15 July 2020

Testimony from the Honorable Mike J. Rogers

Former Chairman, House Permanent Select Committee on Intelligence
Former Representative of the 8th District of Michigan

Chairwoman Maloney, Ranking Member Comer, distinguished Representatives, I am both delighted and honored to testify before you on Rep. Langevin's bill to create the National Cyber Director.

It is heartening to see so many of my distinguished former colleagues listed on this bill: Congressman Jim Langevin (D-RI), Congressman Mike Gallagher (R-WI), House Oversight and Congresswoman Carolyn Maloney (D-NY), Congressman John Katko (R-NY), Congressman C. A. Dutch Ruppersberger (D-MD), and Congressman Will Hurd (R-TX). Truly a bipartisan dream team of congressional cyber experts.

In the testimony that follows, I will outline why I believe the National Cyber Director is necessary for our Nation's cybersecurity now and into the future. I am basing this testimony on the four areas of responsibility outlined by the Cyberspace Solarium Commission: (1) principal advisor to the president; (2) national-level coordination; (3) driving the inter-agency process; and (4) budgetary oversight.

The cybersecurity challenge we face as a nation is both daunting and complex. Just when we think we have a handle on it, something new comes along and disrupts our frame of reference. Quantum computing, machine learning, artificial intelligence, 5G technology, and more, are just the tip of the cyber iceberg that is heading our way.

The 2018 National Defense Strategy rightly noted that "the re-emergence of long-term, strategic competition between nations"[1] was the primary threat to America's security. We are seeing this play out in technology and innovation as much as we are watching it in overt and covert military activities. In 2017, Russia's President Vladimir Putin said, "Artificial intelligence is the future, not only for Russia, but for all humankind… It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world."[2]

China, for its part, aims to "occupy the commanding heights of AI technology" by 2030[3] and is aggressively pursuing 5G dominance—the next generation of mobile communications that will revolutionize how we live and work. North Korea understands the value of technology and cyber capabilities, too. Kim Jong-Un said, "Cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly."[4] Iran is

[1] https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
[2] https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world
[3] https://thediplomat.com/2017/07/chinas-artificial-intelligence-revolution/
[4] https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

also developing its cyber weapons and Tehran's past behavior indicates its willingness to use these tools to attack its adversaries.[5]

If we do not get our national-level policy sorted now, and if we do not empower the right person and the right office with the responsibility today, I fear we will have a different type of Commission soon—one that looks at why a national cyber incident happened at the hands of China, Russia, or North Korea, and what could have been (or should have been) done to prevent it in the first place.

1. *Be the President's principal advisor on cybersecurity and associated emerging technology issues and the lead national-level coordinator for national cyber strategy and policy*

The current and previous administrations have struggled to handle and manage cybersecurity policy and emerging technologies. This is not a failing inherent to the composition or structure or political ideology of these administrations, but a result of the rapidly changing and complex digital world clashing with the information era.

Our federal government is an industrial era design. Its departments and agencies are structured to focus on narrow areas and their legal remits. This system worked well, for a time. It delivered us a victory in World War II, put a man on the Moon, implemented the Great Society programs, and more. To be sure, it is far from a perfect system and it has a lot of redundancies and could operate a lot smoother and faster, but it largely—in a broad sense—does the job.

But that industrial-era structure is woefully inadequate for the speed of the information-era, its threats, and its opportunities. Cybersecurity is an issue that affects all agencies and all departments and necessitates a unified approach. Expecting them now, and in the future, to develop appropriate policies and respond to emerging technologies is setting them up for failure.

The lack of consistent and indeed institutionalized leadership on cyber issues prevents addressing this government-wide challenge. In my view this is not a transitory issue; it is an issue that will remain front and center, will continue to become more challenging, and will only become more important as American society becomes more and more reliant on data.

It is an overused cliché, but in this case, it is appropriate—data is the new oil, and just like oil needs pipelines and secure networks to power industry, so too does data need security, confidence, and assurance to support the business of business and the business of government.

