Testimony to the Cybersecurity, Infrastructure Protection and Innovation Subcommittee of the House Homeland Security Committee

Niloofar Razi Howe

Senior Fellow, Cybersecurity Initiative, New America

October, 22 2019

Chairman Richmond, Ranking Member Katko, distinguished committee members, thank you for inviting me to testify on cybersecurity and emerging technologies. I am a Senior Fellow in the Cybersecurity Initiative at New America, a DC-based non-partisan think tank, and have spent close to three decades in the technology sector, the last 15 years focused on innovation in the national security and cybersecurity sectors. I have been a venture capitalist, an entrepreneur, and a corporate executive in the cybersecurity industry. I am also a member of a number of corporate and government advisory boards.

Overview: Where We Stand Today

We must rethink our approach to cybersecurity and cyber defense.

We are at an inflection point as enormous technological and societal shifts are converging to reshape the national security landscape and the underpinnings of our democracy. The world is changing dramatically with the speed, scope and scale of nothing we have ever experienced. New, highly advanced technology is being adopted at a blinding pace as we digitize business, economic, defense and social infrastructures. We are embracing cloud computing, autonomous vehicles, small low orbit satellites with advanced sensor platforms, the Internet of Things (IoT), drones, distributed ledger technology, augmented and virtual reality. On the horizon we see the emergence of 5G and microsensor proliferation, autonomous weapons (for both military and private use), quantum computing, artificial intelligence and synthetic biology, to name a few. It's an exciting time, but there are consequences. Over time almost everything that we have experienced in the physical world - prosperity, democracy, corruption and warfare - will happen digitally but with a speed and severity that we are just starting to comprehend. This isn't about technology alone or something that takes place in a dark corner of the Internet somewhere. It's happening every moment in our offices, our cars, our family rooms and in our children's pockets. Every device is a supercomputer, every application an attack vector, and with the Internet, "every sociopath is now your next door neighbor." This is a defining moment for our society as we face emboldened groups of adversaries with complex motivations creating new social, political and economic challenges that we are out of position to deal with and almost out of time.

Good cyber hygiene is no longer sufficient as the path forward in the face of increasing sophistication and the volume of threats our society faces. In cyberspace, we are certainly in conflict, and many believe we are at war every day. Our adversaries are committed, well-coordinated, persistent, and agile and they are growing in number, especially as we continue to digitize the world, including some of the world's most fragile societies. They are focused on using digital tactics to exploit weaknesses in our technology infrastructures and in our human nature. They are penetrating the seams that exist in society, sometimes for greed, sometimes for power, and sometimes for their national security imperatives.

For decades, our nation has played a critical global leadership role, providing vision, diplomacy and stability to further our interests and our allies' interests, and this role is core to the trust and partnership required for a stable society and effective governance at home and around the world. We must do this in the digital world as well. To move us to a world of trustworthy systems and a resilient society, we must reclaim our technology innovation edge and set the standards for our digital infrastructure, which increasingly underpins every aspect of our existence. We must work together—individuals, businesses, innovators, technologists, educators, policy makers, and our government and military leaders-- to define this new world order in cyberspace, or at least mitigate the risks that compound with every moment.

And we must move fast.

It took centuries for Gutenberg's invention, the printing press, to fundamentally change society by transforming information sharing and communication. The Internet has transformed society on a fundamentally different, faster timeline. Today, time is not on our side. Our starting point is a society that is polarized, a political system that is under attack, and a way of life that feels remarkably uncertain and fragile to many Americans. The accelerating pace of technology innovation for the first time in human history is outstripping our ability as humans to adapt, adjust our policies on a timeline that is meaningful, and avoid the inevitable widening of the income divide in society that this acceleration will drive. Automation will diminish the importance of labor over time adding to income disparity between the highest earners and the low wage labor force, reinforcing a belief for many in our society that the future will not be better for them or their children. In fact, an Oxford University study estimates that 47% of total US employment is at risk with automation. It is these seams in society that our adversaries are exploiting. They are using cyberspace to undermine the very foundation of our democracy. The amplification of polarization as a result of the structure of our technology platforms as well as exploitation of those platforms by our adversaries to sow discord and chaos in society has undermined the effectiveness, stability and consistency of our government leaders and policymakers to address

these pressing problems and to find common ground to rally around as a society with shared values and a shared vision for the future. Not surprisingly, people's faith and trust in their leaders —government, business and religious leaders-- continues to decline, especially and most alarmingly, among our youth.

