House Committee on Homeland Security

"Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience"

Written Testimony of:

Michael Daniel

President & CEO, Cyber Threat Alliance

February 10, 2021

Virtual Hearing

Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience
Michael Daniel
Written Testimony
House Committee on Homeland Security
February 10th, 2021

Thank you for the opportunity to appear before you today for this hearing on Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience. My name is Michael Daniel, and I am the President & CEO of the Cyber Threat Alliance (CTA)—an information sharing organization that now includes 32 of the world's leading cybersecurity companies. Prior to CTA, I served for over 20 years in the U.S. federal government, including four and a half years as Special Assistant to President Obama and Cybersecurity Coordinator at the National Security Council.

Let me begin my testimony by thanking the Committee for holding a hearing on this important issue. The cybersecurity threats facing the US are significant, urgent, and potentially life-threatening—and our nation must improve its ability to counter them. This Committee plays a key role in enabling the Federal government to meet this challenge. This testimony will lay out the cyber threat landscape the US faces, the types of adversaries conducting cyber operations, and some long-term goals and principles to address these threats. I will also touch on Federal government organization, Federal agency cybersecurity, and how to think about cybersecurity in more productive manner.

The Cyber Threat Landscape

We live in a digital age. Digital technologies increase efficiency and productivity, shrink distances, and enable news ways of working and connecting. However, digitization also brings challenges and potential vulnerabilities that—left unchecked—threaten to undermine our national security, economy, and public health and safety. Although the US faces a myriad of cyber threats, five trends are making these threats worse over time:

1) Cyberspace is expanding: As we connect more devices to the Internet, we are making cyberspace bigger. It is the only human environment that is continually expanding at a meaningful pace. Land, sea, air, and near earth orbit are not growing to any appreciable degree, but cyberspace is different. While estimates vary, everyone agrees that the growth is enormous. For example, Cisco conservatively estimates that by the end of 2021, 27.1 billion devices will be connected to Internet, an increase of 10 billion devices since 2016. That figure translates to 5.5 million devices per day or 60 devices every second.

2) Cyberspace is becoming more heterogenous: Beyond raw expansion, the variety of devices connected to the Internet keeps increasing. These devices are not just desktops, laptops, or smartphones. They are light bulbs, refrigerators, cars, thermostats, sensors, machine tools, dams, water purification plants, oil rigs, toll collectors, and thousands of other "things"—a huge array of different kinds of devices with different functions, protocols, and security features. The combined growth in volume and heterogeneity makes effective cyber defense extremely difficult.

3) Malicious cyber actors are becoming more numerous: The number of malicious actors in cyberspace continues to grow rapidly as hacktivists, criminals, and nation-states all learn that they can pursue their goals relatively cheaply and effectively through cyberspace. The barriers to entry are low and the potential return on investment is high. As a result, the volume and frequency of malicious cyber activity is increasing dramatically.

4) Cyber threats are becoming more dangerous: As recently as a decade ago, cyber actors generally limited their malicious activities to stealing money or information, temporary denial of service attacks, or website defacements (the digital equivalent of graffiti). But over the last ten years, malicious actors have shifted to more destructive and disruptive activities. The physical disruption of the Ukrainian power grid, the use of cyber-enabled information operations to influence electoral processes, the release of the destructive NotPetya malware, and the scourge of ransomware are all examples of this trend.

5) Cyber incidents are becoming more disruptive: as we have become more and more digitally dependent, the potential impacts of a cyber incident have also increased. It is becoming harder for us to operate without access to the Internet; the need for a significant portion of the workforce to work remotely during the pandemic highlights that dependence. What would have been a nuisance a few years ago can now kill people if they cannot get access to timely medical care due to a network outage.

Specific threats

Within these broad trends, I would highlight two specific threats:

Ransomware: Over the last couple of years, one key threat that has emerged is ransomware. This malware encrypts data on a victim's system and in order to regain access to the data, the victim has to pay a ransom. In addition, adversaries are also stealing private information prior to encrypting it and threatens to release the data publicly or onto the dark web if the victim does not pay. This threat has grown to such a degree that it is no longer just an economic nuisance but a national security and public health and safety threat.

Operational Technology malware: for many years, the computers that run operational processes in manufacturing, power generation, water distribution, and other industrial activities were largely proprietary and difficult to access from the Internet. However, these systems are becoming increasingly connected and more standardized. As a result, the ability for adversaries to target and disrupt these systems has increased. A cyber attack against one these systems would have a much higher impact across our digital ecosystem that the typical criminal activity.

