The Nationalization of Cybersecurity
The Potential Effects of the *Cyberspace Solarium Commission Report* on the Nation's Critical Infrastructure

H. Chris Tecklenburg, JD/PhD;
and José de Arimatéia da Cruz, PhD/MPH

Abstract: The United States is susceptible to cyberattacks. The *Cyberspace Solarium Commission Report* provides several recommendations to prevent and respond to such attacks. However, many of these recommendations attempt to nationalize cybersecurity. This article presents a historical overview involving the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency, and the Commerce Clause, which outlines nationalization and its effects. It will note a similar trend for cybersecurity. Finally, the positive and negative consequences of nationalization are presented.

Keywords: cybersecurity, nationalization, homeland security, critical infrastructure, commerce, *Cyberspace Solarium Commission Report*

Introduction

According to the *Cyberspace Solarium Commission Report* (the report hereafter), the United States is susceptible to cyberattacks.[1] Several countries and nonstate actors have been identified as presenting the most credible threats to the United States, including China, Russia, Iran, and North Korea. To combat these cyber threats, the report outlines several recommendations. Many of these require cooperation from the states and private sector with the federal government. However, based on the report, some may wonder whether cooperation is possible, what the result of such cooperation is,

Dr. H. Chris Tecklenburg, JD, is an associate professor of political science at Georgia Southern University, Savannah Campus. Dr. José de Arimatéia da Cruz, MPH, is a professor of political science at Georgia Southern University, Savannah Campus, and a research professor at the U.S. Army War College Center for Strategic Leadership, Homeland Defense and Security Studies, Strategic Landpower Futures Group.

Journal of Advanced Military Studies vol. 14, no. 1
Spring 2023
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20231401007

and whether the cooperation is constitutional. This article will address each of these issues and focus on how the recommendations lead to the nationalization of cybersecurity. This article will briefly conclude by noting such nationalization's potential advantages and disadvantages.

The Old Mantra: Is Public-Private Cyber Cooperation Possible?

The report's recommendations hinge on cooperation. As the report makes explicit, layered cyber deterrence, which includes cooperation between the government, private sector, and citizens, is the strategy adopted. Cooperation is required since, as the report recognizes, many "devices and applications, as well as the communications infrastructure on which they rely, are overwhelmingly controlled by the private sector."[2] Thus, effective cybersecurity requires participation by the private sector with the government. In addition, cooperation between the state and the federal government is also required.

To accomplish this goal of cooperation, the report presents several proposals involving various topics. First, the report focuses primarily on cooperation between the private sector and the federal government. This is mainly seen with the recommendation of creating a congressionally funded grant, labeled the National Cybersecurity Assistance Fund, which provides funding for the mitigation of a clearly defined risk where there is no market-based solution and where there is a clear need for federal involvement.[3]

Another private-sector recommendation involves the executive branch and suggests that "Congress should direct the executive branch to develop and maintain continuity of the economic planning in consultation with the private sector to ensure the continuous operation of critical functions of the economy in the event of a significant cyber disruption."[4] This proposal includes private sector entities responsible for critical infrastructure, such as power and electric systems, gas pipelines, and other items comprising national and international financial exchanges and communication networks. According to the *National Response Plan*, critical infrastructure encompasses "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[5]

The final group of proposals involving the private sector regards recommendations that include sharing information. For example, the report notes that "Congress should . . . direct and resource the federal government to establish a formal process to solicit and compile private-sector input to inform national intelligence priorities, collection requirements, and more focused U.S. Intelligence support to private-sector cyber security operations."[6] In addition, the report recommends the creation of a Joint Collaborative Environment in which information and relevant data can be shared across the federal government and between the public and private sectors.[7] Information sharing, especially within

the cyber environment, will be the most difficult challenge facing the United States as our near-peer competitors and adversaries continue improving their cyber capabilities. For example, our near-peer competitors and adversaries are using all the elements of mis-, dis-, and malinformation (MDM) to "elicit a strong emotional response from the consumer and bypass logical reasoning to incite action, whether the action is simply spreading the content further on social media or taking action in the real world, including acts or threats of violence."[8] Cybercriminals and nonstate actors are also migrating toward the "crime-as-a-service" model. Russia, one of our most important competitors, is heavily involved in the MDM business. A growing sector of Russia's MDM economy is the "Manipulation Service Providers," both in the national and international arenas.[9]

