The Case for a National Cyber Director
Michael Daniel
Written Testimony
House Committee on Oversight and Reform
July 15, 2020

Cybersecurity is a new problem compared to many other national policy issues. Questions about the role of government in society or how to manage international boundary disputes have been debated for hundreds of years. We have had considerable time to try different organizational structures for other Federal government activities. In contrast, cybersecurity issues are about 30 years old – still in the toddler stage relatively speaking. Therefore, it should not be surprising that we are still working out how to organize the Federal government to manage the problem.

Yet, as even more of our economic and social life has shifted on-line as a response to the Covid-19 pandemic, the need to improve the Federal government's cybersecurity capabilities has increased. The government's capabilities must catch up to and keep pace with society's growing digital dependence. We do not have the luxury of waiting another 10 or 15 years for the issue to mature.

Thankfully, we are not starting from scratch. Over the past four Administrations, we have made significant progress, particularly in laying the necessary policy foundation. A few illustrative examples include:

- The Clinton Administration issued Presidential Decision Directive-63, which prompted the private sector to form Information Sharing and Analysis Centers.
- The Bush Administration created and funded the Comprehensive National Cybersecurity Initiative.
- The Obama Administration created the Cybersecurity Coordinator position, directed the National Institutes of Standards and Technology to facilitate the creation the Cybersecurity Framework of Standards and Best Practices, and ramped up our international engagement.
- The current administration made the Vulnerability Equities Process directive public and issued a national cybersecurity strategy.

Congress has been active as well, passing the Cybersecurity Information Sharing Act of 2015, forming the cyber caucus, and creating the Solarium Commission.

As a result of these effort, Federal agencies, particularly the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS), have made significant improvements over the last few years. Across the board, we have more capacity, more expertise, and more awareness of cybersecurity as a key policy issue. The answer to the question "Are we better off now than 10 years ago?" is unequivocally "Yes."

However, we have reached the point where making more than incremental progress will prove difficult unless we address at least four impediments. First, cybersecurity's cross-cutting nature does not fit with the US government's bureaucratic structure, making the issue difficult to deal with during policy development. Second, agencies are not incentivized to sustain the degree of coordination required for effective cybersecurity over the long term. Third, a lack of central coordination hinders effective incident response actions. Fourth, cybersecurity's complexity and unusual nature make it tough for the President and other senior leaders to tackle without access to expertise. Addressing these impediments would be challenging under normal circumstances, but this Administration has chosen to take a step backward by eliminating the cybersecurity coordinator position at the White House, which makes it even harder.

Clearly, no single policy action will solve these problems. They are too complicated for a one-shot solution. That said, creating a position like a National Cyber Director along the lines the Cyberspace Solarium Commission recommends or that Representative Langevin has proposed is a necessary part of the solution.

Cybersecurity is messy

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 role in cybersecurity. Thus, cybersecurity is too broad for any single agency's remit. Trying to stuff the whole issue inside one existing department or agency will not work.

On the other hand, creating a "Department of Cybersecurity," will not work either – in fact, it would be a disaster. To begin with, cybersecurity is too integral to too many agency's 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.

Cybersecurity is interdependent

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 personnel focus on mitigation, while the Federal Bureau of Investigation and Department of Justice concentrate on prosecution. Network defenders want information from the private sector, but many in the private sector are worried about regulatory action if they share. Welding these disparate activities into an effective whole requires intense, regular, sustained inter-agency coordination. This coordination does not occur naturally in government or any 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.

Cyber threats are intensifying

Another problem is that malicious cyber activity is going to increase in frequency and intensity over the next few years. Many countries have discovered that cyberspace is an effective medium through which to pursue their national interests. Criminals have discovered that cybercrime pays well with low risk, and hacktivists use cyberspace to spread their messages quite easily. With more actors entering the space, the rate of cyber incidents will grow. Moreover, these incidents will become more intense in their effects. Nation-states are already moving past just using cyber operations for espionage, but to shape decisions and impose costs. Criminal groups are using ransomware to cause business interruptions to extort money. On top of this expansion in the number of actors, our increased digital dependence means that cyber incidents that would have been minor nuisances a decade ago will now be organizationally catastrophic. Finally, adversaries are creative. They will find ways to attack us in ways we do not and frankly cannot anticipate. No matter how good we get, we will sometimes be surprised. Thus, we will face more frequent, more significant cyber incidents whose consequences will be impossible to predict ahead of time.

We know from experience in other areas where uncertainty is high and effects are systemic, including natural disasters and pandemics, centralized leadership is critical to effective crisis management. Without effective coordination, the response can be haphazard and can easily get in its own way. Assets will not be brought to bear that should be, or they will be misallocated to lower priority activities.

Access to cyber expertise

Finally, given the complex nature of cybersecurity and its importance to our national security, economic security, and foreign policy, the President needs an empowered senior advisor focused on this issue. Cybersecurity is not just a lesser included case in other areas; it is its own discipline with its own expertise, albeit one highly intertwined with other disciplines. Since it is unlikely that the next few Presidents will have deep cyber expertise (although I will be fascinated to see what happens what that day arrives), they will need access to a senior advisor with a cross-agency point of view who focuses on this issue.