Cyber Adversaries

While the number of malicious actors in cyberspace can seem almost limitless, these adversaries are typically operating as one of four types. Each type has different goals, motivations, and resources, and while individuals can operate as different types at different times, this typology is useful for thinking about how to counter the activities of a specific type.

Terrorists – many terrorist groups make extensive use of cyberspace for recruiting and communication, but fortunately very few are able to undertake disruptive or destructive actions. However, these groups almost certainly have aspirations to conduct visible, spectacular attacks

and if a nation-state decides that it is in their interest to train and equip a terrorist group, the result could be a destructive attack.

Hacktivists – this type of actor has decreased in importance over the last few years, but they can still cause problems. Their motivation is primarily to gain attention for their cause or embarrass their opponents. While they might be okay with harming a "corporation" or a government agency, they generally are not interested in causing wide-spread, permanent harm.

Criminals – these actors are by far the most prevalent in cyberspace. The motivation for these actors is simple: money. They can be quite innovative and creative, but money is the driver. They are unlikely to spend time and resources trying to gain access to just one target; if their first few attempts fail, they will move on to the next target, just like in the physical world.

Nation-states – these actors are pursuing their national security or foreign policy interests through cyber actions. Such interests can include espionage, influence operations, theft of intellectual property and trade secrets, deterrence, low-grade conflict and disruption, or destruction. While some nation-states have less technical capability than some high-end criminal groups, nation-states generally have discipline, patience, personnel, and complementary capability (such as dedicated intelligence agencies) to bring to bear.

Long term goals

Given these trends and malicious actors, the US government should pursue three long term goals to counter the cyber threats we face. It should seek to raise the level of cybersecurity and resilience across our digital ecosystem; disrupt adversaries at a faster pace and larger scale; and respond more effectively to cyber incidents when they occur.

Raise the level of cybersecurity across the ecosystem – despite a growing recognition that cyber threats affect everyone, many organizations still have not implemented basic cybersecurity measures, such as two-factor authentication, and very few have reached a high level of maturity, even those that manage or perform critical national functions. They also have not developed sufficient resilience to cyber incidents. Given this situation, the Federal government should aim to improve cybersecurity and resilience across the board. Setting such a goal does not require the government to treat all organizations the same or not prioritize some functions over others; in fact, achieving this goal requires such prioritization. However, given the interconnected and interdependent nature of cyberspace, the goal should be that all organizations reach a level of cybersecurity commensurate with their size, industry, and overall function.

Disrupt adversaries at scale – since we cannot rely on defense alone, the US government also needs to increase the pace and scale of its disruption efforts, whether against nation-states, criminals, hacktivists, or terrorists. Disruption should involve all the elements of national power, including diplomatic, economic, law-enforcement, cyber-technical, military, and intelligence tools. It will also require working with private sector cybersecurity providers and collaborating internationally. While we have made significant progress in these activities over the last decade, we need to impose greater costs on our adversaries.

Respond more effectively to incidents – no matter how much we improve our defense and offense, our adversaries will sometimes achieve their goals. They will succeed in stealing information or money, causing disruption, or holding a critical function at risk. To deal with those situations, the Federal governments needs to be able to deal with such incidents rapidly and

efficiently, enabling private sector owners and operators to restore functionality expeditiously.

The US government could achieve these goals in different ways; indeed, whole books have been written on specific aspects of these three goals. However, based on my experience both in and out of government, employing the following principles will increase the chance of success:

1. *Focus on comparative advantage* – The Federal government should not try to replicate the technical capabilities available in the private sector. The technical information available to the cybersecurity industry is extensive, and the government is unlikely to have technical information the private sector does not. However, the Federal government does have unique information in the form of attribution, context, and a strategic view point. It also has a comparative advantage in funding basic R&D into cybersecurity, such as how to reduce the exploitable error rate in computer code. While some private sector entities can disrupt adversaries using a variety of means (such as Microsoft's legal actions), the Federal government can impose costs on adversaries in ways that the private cannot and should not: public attribution, law enforcement actions, economic sanctions, diplomatic actions, and other means. Focusing on each sector's comparative advantage will enable the collective whole to be greater than the sum of the parts.

2. *Incentivize good cybersecurity behavior* – While at times the government may need to compel certain actions, the Federal government should increase the incentives for organizations to implement better cybersecurity:

    - Strategic use of existing regulations – The Federal government should ensure that existing regulations promote good cybersecurity behavior, not inhibit it. Most of the time, new regulation is not required; instead, agencies should focus on implementing regulations that are already on the books.