Regarding cooperation between the federal and state governments, the report recommends two proposals. The first proposal involves election security and assists in funding for maintaining election infrastructure. This assistance includes grants to the states for auditable voting systems, replacing outdated voting equipment, and providing for sufficient provisional ballots and post-election audits. Under this proposal, states must fund 30 percent of the cost.[10] The second proposal involves state and federal cooperation regarding the promotion of cyber insurance. Mainly, the report involves cybersecurity insurance products and provides for collaboration between federal officials and state insurance regulators.[11]

Based on these proposals, there is ample room for cooperation between the federal government, the private sector, and states. These recommendations make it clear that cooperation is required to protect the United States from cyber threats adequately. This requirement leads to the possibility of cooperation. However, while possible, it is still left to be explored what the result of such cooperation and is constitutional.

The Results of Governmental Cooperation with the Private Sector and States

Over time, there have been several instances in which the government has cooperated with the private sector or states. But unfortunately, the results of such cooperation typically lead to national government domination. Due to this domination, more trust may be needed between the private sector and the federal government or the states and the federal government. Such cooperation may therefore prove difficult as there may be a reluctance on the part of the private sector and states to participate willingly in such a cooperative approach as envisioned in the report. Regardless, this section will provide several examples of cooperation that led to such domination, which may account for the reluctance on behalf of the private sector and states.

Homeland Security and Defense after the 9/11 Attacks

The cyber domain is the new battlefield of the twenty-first century. The cyber

domain is no longer the domain of wannabe cyber hackers or script kids, who are unskilled computer users that use programs or scripts developed by others to carry out their nefarious activities online. Today, the domain is dominated by nation-states and their proxies, transnational criminal organizations (TCOs), and cyber criminals using sophisticated and malicious tactics to undermine our nation's critical infrastructure, steal intellectual property and innovation, engage in espionage, and threaten our democratic institutions. TCOs directly threaten the United States and its allies "through human trafficking, the production and trafficking of lethal illicit drugs, cybercrime, and financial crimes and money laundering schemes eroding the integrity of the international financial system."[12] According to the *Federal Bureau of Investigation Internet Crime Report* produced by the Internet Crime Complaint Center (IC3), in 2021, IC3 received 847,376 cyber complaints and reported a net loss of U.S. $6.9 billion. The top five crimes in 2021 were: extortion (39,360 cases), identity theft (51,629), a personal data breach (51,829 cases), nonpayment/nondelivery (82,478 cases), and phishing/vishing/smishing/pharming (323,972 cases).[13]

Another important group operating within the cyber domain carrying out its nefarious activities are digital influence mercenaries. Digital influence mercenaries are also called virtual mercenaries. They are highly skilled computer users available on the gray market to the highest bidder, be it a nation-state, nonstate actor, terrorist organization, or private individual. The digital influence of mercenaries' rise is also due to the simple economic forces of supply and demand.[14] Digital influence mercenaries claim "their services only focus on criminals and terrorists"; however, Meta's monthslong investigation concluded that targeting is indiscriminate and includes journalists, dissidents, critics of authoritarian governments, families of opposition, and human rights activists.[15] Digital information mercenaries are also responsible for spreading misinformation, disinformation, and malinformation.

