THE WALL STREET JOURNAL.

https://www.wsj.com/articles/does-the-u-s-need-a-cabinet-level-department-of-cybersecurity-11559586996

JOURNAL REPORTS: TECHNOLOGY

Does the U.S. Need a Cabinet-Level Department of Cybersecurity?

Some say a new department is needed to coordinate the nation's defenses. Others say it would only weaken those defenses.

Updated June 3, 2019 2:38 pm ET

The roster of U.S. cabinet-level departments has grown over the decades in response to one pressing need or another. Most recently, the Department of Homeland Security was formed in 2002 in response to the attacks on the U.S. of Sept. 11, 2001. Another relative newcomer is the Energy Department, formed in 1977 in the wake of the energy crisis caused by the imposition of an oil embargo on the U.S. earlier in the decade by the Arab members of the Organization of the Petroleum Exporting Countries.

Today, the U.S. faces a growing threat from cyberattacks, including a surge in recent years in attacks that have been traced to foreign governments and other hostile entities abroad. The danger of the country's critical infrastructure being crippled by a cyberattack has grown as hackers continue to hone their abilities to infiltrate computer systems.

Some argue that this threat calls for the creation of a new cabinet-level department to coordinate the country's efforts to respond to a steady stream of attacks and prevent as many attacks as possible. The current government approach to cybersecurity, which spreads responsibility among several agencies, is inefficient and inadequate, according to this argument.

But others warn that attempting to consolidate all cybersecurity responsibilities in a single agency would only make matters worse. Far from creating cohesion and efficiency, they argue, it would diminish the effectiveness of current cybersecurity efforts, which are deeply woven into the operations of a number of government agencies. Greater coordination and stronger leadership are needed, they say, but not a new cabinet agency.

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

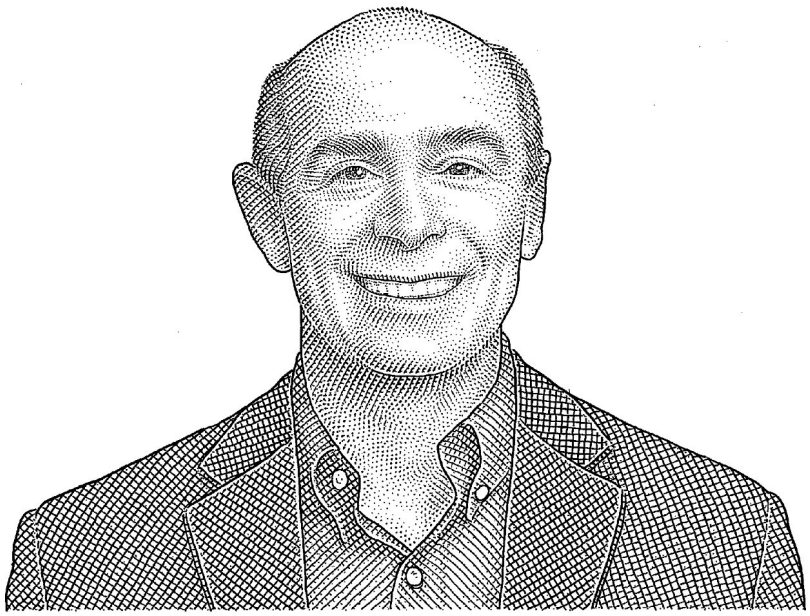
MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition

Ted Schlein, a partner at Kleiner Perkins and NSA Advisory Board member, argues in favor of a cabinet-level Department of Cybersecurity. Suzanne Spaulding, a former undersecretary at the Department of Homeland Security who now directs the Defending Democratic Institutions project at the Center for Strategic and International Studies, says such a department would be a mistake.

YES: To Be Safe, the U.S. Needs to Be a Lot More Organized

By Ted Schlein



Cyberattacks for geopolitical and other nefarious purposes are the biggest existential threat to our society. Having a cohesive policy and method for deployment of our country's cybersecurity assets to protect us against that threat should be an imperative.

This is not an area where being second best will suffice, where being good but not great will win, and where turf wars can be allowed to rule the day. To be safe, the U.S. must be the greatest superpower on Earth in cyberspace, and to do that we need to gather our cyber assets into one cabinet-level agency.

There are three main reasons why a unified cyber agency is critical: organization, authority to act, and capability.