    - Support and encourage the use of best practices – The Federal government can be a neutral, reliable party in identifying good cybersecurity practices. Two good examples are the National Institute of Standards and Technology's Cybersecurity Framework and the Software Bill of Materials initiative.

    - Drive industries to set standards of care – Establishing the generally accepted level of cybersecurity for organizations within a given industry would have a dramatic impact across the ecosystem. It would remove considerable uncertainty and enable businesses to plan investments. It would address concerns about liability and reduce barriers to collaboration and information sharing.

    - Increase publicly available information – The government can facilitate disclosure of information that can help customers, clients, shareholders, and other relevant parties take appropriate defensive actions, better assess risk, and advocate for improved security. Examples of such requirements could include data breach reporting, information about material cybersecurity risks on financial statements, and public acknowledgements about how a publicly traded company is assessing and managing its cyber risk, particularly at

the board of directors' level. Such disclosures do not assist criminals or other bad actors – they already know where the weaknesses are; instead, these requirements allow market forces to operate more efficiently. These requirements should be standardized as much as possible at the national level and harmonized at the international level to the extent possible, to reduce burdens on companies and simplify reporting for consumers.

3. *Reinforce stability in cyberspace* – Governments should strive to make cyberspace a stable, reliable environment in which to conduct business. Some key tools include:

   - Transparency – The US government should set the standard for transparency about its offensive cyber capabilities. Not in terms of details about tradecraft or tactics, techniques, or procedures, any more than we are transparent about the technical specifications for military weapon systems. However, we are quite open about the fact that we have attack fighters, submarines, and tanks. We should apply a similar approach to our use of offensive cyber. For example, we should continue to evolve our doctrine, being clear about how and when we would use cyber capabilities as a tool of national power. We should also be transparent about the fact of offensive cyber capabilities, just as we are open about our kinetic capabilities.

   - International norms of behavior – Norms can put certain activities "out of bounds." Not all nations will adhere to all the norms all of the time, but norms can help constrain behavior. Of course, we must adhere to the norms we promote—we cannot be "do as we say, not as we do" country. The US has been effective in this area over the last decade, and we should continue to build on that success.

   - Confidence-building measures – Adapting these approaches from arms control and conflict resolution field has promise to reduce the risk of escalation due to accidents or unintended consequences.

   - Coalitions of the willing – Given the divergent views among nations regarding cyberspace, privacy, and other issues, gaining global consensus on most topics is unlikely. However, this inability to reach consensus should not prevent the US from assembling coalitions of the willing. Such groups will be far more effective than trying to go it alone or letting the perfect be the enemy of the good.

4. *Increase resilience* – If we increase our ability to weather cyber attacks and maintain operations, then the value to our adversaries of conducting attacks decreases. Resilience also enables US leaders to worry less about pre-empting foreign threats and escalating responses.

5. *Increase operational collaboration between the public and private sectors* – Unlike in the physical realm, governments do not have a monopoly on cyber "force," and they are not likely to obtain such dominance any time soon. Therefore, the most effective action in cyberspace will involve public and private sector actors working together. Such

collaboration goes beyond information sharing to synchronizing activity and it already occurs in certain circumstances. However, we need to vastly expand the scope and scale of these collaborative activities if we want to have a meaningful impact on our adversaries.

Federal government organization

Given the seriousness of the threats and the broad nature of the long-term goals I have outlined, reviewing the Federal government's structure, agency roles and missions, and coordination capabilities makes sense. However, traditional policy solutions usually do not work for cybersecurity due to four unusual aspects about the issue.

Cybersecurity is inherently interagency

Bureaucracies prefer issues that fit neatly into one organization's mission. Cybersecurity is almost the exact opposite. It is a national security, military, intelligence, economic, public safety, privacy, diplomatic, law enforcement, business continuity, and internal management issue all rolled into one. It touches every Federal department and agency, and many Federal organizations have a legitimate, necessary role in cybersecurity. Thus, cybersecurity far exceeds any current agency's remit. Trying to stuff the whole issue inside one existing department or agency will fail.

Creating a "Department of Cybersecurity," will not work either – in fact, it would be a disaster. Cybersecurity is too integral to too many agencies' missions to centralize those functions in one department. We cannot remove cyber investigations from the FBI, oversight of financial service companies' cybersecurity from Treasury, incident response from DHS, and offensive cyber operations from the Department of Defense and consolidate them inside one department. FBI, Treasury, DHS, and DOD would end up recreating those functions to support their core missions. We would end up with even more complexity.