Confronting the problems

How do we organize across agency lines, sustain interagency coordination, improve our cyber crisis management, and enable the President to get good advice? Creating a national cyber director could address these problems. I do not arrive at this conclusion lightly. Washington likes to re-arrange the deck chairs as a solution to problems and that approach often fails to yield results, so I view organizational solutions with healthy skepticism. However, after working this issue for many years, I have concluded that the nation needs a position like a national cyber director (NCD) with staff housed in the Executive Office of the President (EOP).

Why a National Cyber Director?

Cybersecurity is a strategic, national level problem that defies easy categorization. Cyberspace and the Internet are permanent features of our society, economy, public safety, and national security. We will not "solve" our cybersecurity problems; cyber threats are now a permanent feature in society and international relations. Instead, we will manage and mitigate the threat. Thus, we need a strategic level leader focused on this problem with a government-wide perspective. Moreover, we will need a national cyber director for the long-term.

Why the EOP?

The EOP is the only part of the executive branch with a sufficiently broad scope to look across all the different aspects of cybersecurity. It is the only part of the executive branch that can overcome the "you're not the boss of me" effect and incentivize agencies to engage in regular, sustained, and intense coordination. It is the logical place to organize a cyber crisis response because it can serve as a neutral, inter-agency hub and activate resources across the entire Federal government. Finally, it is the primary organization for direct Presidential advisors.

How to make the position effective

However, in creating an NCD or similar position, we should carefully scope its authorities. While it is hard to create a new position, it is even harder to make a new position effective. In creating such a position, we need to be creative, considering new arrangements that have never been tried before. As Congress debates this issue, I would urge it to consider certain parameters in crafting the position:

- The NCD Office should be big enough to run effective processes, but not so big that it tries to be operational. If we want the office to succeed, then it cannot be so small that the staff do not have time to do anything right. On the other hand, it should not be so large that its staff are tempted to try to run operations directly.

- The NCD Office should integrate tightly with OMB's budget process and NSC's policy process, otherwise it will be irrelevant. Both the Solarium Commission and the Langevin bill propose mechanisms to integrate the NCD into the budget process, and provisions along those lines would be a good lever to achieve this goal. Similarly, the NCD will need an official role in the NSC policy process. Many of the issues the NCD will work on are national security and foreign policy related, and the NSC process is the only way to reach policy consensus on these issues. Achieving this goal while allowing appropriate flexibility for executive authority will likely be difficult – no President wants Congress to mandate how the White House should be organized. One approach would be to require the position be included in the National Security Council but allow the President to determine the mechanism for doing so. For example, the President could choose to "dual-hat" the NCD as a Deputy National Security Advisor and a portion of the NCD's staff as an NSC directorate. Just because such an arrangement has not been done before does not mean we should not do it in the future.

- The NCD Office should have insight into and a policy oversight role for all Federal government cyber functions, including military, intelligence, or law enforcement activities; this insight must extend to offensive cyber operations. We cannot exclude those activities from the NCD's purview and expect the position to succeed. For the record, I strongly support the independence of indictment and prosecutorial decisions from the White House, but that separation does not mean the NCD should not understand what law enforcement operations are occurring or influence our strategic level policy toward cybercrime. If the NCD only has oversight and coordination roles for network defense activities and working with the private sector, then the position would largely duplicate the CISA director, which we do not need.

- NCD staff should not participate in policy execution. Law enforcement agencies investigates and prosecutes crime, intelligence agencies collect information, the military conducts offensive cyber operations, and the sector specific agencies work with their industries. Policy execution should remain the domain of the departments and agencies.

- The office will need a clear relationship with the Federal Chief Information Security Officer (CISO). This existing office has worked hard to improve the security of Federal networks. The NCD's office will need to work closely with the Federal CISO to ensure that Federal agencies are following the general guidance and advice the government gives the private sector. We must walk our talk.

Why not just re-create the Cybersecurity Coordinator?

Although I held a coordinating position in the Obama Administration, simply recreating the Cybersecurity Coordinator within the NSC structure is insufficient (although that would be an improvement over the current state). The NSC is designed to work primarily within the US government and to interact with foreign governments; it has strict limits on how its staff can interact with the private sector. It also is not organized to deal with implications of emerging technologies or the domestic economic impact of cybersecurity issues. However, much of the nation's cybersecurity capability and expertise resides in the private sector, and emerging technology and economic issues are pervasive in cybersecurity. Rather than create exceptions to allow one directorate to have significant interaction with the private sector or try to wedge non-national security issues into the NSC, a better solution would be to create a separate office with its own authorities, albeit closely linked to the NSC.

Conclusion

Many Federal cybersecurity problems stem from organizational shortcomings. In fact, cybersecurity itself is more than a technical problem; it is also an organization problem. Thus, effective solutions will involve an organizational element. Creating an NCD will not suddenly make the Federal government into a well-oiled cybersecurity machine, but it will put a crucial piece in place. We have built the policy foundation to improve our cybersecurity and we have made some needed organizational changes, such as establishing CISA and US Cyber Command. Now we need to take the next step and create a position that can bring it all together.