The government needs data to ensure that Americans receive the services and support they need to live their lives and pursue a better future for themselves and their families. The Department of Education has over 49 million student loan borrowers.[6] Another 38 million receive Supplemental

[5] https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
[6] https://www.americanprogress.org/issues/education-postsecondary/reports/2019/06/12/470893/addressing-1-5-trillion-federal-student-loan-debt/

Nutrition Assistance[7] benefits administered by the Department of Agriculture. Another 44 million Americans receive Medicare benefits from the government, roughly 15% of the population,[8] and nearly one in six Americans receive social security benefits (63 million people).[9] Think of the amount of data about each individual that is needed to accurately process and record those benefits. Now think about how attractive that data is to cybercriminals and nation-states alike.

2. *Oversee and coordinate federal government activities to defend against adversary cyber operations inside the United States*

The absence of central coordination for the nation's cybersecurity is a significant vulnerability. With each agency and department pursuing independent cybersecurity policies and practices, significant gaps emerge—gaps that are ripe for exploitation by America's adversaries. Hackers, whether criminal, nation-state, or some flavor of both, aim to find the path of least resistance. The absence of consistency across agencies and departments creates multiple pathways that are ripe for exploitation.

This is not an abstract problem. In April 2015, IT staffers at the Office of Personnel and Management (OPM) discovered that their systems were breached by hackers, ultimately linked to China, that extracted millions of sensitive SF-86 personnel security clearance forms and millions of fingerprint cards. This is not to say that had the National Cyber Director been in place that the OPM hack would not have happened—but it is to say that there would have been a person responsible for ensuring that the nation's cybersecurity posture was as strong and robust as possible, and whom Congress could hold accountable for failings and shortcomings.

The fragmented nature of the federal government's approach to cybersecurity has stood in the way of best practices, efficiency, and effective management for too long. Individual departments and agencies have pursued their cyber policies, best practices, and software resulting in duplicative programs, gaps between and among networks, and significant inefficiencies.

This is to say nothing of the vulnerable position in which the lack of central coordination puts the country. China and Russia are aiming to dominate the next generation of technology—artificial intelligence, quantum computing, 5G, and more. They are not going to sit idly and use those capabilities for purely domestic and benevolent activities. Rather they will use these capabilities against the United States and our allies, just as they are using current technologies against our country. Whether it is intellectual property theft[10] and economic espionage,[11] or electoral

---

[7] https://www.cbpp.org/research/food-assistance/a-closer-look-at-who-benefits-from-snap-state-by-state-fact-sheets

[8] https://assets.aarp.org/rgcenter/health/fs149_medicare.pdf

[9] https://www.cbpp.org/research/social-security/policy-basics-top-ten-facts-about-social-security

[10] https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc.html

[11] https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat

interference[12] via social media and the probing of electrical grids,[13] both Beijing and Moscow have shown their willingness to use cyber capabilities against our country.

What is needed is both a whole-of-government approach and a whole-of-nation approach to cybersecurity. This must go beyond the interagency process and, to do so effectively, needs the National Cyber Director. The Director would coordinate the federal government's domestic cybersecurity posture, ensuring the application of best practices, implementing the latest technologies, and eliminating redundancies, duplicative effort, and—with the budgetary oversight—wasteful spending.

Beyond that, having a National Cyber Director would serve as a focal point for cooperation and collaboration with the private sector. Here, the relationship is not as strong as it could be and indeed should be. The speed with which Silicon Valley companies are conceived, born, grow, and die is unfathomable to the Federal bureaucracy.

When the tech industry looks at Washington, it sees a byzantine structure that is inefficient, does not know what it wants (let alone what it needs) and believes that process is progress for its own sake. In many ways, industry is not wrong. Establishing an individual and an office with the responsibility of leveraging the tech sector, academia, and think tanks towards national cybersecurity policy would—with the right person—give the private sector a measure of confidence that hitherto has been sadly lacking.

Perhaps the greatest challenge is finding the right person to fill this critical slot. That is a task I do not envy. You need someone technically savvy, bureaucratically agile, and can provide confidence to both the government and the private sector. Putting the wrong person in this position would be detrimental not only to the office but to the Nation's cybersecurity posture as well.

If we look at government like a business, it is akin to having the finance department operating one system, human resources another, and logistics ignoring the problem entirely. A simplistic shorthand to be sure, but it is illustrative of what is happening in the absence of a single person coordinating the cybersecurity practices of the organization as a whole.