At the same time, cybersecurity's different aspects are not independent—they interact with each other constantly, sometimes in unexpected ways. Military cyber operations can disrupt intelligence activities or law enforcement investigations. Treasury sanctions could upset diplomatic negotiations. DHS' focus on mitigation could hinder DOJ's ability to prosecute a cybercrime—or vice versa. Network defenders want information from the private sector, but many in the private sector are worried about regulatory action if they share.

As a result, we can employ neither of the standard government approaches to emergent issues -- make it one agency's mission or create mutually exclusive agency siloes for different aspects of the problem. Instead, we must weld these disparate activities together into a single whole through regular, intense, sustained interagency coordination. Such coordination does not occur naturally in any government or large bureaucracy: personnel have limited incentives to coordinate activities across departmental and agency lines. That is not a moral failure or laziness, but a reality of human psychology. Instead, we must account for this facet of human nature and design our systems accordingly.

Inherently intergovernmental

Cybersecurity also affects governments at all levels, from municipalities to counties to state governments. It does not exclusively belong to the Federal government. As cybersecurity has become a more pressing issue for organizations of all kinds and the threat of disruptive or destructive activity has grown, the need to incorporate State, local, territorial, and tribal governments into our cybersecurity activities has grown. For example, State, Local, Territorial, and Tribal (SLTT) governments play a crucial role in a critical national function, elections. As a matter of democratic principle, we want to maintain SLTT control over elections; on the other hand, expecting an SLTT organization to defend itself against the Russians or Chinese without Federal help is foolish. Therefore, we need to enable the Federal government to collaborate more effectively with SLTT entities. In particular, the Federal government will likely need to allocate additional resources to improving SLTT cybersecurity. However, we cannot make cybersecurity exclusively a Federal or SLTT issue.

Inherently international

Cyber threats cross international boundaries quite fluidly. During my time at the White House, virtually no issue was exclusively domestic. If nothing else, much of the cybercrime that afflicts US citizens and businesses has an international connection. On the flip side, what we do domestically has implications abroad. Therefore, countering the threats we face requires significant international collaboration and cooperation.

Further, the international cyber environment is very complex, with many overlapping and intertwined issues. Internationally, cybersecurity involves diplomatic relations, law enforcement cooperation, financial interactions, trade issues, intelligence collaboration, and military operations, not to mention technology and competitiveness concerns. Trying to confine cybersecurity to a specific channel or type of interaction will not work.

Inherently public and private

Finally, cybersecurity forces the government and the private sector into a different kind of relationship. Traditionally, the government is either a regulator or a customer for the private sector. While the government does have those relationships in cybersecurity, the government and private sector can have a third type of relationship in this area, that of partner or peer. This peer relationship stems from the fact that the private sector owns and operates vast majority of cyberspace, has equivalent (or better) technical insight and capability, and can take action that affects much of cyberspace without the government. This type of peer relationship is relatively new and we do not have the necessary laws, policy, procedures, or even vocabulary to fully manage it, other than the overused public-private partnership term. Thus, we need to fully develop the laws, policies, and procedures to govern this type of interaction, so that the relationships remain aligned with our overall sense of equity and appropriate roles for government versus the private sector.

Federal agency cybersecurity

In December, several private sector companies identified malicious activity that enabled the Federal government to unravel an incredibly broad cyber-enabled espionage campaign. This intrusion effectively gave the Russian government unfettered access to numerous unclassified US government networks for over nine months. It is difficult to overstate the intelligence value the Russians gained from this access or the likely damage to our national security. That said, based on the publicly available information, the activity associated with this intrusion appears to consist of espionage, something in which all states engage. As a result, although extremely damaging to our national security, this intrusion is not an "attack."

The fact that the intrusion does not constitute an attack necessarily constrains the US response. "Constrain" does not mean "prohibit." We should respond forcefully to this intrusion through diplomatic channels, such as by expelling Russian diplomats or exacting a cost in other venues. We should also signal that if the incident turns out to involve activities other than espionage, the US reserves the right to escalate accordingly. But we should carefully calibrate our response with the knowledge that the US also conducts cyber-enabled espionage.

Regardless of the US response, the intrusion revealed some on-going weaknesses in Federal cybersecurity structure, practices, and funding. While the 2021 National Defense Authorization Act included several provisions that directly address some of these weaknesses (for example, authorizing CISA to conduct threat hunting across Federal civilian agencies), the Federal government still needs to aggressively reduce its cyber risk. First, it needs to continue consolidating cybersecurity services within a smaller number of agencies; just as with payroll services, only a small number of agencies should provide cybersecurity services to most Federal agencies. Second, Congress needs to enable agencies to retire their legacy IT systems at a much faster rate. Replacing legacy systems would reduce cyber risk, improve productivity, and enhance service delivery. The $9 billion for cybersecurity originally proposed in the Biden Administration's American Rescue Plan would help achieve this goal, especially resources allocated to the Technology Modernization Fund.