Efficient organization is critical to accomplishing any meaningful objective.Today, we are organized for failure. Our best people are scattered across too many agencies with ill-defined responsibilities. It's an inefficient approach that wastes money. The result of this system is that

no one cybersecurity group embodies trust and competence or impels fear in our enemies. You would never organize a company this way if you wanted to dominate a market, and we need to be dominant in cybersecurity.

By having all the available talent, management and leadership in cybersecurity under one agency—pulling together in unison instead of working separately—the country would be able to build a world-class operation that would inspire trust and be seen as a formidable foe.

A unified cybersecurity agency also would gather all the legal authority to act against cyber threats and attacks under one roof. Today, agencies including the Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, Central Intelligence Agency and National Security Agency, among others, all have different authority to act in the realm of cybersecurity. And they don't always cooperate fully. Sometimes they talk to each other, and sometimes they don't—sometimes it isn't even clear what information they can legally share with one another. This inefficiency impairs our ability to respond quickly to cyberattacks or to prevent attacks. A single cybersecurity agency would solve that problem.

Finally, a cabinet-level cybersecurity agency would allow for a coherent approach to hiring and training top new talent, getting the private sector involved and acquiring the technology needed to protect the country—and create the opportunity to do all those things in new ways that would be nearly impossible to institute across a broad range of departments.

For instance, a new agency would give us the opportunity to create a whole new set of personnel policies that would make working for the government more attractive, including greater opportunities for advancement and increased compensation than are currently available in many of the agencies with cybersecurity responsibilities. For private-sector involvement, we could create a special program that rotates individuals from the private sector through the department so they can serve their country, the agency gets the best talent and information, and the private sector gets a better idea of how the public sector works. In today's world, just to get security clearance to do this would take a year per person.

As for technology procurement, special acquisition rules could be set for this agency so that the best technology can be purchased without the red tape that makes this so difficult elsewhere in government.

There can be no duplication of the role of the new Department of Cybersecurity among the agencies currently involved in cybersecurity—that would simply worsen the inefficiency the department would be created to eliminate. Those other agencies will fight their loss of control, budget and personnel, and the transition will be difficult, but those aren't reasons not to move ahead. Neither is the idea that taking cybersecurity responsibilities away from any of those agencies will damage their other operations or the overall effectiveness of our cybersecurity. I'd rather figure out, for instance, how to let the Cybersecurity and Infrastructure Security Agency

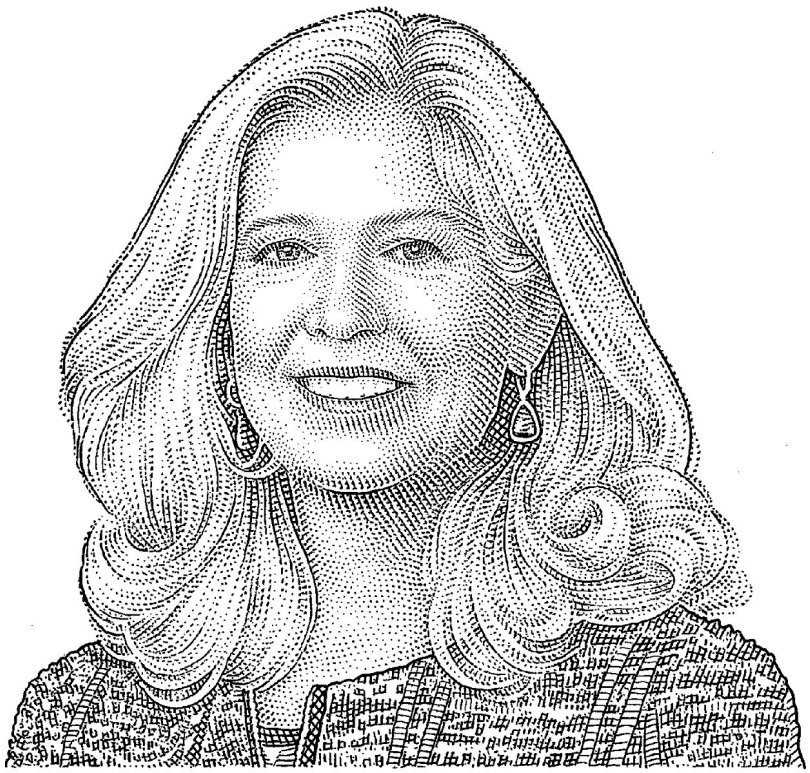
protect physical infrastructure in a really good manner and still fix the cyber issues we face in this country in a new department than tackle both problems with less than our best possible efforts.