We must also move fast because our people and our businesses will not wait for our policymakers to catch up or security to be designed in before they embrace new waves of technology innovation that can bring with them new disruptions to society. IoT, powered by 5G networks, will be embraced by businesses to take advantages of the $11 trillion of economic gain waiting to be captured. Many of these devices are inexpensive and rely on slim profit margins and with little to no regulation or liability they generally lack even the most basic security features we have come to expect in our connected devices. The result is that most IoT devices have known vulnerabilities, and they have already become a key component of adversary attack tactics such as botnets. IoT devices are proliferating in every corner of society from business-to-business applications in manufacturing, agriculture, healthcare, and transportation to consumer applications such as home automation. As a result, the vulnerabilities of these systems will also proliferate into every aspect of our corporate and personal lives.

The growing market in low orbit satellites, which gets little airtime from security and privacy experts, threatens to form the most ubiquitous surveillance platform ever built with no meaningful regulation to control what they are used for or by whom. These platforms can now be easily tasked by individuals at low cost with few limits, regulatory or technical, on what they can be tasked to track or what information they can obtain and sell. The privacy debate, which is a critical corollary to any discussion about cybersecurity, needs to take into account the implications of the 4,000 satellites that are being launched into orbit.

The consequences of the digitization of fragile societies without thought to security ramifications poses a credible security risk both to those societies and possibly to the broader interconnected world. While over half of the world's population is online, many of the people who are now being brought online live in some of the world's most chaotic geographies. As these populations get connected via the Internet, with few norms to truly govern their behavior or those who seek to destabilize and manipulate them, we must be prepared for new forms of malfeasance and exploitation.

As more money pours into artificial Intelligence from governments and technology firms, the ramifications are poised to be immense and by definition beyond what the human brain can comprehend. We can expect every industry and every aspect of society to be impacted by AI.

What this impact will be exactly is yet to be fully understood and must be carefully researched and studied at every stage of development.

Our adversaries have repeatedly shown in the past that they can move faster than we do in the United States. We have witnessed how quickly they can adapt and exploit technology while we grapple with emerging technologies, emerging social norms, and a political process that does not function at cyber speed. While we have been studying the problem of cybersecurity, cybercriminals have innovated and adapted. Cybercrime is now an industry, often protected by the governments of the geographies in which the cybercriminals operate, and has quickly grown to be the most lucrative form of crime, overshadowing the global illegal drug trade. The Hacker-Industrial Complex - networks of cybercriminal who crowdsource their tools and share their services - continues to operate with little fear of prosecution or retribution.

Just in the past few years, ransomware, which started out as a troublesome cybercrime issue for petty criminals to extract value from locking down access to data, has grown to represent a national and homeland security issue threatening the very ability of our government to provide services to its citizens. This past year multiple jurisdictions in the United States were hit with ransomware attacks that crippled municipal services for prolonged periods of time. If this was a testing ground for a new attack vector, these incidents proved the vulnerability of our under-resourced state and local municipalities to ransomware attacks and the potentially disastrous effect on the communities they serve.

Our adversaries over the past three years have developed a better understanding of, and therefore improved their use of, social manipulation through the internet. The growth and reliance on social media in the United States has enabled our adversaries, especially Russia and China, to engage in State on Individual activities (manipulation) exploit vulnerabilities in our society, amplify polarization, radicalize our youth, and undermine any sense of objective truth in society. By definition, polarized societies are ineffective at governance as there is no common ground to build consensus to enact bipartisan policies, laws and regulations that benefit all of society. As our ability to govern erodes, so does people's faith in the government leaders and their political system. A recent Pew Research study found that Republicans and Democrats are more divided along ideological lines – and partisan antipathy is deeper and more extensive – than at any point in the last two decades. The "middle" has literally disappeared.