The 9/11 attacks against the homeland showed how ill-prepared the United States was to protect the homeland. As a result, discussions ensued about what was needed after the attacks on the World Trade Center towers and the Pentagon. According to James Jay Carafano at the Heritage Foundation, post-9/11 "there was an effort to create a permanent and persistent federal structure to deal with the inside-outside enemy."[16] The solution to the 9/11 attacks on the homeland was the creation of the Department of Homeland Security (DHS). The DHS was created when President George W. Bush signed the Homeland Security Act of 2002 on 25 November 2022.[17] Former Pennsylvania governor Tom Ridge (R-PA) was appointed the first director of the Office of Homeland Security.

The DHS mission is to prevent attacks and protect Americans—on the land, in the sea, and in the air. Furthermore, DHS combines all or part of 22 different federal departments and agencies into a unified, more effective, integrated department, creating a strengthened homeland security enterprise and a more secure America that is better prepared to confront the range of threats the

United States faces. The DHS has three core values that all federal departments and agencies share under its overarching organizational structure. The first core value is integrity or "service before self." According to the DHS's website, members of the DHS family "will faithfully execute the duties and responsibilities entrusted to us, and we will maintain the highest ethical and professional standards." The second core value is vigilance or "guarding America." DHS professionals state, "we will constantly be on guard against threats, hazards, or dangers that threaten our values and our way of life." Finally, the third core value is respect or "honoring our Partners." According to the DHS's website, "We will value highly the relationships we build with our customers, partners, and stakeholders. We will honor concepts such as liberty and democracy, for which America stands." In summary, DHS's mission is:

> With honor and integrity,
> We will safeguard the American people,
> Our homeland, and our values.[18]

In addition to the three core values mentioned above, DHS is guided by five principles that shape its missions. The five guiding principles are to champion "Relentless Resilience" for all threats and hazards; reduce the nation's risk to homeland security dangers; promote citizen engagement and strengthen and expand trusted partnerships; uphold the privacy, transparency, civil rights, and civil liberties; and ensure mission-driven management and integration.[19]

According to the U.S. Department of Homeland Security's strategic plan for fiscal years 2020–24, DHS has six overarching homeland security missions that make up its strategic plan.[20] The six missions are counterterrorism and homeland security threats; secure U.S. borders and approaches; secure cyberspace and critical infrastructure; preserve and uphold the nation's prosperity and economic security; strengthen preparedness and resilience; and champion the DHS workforce and strengthen the department.[21] This article will primarily discuss how DHS's mission to secure cyberspace and critical infrastructure disproportionally favors the federal government. This potential federalization of the cyber domain may minimize the roles private entities can play in protecting the cyber domain and could hinder a partnership between the federal government and private entities vital to detecting, deterring, neutralizing, and protecting the cyber domain.

Recognizing that the cyber domain is a force multiplier within the operational environment in which nations compete for supremacy, thus rendering the threat landscape more challenging than ever, DHS has taken several steps to mitigate the potential cyber harm that could paralyze the nation's critical infrastructure. For example, in 2004, DHS created the National Cyber Security Division (NCSD). One of the primary functions of the NCSD is to "partner with government, industry, academia as well as the international community to make cybersecurity a national and shared priority."[22] Another vital DHS agency in the fight to protect our critical infrastructure and nefarious activities online

by criminal elements is the Cyber Crimes Center, composed of the following units: Cyber Crimes Unit, the Child Exploitation Investigations Unit, and the Computer Forensics Unit.