The U.S. can only win the cyberwar by taking a different approach than it has with other areas of government, and that starts with a unified cybersecurity agency.

Mr. Schlein is a partner at Kleiner Perkins. He founded a Defense Department sponsored program, DeVenCI (Defense Venture Catalyst Initiative), focused on increasing the department's awareness of emerging commercial technologies. He sits on the board of trustees at InQTel and is an NSA Advisory Board member. Email reports@wsj.com.

NO: A New Department Would Do More Harm Than Good

By Suzanne Spaulding



Creating a cabinet-level Department of Cybersecurity would not improve the nation's cybersecurity. In fact, this bureaucratic shuffle could have the opposite effect.

A new cabinet department would either pull current cyber activities out of existing departments, which would be hugely disruptive and hamper overall cyber risk management by separating cyber from sector expertise—or replicate existing activities and expertise, which would increase costs, complicate coordination and exacerbate private-sector confusion.

It is highly unlikely, for instance, that all relevant law-enforcement and counterintelligence activities of the Federal Bureau of Investigation, the National Security Agency and the U.S. Cyber Command would be moved into a new department. Those agencies would fight extremely hard not to lose those responsibilities, and it isn't clear that you could disentangle their cyber-related assets

and people from their broader intelligence and law-enforcement efforts. Thus, the new agency would not advance the need for coordination between the three key players—the Department of Homeland Security, NSA/Cyber Command and FBI.

Similarly, a new cabinet-level agency focused on cyber would lack the necessary expertise in key industries' physical operations, as opposed to just their information technology. Understanding both is essential for assessing risks and ensuring resilience. The convergence of cyber and physical makes a cyber-only department anachronistic, as reflected in DHS's Cybersecurity and Infrastructure Security Agency, which has a combined mission.

CISA, building on years of close cooperation with the private sector and in collaboration with sector-specific agencies, has identified key functions, like electricity distribution or elections management, whose disruption—by any means—would impact national security, economic security, or public health and safety, and develops the best ways to reduce the likelihood and/or impact of such disruptions. Lessons learned by businesses in how to mitigate consequences of a natural disaster or physical attack often inform planning for resilience against cyber incidents. And a deep understanding of the risks businesses face and the consequences of their operations being disrupted, including across sectors, helps the government prioritize cybersecurity assistance. Having the physical and cyber critical-infrastructure mission together makes them both more effective.

Moving all of CISA to a new Department of Cybersecurity likely would mean that these other essential missions of CISA would be given less emphasis—including working on physical security with schools, shopping malls and other places the public gathers, as well as working with operations like electricity facilities, fuel terminals, ports, airports, banks and hospitals to build resilience against all forms of sabotage or extreme weather.

Congress considered pulling CISA's cybersecurity operations out as a separate agency but did not. They understood the importance of relying on the sector expertise the DHS has built up over years of working with electricity, chemical, water, transportation and many other industries to prepare for and respond to all hazards, from natural disasters to terrorist attacks to cyber incidents.

It is also hard to argue that separating accountability, which would still reside with the government's various department heads, and capability, which would be put into a separate department, would make us more effective. Maintaining mission-critical functions will always fall on the individual cabinet secretaries. For instance, when a breach was discovered at the Office of Personnel Management in 2015, it was the director of OPM who was ultimately held accountable. Having a Department of Cybersecurity will not change that.

Creating a new bureaucracy and then making it operate with unity of effort is extremely hard. The Defense Department still needed major reform 40 years after it was created. Nearly 17

years in, DHS is finally achieving greater unity, and the five-year effort to establish CISA is a significant milestone that should be given the opportunity to succeed rather than be immediately uprooted.

So, how do we improve cybersecurity? We need to continue the hard work of clarifying roles, harmonizing guidance and regulations, and coordinating activity among various agencies. We need strong White House leadership in that coordination and in the development of a national strategy that deters adversaries, builds resilience in the wake of cyberattacks, and includes the expertise of the private sector. We need resources that match the urgency of the threat. None of this requires a new department.

Ms. Spaulding was undersecretary at the Department of Homeland Security from 2013-2017, responsible for cybersecurity and critical infrastructure protection. She directs the Defending Democratic Institutions project at the Center for Strategic and International Studies and is on the advisory boards of Nozomi Networks and Cyber Specialty. Email reports@wsj.com.

SHARE YOUR THOUGHTS

Should there be a cabinet-level Department of Cybersecurity? Join the conversation below.

Appeared in the June 5, 2019, print edition.