Underpinning all of these issues is the fact that human beings have a flawed operating system (OS) that relies on outdated mental models and cognitive biases that perhaps were useful when we lived in caves, surviving attacks from the wild, but do little to help us in the age of technology acceleration or protect us against our increasingly vulnerable digital existence. This flawed

human OS sits at the intersection of our networks and devices and continues to be the weak link in our security programs and architecture. For example, 91% of all cyber attacks start with a phishing email, which still drives a better response rate than most marketing programs. This flawed human OS is also responsible for developing the policies, laws and regulations to protect our people and our businesses from harm. The pace at which we have historically developed societal and government solutions, adapted to new technologies, and built consensus with respect to our most pressing problems is too slow for the age of technology acceleration. It is time to change our perspective and mental model with respect to the timelines we must operate on, the agility with which we take action, and the collaborative model we employ. Our adversaries have.

Where We Need to Go

It is critical to put in place the right policies to address our most existential threats in real time. It is time for the United States to set a bold cyber agenda capable of restoring trust globally- trust in our technology, trust in our systems, trust in our infrastructure, and through that trust in our political system, our political process, and our leaders. To be effective, our government will have to do this in partnership across the government and with the private sector. There is no time for silos or provincialism as we turn into solving an existential crisis for our homeland, for the people, and for the world.

A bold new cyber agenda should include the following elements:

1. **Speed and transparency**: The US government must remove any barriers that prevent government agencies that have threat and adversary information from sharing that information real-time and with context with the entities that are most affected. Sustained and real-time cooperation and collaboration between all relevant government agencies and the private sector is the only way to rebuild trust and have a real impact on our adversaries. We now have multiple agencies with unique capabilities to help the private sector, including The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Protection Agency (CISA), United States Cyber Command, the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and sector-specific agencies such as United States Treasury and Department and Energy (DOE) to name a few. Each plays a unique role in the nation's cybersecurity mission, but only if they are working together and without barriers and provincial turf wars, can we actually change the landscape of cybersecurity for the country. The Russia Small Group, with a clear mandate to protect the 2018 elections, was a tremendous example of what happens when we bring the full power of multiple government agencies to solve a problem, hand-

in-hand with the private sector. We need to rethink our US government operating model to empower consistent and real-time coordination and collaboration. Many of the authorities for securing our systems were written long before there was a commercial Internet. We need take a holistic look at these authorities through the lens of how we can most effectively defend the nation, our enterprises, and our people, with the goal of enabling effective real-time consistent collaboration and coordination.

2. **A relentless focus on unique value drivers and outcomes.**
    a. **Government's unique role.** Government must do what only the government can do—deter malfeasance in cyberspace, especially by nation-state adversaries, by using our tools of national power against those adversaries who are harming us. The private sector cannot defend itself alone against nation-state adversaries and criminals who are agile, persistent and creative. Even the strongest walls will eventually succumb to a capable well-funded adversary if there is no deterrence. This is uniquely the government's role. Peter Singer, a Senior Fellow at New America, wrote last year about the collapse of cyber-deterrence: "Less generously, these trends have created the opposite of deterrence: incentives. The failure to clearly respond has taught not just Russia, but any other would-be attacker, that such operations are relatively no pain on the cost side, and all gain on the benefits side. Until this calculus is altered, the United States should expect to see not just Russia continue to target its citizens and institutions but also other nations and non-state groups looking for similar gains." Strong deterrence is the cornerstone of any security framework and the US government must take up this challenge in a decisive way, with a consistent policy and framework for imposing cost on those who do us harm.

    b. **Private sector's unique expertise.** The private sector has developed deep technical expertise in certain domains and the US government must leverage the private sector better and not duplicate effort in areas where private sector capabilities now surpass government capabilities. In the threat intelligence market, while US intelligence agencies can bring the full power of their capabilities to bear on a selected basis producing unique insights into foreign adversaries, the private sector has advanced capabilities across a broad group of actors (foreign and domestic), including insight into attacker behavior, tactics techniques and procedures (TTPs), and campaigns. Coordinating intelligence between private and public sector to understand adversary behavior and create a coordinated response to defend and defeat the adversary is critical. As we build and invest in

government capabilities, we must be careful not to duplicate or compete with private sector capabilities.

