work around a power imbalance. This points to a key aspect in our deterrence today: our willingness and ability to escalate in the opposite direction as the Cold War. If an act in cyberspace is an "act of war,' we retain the option to respond with acts of war in other domains where we may have an even great advantage, with the knowledge of that fact providing an added dose of deterrence.

Fourth, the timing is fundamentally different. The physics of a ballistic missile's speed and arc determined conceptions of deterrence during the Cold War. The critical 30 minutes it would take an intercontinental missile to fly across continents was essential to planning and strategy.

In cybersecurity, however, time operates by different rules. While cyberattacks seemingly move at digital speed, the ones that are actually effective take months or years to plan, organize, conduct, and -- most importantly -- detect. An attacker often carries out long periods of preparation and intelligence gathering, all with the goals of gaining and keeping entry. The alleged Chinese OPM hacks that stole sensitive data of over 21 million Americans may be on policymakers' minds now, but the attack actually started as early as March 2014, well over a year before it became an issue of defender or Congressional awareness. Indeed, the average time it takes a victim of a cyber attack to detect that they have been breached is 205 days. In its study of APT1, a hacking campaign linked to the Chinese People's Liberation Army (PLA) Unit 61398, the security firm Mandiant found that the unit spent as long as 5 years undetected inside several of its targets' networks.

It is not just about preparation or detection; the timeline of reaction is also fundamentally different. As opposed to the need to act within the tight, 30-minute window of Cold War missiles, in cybersecurity the defender's best move may well not be to strike back as rapidly as possible, but to show no outside awareness of the ongoing attack. This complicates the attacker's damage assessments. It even allows the victim to turn the tables and steer the attacker into areas where they cannot do harm, or feed them false information that undermines their whole endeavor.

The weapons also come with different timelines -- not just in their creation, but also in their utility. The Minuteman Intercontinental Ballistic Missile (ICBM) was conceived in 1956, and served as the central tool of U.S. nuclear deterrence for the next three decades of the Cold War. But its utility did not stop there. Indeed, roughly 450 Minuteman III missiles still protect the United States today, with plans for them to serve to 2030 or even beyond. By contrast, the most dangerous cyberweapons depend on new "zero days" -- vulnerabilities the victim is not yet aware of. Yet, what is most potent today, a single software patch can render inert tomorrow.

Fifth is a fundamental difference in the players of the game itself, in their makeup, number, and interests. The actors who the United States is supposed to be cyber deterring are far more diverse than the Cold War list that included only the Soviet Union (which notably had a fairly similar power status and even nuclear doctrine). More than 60 countries have cyber-military capabilities, ranging from large and powerful states to weak regimes. Non-state actors also are in the game, and they range from transnational criminals to hacktivist networks to maybe the most difficult of all, proxy groups taking advantage of the grey space in between, sometimes working on behalf of states and sometimes on their own. Moreover, it is not just the different numbers, but that each actor comes with vastly different interests and stakes in the game. Akin to terrorism or crime, some players have assets or positions they greatly value, and thus are deterrable, while some value mere chaos, and thus are not.

Sixth, as diverse as the players are, another difference is the diversity of attacks they might carry out. Those vary from theft of intellectual property to online dumps of embarrassing Hollywood studio emails, to the (not yet realized) risks of a massive kinetic attack on critical infrastructure, such as using Stuxnet style digital weaponry against industrial control systems to collapse power grids or transportation networks. So when people talk today about their fears that US cyber deterrence has failed, they are both right and wrong. Not every kind of attack is being thwarted, yet the worst kind of attack that major states are capable of are indeed being deterred.

This variety reinforces a key aspect in the discussion of digital war: not all attacks in constitute an act of war. They range from acts of theft to protest to espionage that ranges from sabotage to subversion to the fear of an actual act of war, traditionally defined as political violence on a mass scale. The stealing of a secret, for instance, is vexing, but no nation has ever gone to war over such an event. Such distinctions are important not just in defining what is and isn't war, but also what is and isn't a US military responsibility. If every cyber threat becomes a military issue, not only is that inefficient in term of applying the right response, but it also over burdens an already busy US military.

While attribution is often identified as a central problem in cybersecurity and acts of war discussions -- unlike an ICBM, a cyberattack does not emit a clear plume of smoke to identify the attacker -- the existence of diverse attackers and diverse attacks muddies the water further: it can be incredibly complicated to determine the intent of an attack, even if its form and sender are known. When a Russian criminal group with ties to Russian intelligence was detected attacking U.S. banks in 2014, for instance, the security community debated whether it was regular old cybercrime, or an attack linked to Russian state interests, designed as a response to the sanctioning of the regime for its invasion of Ukraine. But even then, was the attack a retaliation that got caught? Or was it akin to a nuclear test in a crisis, a signal that was actually intended to be detected, as a warning of greater consequences if the United States pushed further?