There is also something to be said about the importance of Congressional oversight of cyber affairs. With the fragmented and uncoordinated approach to the government's cybersecurity policy that exists today, there is no single person accountable for the country's posture. This is a severe limitation on Congressional oversight. As a former committee chairman, I know the importance of being able to call the right person before a committee to answer Congress' questions.

---

[12] https://www.dni.gov/files/documents/ICA_2017_01.pdf

[13] https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it

3. *With concurrence from the National Security Advisor or the National Economic Advisor, would convene cabinet-level or National Security Council Principals-Committee level meetings and associated preparatory meetings*

Cyber issues are just as important as national security and national economic affairs. It is an issue, perhaps one of a handful, that crosses both security and economic lines. Without a solid cybersecurity posture, we will not be able to maintain our country's security or economic future. As such, a mechanism must exist to ensure that the principals are aware of and decide upon critical national cyber policy issues. Here, the National Cyber Director would play a critical role in ensuring that these issues are addressed in the White House through cabinet-level meetings.

Responding to this dynamic threat and opportunity environment necessitates the development and implementation of a National Cyber Strategy. The current administration released its latest version in 2018,[14] but in the absence of a National Cyber Director, each agency and department is largely left to its own devices to implement the White House's guidance. This renders the strategy largely aspirational, a dynamic that is untenable going forward.

While the White House may be reluctant to accept Congressional creation of offices within the Executive Office of the President, I would think that the National Cyber Director, with its coordination, budgetary, and convening powers would prove to be an invaluable tool for this and future presidents. It would give future administrations a single person and their associate office the responsibility of implementing a strategy across the whole of the federal government.

4. *Would provide budgetary review of designated agency or cybersecurity budgets*

The most powerful Congressional tool, as the Committee well knows, is the power of the purse. In the cyber realm, we have seen a great deal of money spent on various fixes, programs, and initiatives aimed at addressing vulnerabilities. Unfortunately, these expenditures have not been the most efficient or effective. Each agency and department is pursuing its program, unguided by a central mission or priority.

The National Cyber Director would solve this problem by providing not just a clear mission set through the National Cyber Strategy, but also providing oversight of agency and departmental budgets, the Director will ensure that resources are allocated against the threat and the opportunity. By directing spending, lining out programs that are wasteful or inefficient, or simply ensuring—as the National Cyber Director would—that the expenditures align with the strategy, the nation's cybersecurity posture will be better coordinated.

As we have seen, China and Russia are aligning their budgets to pursue their goals of digital, 5G, and artificial intelligence dominance. We need to ensure that our cybersecurity budgets are aligned towards a common goal. If we fail to do so and continue to act and spend in the manner we have to date, we will find ourselves in a strategically weakened position.

This budgetary oversight authority will become even more important when, as it certainly seems now, the Nation will need to tighten its purse strings in response to COVID-19. One of the most

[14] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

significant threats to our national security is our debt and the current economic downturn is exacerbating that pressure. When added with the external threats from Russia and China, and the speed with which future technologies are approaching, we cannot afford to spend needlessly or carelessly.

Conclusion

As my great friend and former colleague Rep. Dutch Ruppersberger put it, "We have great leaders in cybersecurity throughout the federal government, but we need a cyber quarterback."[15] He is 100% right; we need a serious wakeup call We need to get away from the approach of a seven-year-old's soccer game (to mix sports metaphors) where everyone is chasing the ball and get to American football where everyone knows their job and it's the quarterback's task to call the plays.

Put simply, we cannot afford to continue to do business as we have and expect the situation to improve. Our adversaries are not resting, and the industry continues to innovate, and if we expect to be prepared for the future and to fully seize upon the benefits of the information age tomorrow, we need to organize ourselves accordingly. We cannot afford to sit idly and expect the situation to resolve itself or hope that our adversaries will be cowed by our current capabilities. The time for smart action is now. I believe that the National Cyber Director is a critical step towards that reorganization and a smart, sensible policy that I fully support.

[15] https://langevin.house.gov/press-release/congressional-cybersecurity-leaders-introduce-bipartisan-legislation-establish