3. **Resilience to ransomware**. Ransomware is no longer just a cybercrime issue. Ransomware at the state and municipal level is a national security and homeland security issue. The single purpose of government is to provide services (including protection) to its citizens. Ransomware at scale keeps that from happening as we saw in Baltimore, Atlanta and the State of Texas. A ransomware attack during an election would have devastating affect not just on the election itself, but on people's trust in government and the validity of our political process. State and municipal administrations need federal help in the form of standards, grants, developing response plans, and tax incentives to invest in infrastructure that can be resilient to ransomware attacks and making government systems resilient to ransomware attacks should be a high priority for Congress. It will take a coordinated effort across the whole of government, but especially DHS CISA, NIST, FBI and NSA's Cybersecurity Directorate, working hand in hand with state and local agencies, to make progress against this real threat and to stay ahead of the adversary.

4. **Support secure smart cities.** As a corollary to the ransomware issue, Congress should provide more support to sub-federal entities to collaborate on smart city modernization projects. Our cities do not have the expertise to defend themselves on their own nor the resources to do it. As our cities become smarter, they must do so with security in mind or these modernizations could unwittingly enable disruption of the government's core function of providing services and security to its citizens, and given the criticality of municipal services, actually lead to loss of life. As Natasha Cohen and Brian Nussbaum write in their New America report *Smart is not Enough*, "Despite increasing concern from the information security community, it is far from clear that even the smartest of U.S. cities are in a position to deal with the full range of new risks that the technology may bring. The required financial, social, security, operational, legal, and policy innovations needed for smart cities to deliver on their aforementioned promises do not appear to be moving at the pace of innovation of the technology."

5. **Commit to regaining our innovation edge.** Government funding of innovation so that the US can regain its edge in next generation technologies will be critical to ensuring that those technologies and the infrastructure that supports them is secure by design. While venture capitalists invest over $5 billion per year conservatively in cybersecurity companies and technologies, with a myriad of Innovation competitions such as the RSA Conference Innovation Sandbox and Launchpad Competitions held each year during the

RSA Conference, which now boasts close to 45,000 attendees each year, private sector investment is focused on building businesses based on proven technologies and established market demand. That is not where the funding gap exists. The United States must significantly increase (to the tune of multiple of current federal R&D budgets) its funding in basic and applied research in the areas identified by the U.S. intelligence community such as artificial intelligence, 5G, and quantum computing in order to meet its declared national technology priorities. It is time for the government to fund a bold innovation agenda that will carry us forward to 2030 and beyond, and commit to regaining our innovation edge in these critical next generation technologies.

6. **Fund media literacy programs.** We live in a polarized, hyperconnected world of impatient digital citizens who are being continuously and creatively targeted with misinformation. Developing and funding a media literacy program that teaches individuals how to discern the difference between fact, opinion, misdirection and lies, is critical to a well-functioning society and should be a homeland security priority. IREX, a global development and education organization, developed a Learn to Discern education program for the Ukrainian Ministry of Education to combat Russian disinformation campaigns. Their program integrated information consumption skills into existing secondary school curricula and teacher training programs at pre- and in-service teacher training institutes. Working with the non-profit community as well as the private sector, the US government should fund the development of similar programs and curricula in the United States for our elementary, middle and high school students as well as for teacher training. With a broad media literacy campaign, we can build resilience to state-sponsored disinformation campaigns, help individuals recognize divisive narratives and hate speech, and improve our youth's ability to navigate increasingly polluted online spaces in a safe and responsible way. As we do this, we must pay close attention to misinformation innovations such as deep fakes, which present a unique challenge, and fund research aimed at identifying and mitigating the threat they pose to the very concept of objective truth.