The problem of comparison when it comes attack types does not stop there. Unlike in the Cold War, some cyber attacks that target the United States are the kind of attacks that we would actually like to carry out ourselves, or, in fact, already do. US Military and White

House officials reacted far more mildly to the OPM email breach than many in the public expected. Why? In part, it is because attacks targeting a government agency's networks are the bread and butter of the online espionage operations the United States implements against other governments. As Director of National Intelligence James Clapper said in June, 2015 after the discovery of the OPM attack, "You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute." When it comes to attacks like on the OPM, instead of telling the attackers "Shame on you," we need to look in the mirror and say "Shame on us for making their job so easy."

Seventh, and perhaps where the Cold War parallels fall short the most, is the idea that building up like offensive capabilities will deliver deterrence. This is a constant refrain: not just the need to build up U.S. cyber offense, but the need to make sure others know the United States has those capabilities. As James Cartwright, the four-star Marine Corps general who led much of the initial U.S. strategy in cyber issues until his retirement in 2011, said, "You can't have something that's a secret be a deterrent. Because if you don't know it's there, it doesn't scare you."

The problem is that the evidence so far disproves this link. Unlike concerns over bomber and missile "gaps" during the Cold War (which instructively turned out to be wrong), the United States' offensive cyberspace capabilities have never been in question. And for anyone somehow in doubt, there have been series of public releases that further confirmed it. These included Washington policymakers' leaks designed to take credit for Stuxnet, and then Edward Snowden's 2014 dump of some 1.4 million NSA documents. While Snowden's disclosures obviously angered his former employers, they also show that the experts at Fort Meade have much to be proud of. The NSA has developed unmatched, amazingly exotic capabilities, from a mindboggling scale of global monitoring devices to new classes of cyber weapons that use radio signals to jump software over the previously protective physical divides between systems. And the leaks show the capability is not mere lab work, but that the NSA has used them in operations against targets ranging from Iranian nuclear research facilities to Chinese command networks.

Yet despite this clear and continual gain in offensive capability and the demonstration of its potency, attacks on the United States have only grown, in both number and in intensity. In the year after the Snowden leaks proved the U.S.'s offensive prowess, there was 55% more data lost from hacking than the year before -- and that does not even include the operations targeting major government sites like OPM or the Pentagon's Joint Staff network that began in that same period.

In sum, the flaw is not with deterrence theory, nor with cyber weapons' utility. Rather, it is with the framing of the problem. We too often try to peel off the bumper-sticker version of complicated Cold War deterrence debates and apply it to a more complicated present and future.

A Deterrence Path Forward

So what to do instead? There are the three better ways for the United States to draw the right lessons from the Cold War and reach more effective and more obtainable cyber deterrence goals.

1) Set the Norms

There is a huge value in delineating clear lines of behavior in a combined commercial, espionage, and warfighting space still at its infancy. During the height of the Cold War, the superpowers may have been a button press away from thermonuclear annihilation, but they still found a way to agree on certain norms. Sometimes these were formal arms treaties; other times they were tacit codes of conduct that guided everything from limiting spy-on-spy killings to avoiding interference with nuclear commands. Cutting across all was the goal of avoiding miscalculations that could unintentionally escalate into outright war.

Today, at the global level, much of the norm discussion in the UN GGE process has been about establishing potential rules of the road for military conflict in cyberspace. Inside US defense and political circles, by contrast, much of cyber deterrence and norm discussions has been on how to end the spate of government-enabled attacks on intellectual property, which was at the center of the agreement hammered out this fall between the United States and China. There is mixed reporting since on the impact of the agreement. The overall number of IP theft attacks are reportedly down, with some crediting the reduction to the agreement, while others credit unrelated forces like domestic Chinese government anti-corruption activities.

What is clear is that three activities will continue. Theft of intellectual property is integral to the Chinese mercantilist economic model, so while the number is down, the overall practice is, and by all indications, will still continue. In turn, the United States is wedded to the open flow of information, but Beijing sometimes interprets platforms that share freedom of speech as "information attacks" that threaten its internal stability. So China will perceive itself under continued attacks of a different kind from the US. And both sides, whose militaries are engaged in an arms race in the Pacific, will continue to engage in espionage to better position themselves if there was outright war.