What we can expect from private sector companies

This topic is sensitive one. On the one hand, we do not want to re-victimize organizations that have suffered an intrusion, theft, disruption, or destructive attack; moreover, since no organization can prevent all intrusions all of the time, just because a company experiences a breach does not mean it has failed – it might have really excellent cybersecurity. On the other hand, companies have a responsibility to protect customer data or access to other organizations, which means implementing at least some cybersecurity measures, so it is also possible for a company to be negligent in this regard. The question lies in distinguishing which situation a company is in. Threading this needle is one of the key policy challenges for the US right now.

The solution lies in establishing standards of care for cybersecurity. These standards should vary, depending on factors such as size, industry, function, geography, etc. Standards of care exist in many industries for areas such as safety; sometimes the standards are entirely industry

driven and sometimes they backed up by regulation. These standards should not be static checklists and will need to be flexible enough to evolve as technologies and threats change.

Despite developing and implementing standards of care, the resulting improvements to cybersecurity will still be insufficient to thwart dedicated nation-state intruders. In fact, no amount of cybersecurity investment will prevent a determined nation-state from gaining access all of the time. Therefore, we should not expect individual companies to defend themselves against highly capable nation-states, such as Russia or China, by themselves. The Federal government should be able to quickly come to the aid of an organization facing a nation-state threat, whether at the request of the targeted organization or based on its own knowledge.

How to think about cybersecurity in the long-term

This testimony has identified multiple challenges for improving cybersecurity in the US. While cybersecurity may seem like an impossible task, the truth is that we can improve our cyber defenses. The answer is not purely technological, although technology is certainly required. The primary change we need to make is in our mindset. We need to change how we think about cybersecurity in several ways:

- *Adopt a risk management approach* – Cyber threats are risks to be managed, not problems to be solved. We will never eliminate cyber threats entirely, nor will we reach a point of 100% security. Therefore, we need to think in terms of risk management. Just as a company can never eliminate the risk of bad weather disrupting operations, we need to treat cyber threats as a long-term risk management problem.

- *Use more than technology to counter the threat* – Managing cyber risk effectively involves more than just employing technical solutions. Technology is necessary but insufficient for addressing cyber threats. Instead, we need to bring economic, psychological, organizational, process, policy, and legal tools to bear on the problem. Only by combining all these tools can organizations manage their cyber risk effectively.

- *Prevent adversaries from achieving their goals* – If we think about cybersecurity from a "castle and moat" perspective, we will invariably fail. No organization can prevent all adversaries from gaining access to its networks all the time. Instead, if we think of cybersecurity as preventing the adversary from achieving their goals, then we get many more opportunities for success. If we define success as preventing the adversary from achieving their goal at any point along the way, then instead of defenders having to be "right" one-hundred percent of the time, the adversary has to make zero mistakes at every step. That mindset provides many more opportunities to thwart the adversary than the old castle and moat approach.

- *Recognize that cyberspace is not a global commons* – One key barrier to thinking about cybersecurity effectively is that because we cannot "see" cyberspace directly, it feels

divorced from the physical world. As a result, we often act as if cyberspace is an amorphous domain that resembles the oceans or the atmosphere. In turn, this view leads us to act as if cyberspace has large unclaimed, "international" zones equivalent to international waters or airspace. But cyberspace is intimately tied to territory. It exists due to computers, servers, and other devices that are all owned by a person or organization and residing on someone's territory. This recognition has significant implications for how we should view cyber operations in the international context, and the rules under which we want to conduct them. I want to be clear that in adopting a view that cyberspace is tied to territory does not mean the US has to accede to the Russian and Chinese governments' view that the state should completely dominate cyberspace, controlling everything from access to content. This conceptual approach should, however, shape how the US government and other aligned nations act and operate in cyberspace.

Conclusion

Based on this testimony, many people might conclude that I am a pessimist when it comes to cybersecurity. It is easy to be overwhelmed by the volume of malicious activity and become fatalistic about cybersecurity threats. However, I reject such fatalism. While we will never eliminate cyber threats entirely as long as we live in a digital world, we can improve our cyber defenses and resilience, disrupt our adversaries, and respond to events when they occur. If we achieve these goals, then we can continue to reap the benefits and minimize the cost of an increasingly connected world. Fundamentally, cyberspace is a human-created domain and that means humans can choose to make it safer.

Thank you.