7. **Commit to building a diverse workforce in cybersecurity**. The government is in a unique position to contribute and commit to purposefully reducing the skills shortage in the cybersecurity industry. While there are some great programs in place, including DHS' CyberPatriot competition, CyberCorps Scholarship for Service initiative, and the April 2019 Executive Order focused on reskilling and upskilling federal employees, more needs to be done to recruit individuals from outside our typical skill sets (IT, law enforcement and military) with a clear mandate of solving the diversity gap in the industry. The cybersecurity workforce today significantly lags behind the broader technology industry in terms of diversity and to solve our skills shortage we need all of society to be inspired

by the mission to reclaim cyberspace for good. Elizebeth Friedman, one of the most prolific codebreakers in US history had no background or training in mathematics or linguistics and yet was able to break any code in any language during and after World War II. We need to inspire a new generation of Elizebeth Friedman's to consider a career in cyber. There are a number of good examples of reskilling efforts in both the public and private sector. The UK Cyber Retraining Academy is an effort by the UK government in partnership with the SANS Institute to reskill individuals with high natural aptitude, but no formal cyber background, to enroll in an intensive 10-week program preparing them for a career in cybersecurity. Google launched Google IT Support Professional Certification under its Grow with Google initiative through Coursera, offering a way for anyone from any educational background to get a start in the IT field where the average starting salary for IT support is $52,000 per year. The Homeland Security Act of 2002 envisioned the creation of a National Emergency Tech Guard program, a corps of volunteers whose training is funded by the government and who can be deployed during periods of crisis to restore critical systems and services to their communities. Policymakers should support, fund, expand and incentivize similar initiatives with a mandate of driving diversity in the industry. This commitment would not only help solve the industry's skills shortage, bolster our resilience during times of crisis, but would help address the "digital divide" of the haves and the have nots in our society. As we look to the future we will have to ultimately commit to completely rebuilding our digital infrastructure, cities and nations to face the digital and social challenges of 2030 and beyond. Investment in building the talent base in the right way to tackle this challenge is a necessity for success.

8. **Judicious implementation of regulation.** Regulation must be pursued in a focused and purposeful manner with a willingness to adjust and adapt as we evolve, as technology evolves and as our adversaries evolve. With those guiding principles, we should enact regulation targeted at very specific areas where we can have measurable impact.

    a. **Setting minimum Security Standards for IoT is critical.** Congress should enact basic regulation with respect to IoT. The US Government can help protect the 5G ecosystem of billions of connected devices by setting basic security standards, requiring features such as auto update, and importantly providing the right incentives, including tax incentives for vendors to implement these standards and corporations (including critical infrastructure) to deploy secure products and the financial headroom and reason to make changes.

b. **It is time to enact regulations on big data and social platforms.** The aim is not to regulate "Big Tech" but rather those technology platforms that facilitate communications and propaganda networks, exploit human weakness for profit, are addictive by design, reward virality, not veracity, thereby enabling destructive and chaotic social manipulation by our adversaries, without providing clear benefits to their users that outweighs these costs. These social platforms have demonstrated an unwillingness to self-regulate or put the interests of their consumers or society at large ahead of their profit motivation. The scope of harm they have caused society includes not only the amplification of polarization, but also psychological harm as the amount of stress, anxiety and depression caused by their platforms is on the rise in society and especially with our youth. They are out of time.

Conclusion

All of the recommendations outlined above are intended to support empowering a society that is resilient to the unintended consequences of technology innovation and the inevitable exploitation and use of those technologies by adversaries to gain some form of advantage. This may only be a starting point of a long journey. If our ultimate goal is defending our nation by defeating our adversaries in cyberspace rather than accommodating them, then, in addition to establishing acceptable norms of behavior, developing and committing to a consistent policy of engagement, escalation and deterrence, we must have a working model for successful public-private collaboration and engagement. Defeating our adversaries presupposes our ability to harness the vast technical expertise and resources as well as the unique authorities of the federal government, the vast technical expertise and agility of the private sector, a collaborative intelligence gathering and sharing framework, and coordinated response planning. It presupposes a society where trust exists between the private sector and the public sector, where transparency and fact-based substantive conversation, discussion and communication are the norm.

We have a long way to go, time is not on our side, but we have not yet run out of time.