This dynamic illustrates how reaching a formal prohibition on cyberattacks of any and all kinds between the 21st century powers unlikely. It does not mean, however, that there is no value in engagement and norm building. Rather than a treaty or agreement that unrealistically tries to create a Cold War-style regime of deterrence or arms control, the two sides need to flesh out a mutual understanding of the new rules of the game. Both sides must understand that their opponent will continue to conduct cyberactivities ranging from espionage to theft. The most important goal is not to stop every cyberattack, but to keep them from escalating into something far more dangerous.

This leads to a fundamental change in the typical deterrence discussion. 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.

This returns to the point that not all 'cyberattacks' are act of war. No one wants their state secrets stolen, for example, but it is part of the expected dance of great powers in competition. By contrast, there are other attacks that may not be clear acts of war, but they should be a focus on norm building to prohibit, as they make war more likely. Introducing the digital equivalent of a dormant Tasmanian devil into a nuclear power facility's operating system 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 event 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 in this space, from U.S. agreements on cybersecurity with to the two U.N. General Assembly resolutions that call for respect of the laws of war in cyberspace, to the Tallinn Manual process.

Yet, for all the laudable work in building norms, what threatens to undermine norm-building is inaction when acts clearly violate the norms. One of the consistently agreed upon norms is not to target clear civilian infrastructure with the intent to cause widespread damage (as opposed to monitor or steal information), even more so outside of declared war. Such attacks are viewed as violating the norms of necessity and proportionality that underpin the 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 a 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 (going back to the issue of proxy actors, they have not made clear whether it was government or non government but government linked actors). 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.

2) Deter Through Diversity

Nothing above argues against building up offensive capabilities for cyberspace. 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.

We can and should continue to build our offensive cyber capabilities. The key to their optimal effectiveness, though, will be in doctrine building and integration; i.e. how we meld activities in the cyber domain with conventional operations in the air, sea, land, and space. Achieving ranges from bolstering training and operational planning to clarifying command

and control relationships. Indeed, if there is a historic parallel to worry about, it is not Cold War battles never fought, 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.

That a cyber weapon is not like a WMD does not mean the United States has no options to exact costs on would-be attackers to change their calculations, the goal of deterrence outside of war. Indeed, it may even have more. Just as the timeline is stretched out and the players are proliferated as compared to the Cold War, the options for responding are proliferated. True deterrence building responses can come after the fact and in other realms. For instance, our only option is not to respond to IP theft by taking the exact same action, in the same domain. The defender can also go after other assets valued by the attacker or even those valued by third party actors, from sanctioning companies benefiting from stolen fruit to personal level actions like threatening to revoke valued visas for regime leader family members to attend US schools. Indictments of individuals involved in hacking might 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. This dynamism complicates things to a degree that even the most brilliant Cold War strategist would find vexing.

The raised options increase the complexity we have to work through. Leaders will have to game out not merely the first two moves of the response -- the simple "shoot and shoot back" dynamic that was the whole of thinking they needed in any Cold War nuclear exchange -- but plot out moves in multiple stages by multiple actors. For instance, the success of legal or trade sanctions will depend not just on whether a punishment for past attacks would stop future attacks, but also what the United States is prepared and willing to do in response to loss of market access were China, say, to respond in kind against some American firms.

Creativity and flexibility will beat simplicity in this dynamic. Indeed, the United States may even steal ideas from one attacker's playbook as a useful tool against another. From Sony to Snowden, leaked emails and documents have been among the most vexing incidents for cybersecurity. But the irony is that here the lack of mutuality is to our advantage; the U.S.'s system of government and open society is least vulnerable to them. For all the sturm and drang over revelations of questionable metadata collection and Angelina Jolie gossip, U.S. political and societal stability has never been at risk from this practice of what is known as "doxing," Yet, as Catherine Lotrionte at Georgetown University has noted, threatening to reveal the private financial data of a regime's leader, his family, or allied oligarchs, may be far more potent. In thinking through such targeting for cyber deterrence, we can see sometimes see what regimes fear most by what they ban. Witness the different responses to the Panama Papers, which were short-lived news articles of interest in the US, but led the Chinese government to censor discussion of even the word Panama on its social media.

Across all these efforts, the goal is not to prevent all attacks, like MAD did with nuclear weapons. Rather, it is to change the potential attacker's calculus on whether an individual cyberattack will be beneficial in the final tally.

3) Shake It Off: Build Resilience

The third, most apt lesson from a deeper dive into the Cold War deterrence debates is the value not just in raising the costs, but also in limiting the adversary's potential gains. This is known as "deterrence by denial" -- making attacks less likely by reducing their likely value. In today's parlance, this is the crucial idea of "resilience." If Congress wants to evolve the cybersecurity conversation, it should move resilience to the center of it.

In both strategy and football, sometimes the best defense is a good defense. A half-century ago, strategic planners did not just talk about striking back as the key to deterrence, but also on having "survivable" counter or "second strike" missiles that would nuke the other side, even if it tried a sneak attack. This is why the United States put missiles on expensive submarines and in hardened siloes.

Resilience today is about creating the capacity to power through an attack and shake it off, thereby limiting the gains to the attacker and recovering rapidly from any losses. Building resilience is not as politically appealing as striking back with new cyberweapons, because it means accepting that this is a digital world where the risk of cyberattacks is not going away. Yet it is more realistic, as well as where the United States would be getting far more deterrence bang for its buck. Most importantly to the problem we face in the diversity of cyber problems, it is useful for responding to them all. The great value of building resilience is that it applies to any kind of attacker and any kind of 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, will reach $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.

In the broader federal government, the cybersecurity budget for 2016 is 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.

In October, the White House issued a post-OPM "Cybersecurity Strategy and Implementation Plan" that describes a key series of steps that every federal agency needs to take. It included the basic measures that should have been in place long ago: from identifying high-value assets that need to be protected, to accelerating the deployment of detection systems. Ensuring the implementation of these steps could be one of the most important things that Congress could do on cybersecurity. Indeed, it would likely matter more than passage of the much ballyhooed cybersecurity information sharing bill. While the bill had many laudable aspects, 87% of cybersecurity experts think it will not affect the number of major security breaches.

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.

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. 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.

How this ties together to Congress's role in evolving the cybersecurity conversation is that *we have to rethink the role that government can play in linking cybersecurity policy, markets, and citizenry's 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, funding research on under-studied diseases, and serving as a trusted exchange for information provided by groups ranging from universities to drug companies. A cyber CDC could meet some of the same needs in cybersecurity.

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. 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 injecting more life into this marketplace. We are certainly not at the point yet in the debate to where such insurance should be required, but Congress can 1) hold hearings to better understand the field and draw attention to its possibilities, 2) help establish an Insurance Laboratory within the National Institute of Standards and Technology (NIST) cybersecurity process, 3) work with the industry and state partners to encourage 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 4) explore the passage of a Cyber 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. 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 administration's work in creating a "Cybersecurity Human Resources Strategy" is another of the new, and much needed, milestones in building greater resilience by targeting gaps with scholarship programs and other incentives. But it will fail if it only puts new people in old organizational boxes, using the same pipelines.

Attracting more talented civilian expertise into the government can aid in an overall national strategy, by supporting a "deterrence by denial" strategy across 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. Even after the OPM debacle, however, there is still not a parallel one to shore up cybersecurity.

Here again, Congress can rewrite the conversation by pulling from best practices that bring together the public and private sector in a manner that cuts across traditional partisan lines.

A good illustration is the Pentagon's recent adaption of a "bug bounty" program. This is a program that offers small rewards (The Pentagon program rewards ranged from $100 to $15,000 for a person that identified multiple security gaps) to encourage a "crowd sourced" solution to cybersecurity; in essence it enlists the ingenuity of citizens to find the holes in our security before the bad guys do. The Pentagon's experiment with this project 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 it 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 18 year old David Dworken, who did it during his high school AP exams. Congress could play a powerful role in aiding and encouraging the spread of such programs to other federal government agencies, as well as 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 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 followed a different strategy, choosing 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, 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 more akin to the U.S. Civil Air Patrol, where citizens can build up their own aviation skills, but also volunteer to aid government in aviation-related emergencies. Just in this case, it is a mechanism for Estonian citizens to volunteer their expertise for cybersecurity. They aid 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; 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 perhaps the best-equipped nation in the world to weather one now. 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.

Conclusions: Reaching Real (Cyber) Security

The overall lesson from Cold War deterrence is that the most dangerous period was when both the new technology and the new competition were not well understood -- which made bluster and escalation seemingly easy remedies to complex problems. Fortunately, cooler heads prevailed and the U.S. built up a system that delivered actual deterrence.

Today, we have a similar choice when it comes to the risks of digital attack and the conversation we have about how to face them. The United States can build a new set of approaches designed to deliver true cybersecurity, aiming to both better protect ourselves while reshaping adversary attitudes and options. Or, we can keep talking tough and simple about cyber deterrence, and continue to be victims.

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 blog 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 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