Furthermore, DHS's cybersecurity and critical infrastructure security responsibilities focus on four goals: securing federal civilian networks; strengthening the security and resilience of critical infrastructure; assessing and counter evolving cybersecurity risks; and combating cybercrime. According to DHS, "Serving as the designated federal lead for cybersecurity across the U.S. Government, DHS promotes the adoption of common policies and best practices that are risk-based and responsive to the ever-changing cyber threat environment."[23] Obviously, those so-called common policies and best practices sometimes conflict with the hardware and software used by federal agencies, primarily if they are owned and controlled by private investors. In fact, according to the *Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*, the private sector owns most of the nation's critical infrastructure and key resources—roughly 85 percent.[24] However, the government has historically funded the construction and maintenance of specific infrastructure sectors such as transportation and water.[25]

A concern arises as more of the critical infrastructure used by the federal government is in the private sector's hands and controlled by private investors; the federal government may relinquish its traditional responsibility as caretaker of the nation's critical infrastructure and rely on the private sector to assume its traditional responsibilities instead of the federal government. As is pointed out in the *Solarium Report*, "businesses are often reluctant to let governments onto private, commercial networks without a clear understanding of their shared interests and responsibilities. Afraid of creating moral hazard, the federal government invests little in protecting the cybersecurity of commercial infrastructure or key systems controlled by states and local municipalities."[26] The distrust between the private sector and federal government and the lack of accountability on who is responsible for setting the nation's cybersecurity priorities produces dangerous security gaps. This gap occurs when "public- and private-sector responses are left uncoordinated, and the nation's critical infrastructure is left unprotected and vulnerable to adversaries who can, and will, exploit this opportunity."[27]

The Cybersecurity and Infrastructure Security Agency

The Cybersecurity and Infrastructure Security Agency Act of 2018 established the Cybersecurity and Infrastructure Security Agency (CISA).[28] Its director, Jen Easterly, leads CISA. CISA's Cybersecurity Division is led by Executive Assistant Director for Cybersecurity Eric Goldstein. CISA leads the nation's strategic and unified work to strengthen the cyber ecosystem's security, resilience, and workforce to protect critical services and the American way of life from cybercriminals, cyberterrorism, and adversaries. According to CISA's website, its primary mission is "lead[ing] efforts to protect the federal .gov domain of

civilian government networks and to collaborate with the private sector—the .com domain—to increase the security of critical networks." Protection of the government's .gov domain is accomplished through the following functions:

- Capability delivery
- Threat hunting
- Operational collaboration
- Vulnerability management
- Capacity building
- Strategy, resources, and performance
- Cyber defense education and training

It is often said that the only computer that has not been attacked is a computer that is not turned on. Recognizing the American way of life and its dependency on technology for almost everything, including but not limited to connecting with friends and relatives, banking, traveling, shopping, education, work, and romance, CISA "serves as both America's cyber defense agency and as the national coordinator for critical infrastructure security and resilience."[29] One such program where CISA takes a proactive approach to address our nation's infrastructure security and resilience is the ShieldsUp campaign introduced in late 2021.

ShieldsUp was launched in the aftermath of the Russian invasion of Ukraine. CISA's ShieldsUp campaign encourages "organizations of all sizes to take immediate steps to improve their cybersecurity and protect their critical assets" in the face of "potential spillover effects to the U.S. homeland" as the Russian-Ukraine conflict continues without a diplomatic solution or ceasefire.[30] CISA's position is that the increasing technological interconnectedness of the world and the American people's reliance on technology for almost every aspect of their daily life requires a "continuous, whole-of-government approach that spans all stakeholders."[31] In addition, specific sectors of the economy composing the National Critical Functions are essential to CISA's mission, which is "to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure."[32] According to the CISA's website, there are 16 critical sectors comprising the U.S. critical infrastructure. Those 16 essential sectors of infrastructure are crucial since their "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[33]

Sectors of the U.S. economy considered part of the National Critical Functions are required by CISA to "put in place measures to detect, delay, and respond to physical and cyberattacks such as establishing security officials; creating barriers and access control measures; implementing intrusion detection capabilities; and developing incident reporting, response, and investigation programs for both physical and cyberattacks, among other measures."[34] That

is a tall order to accomplish given that the "majority of the critical infrastructure, hardware, and software that powers the information age resides in the private sector."[35] Furthermore, because private-sector companies are not "part of the defense industrial base, they have no legal obligation to report information technology system anomalies, increased traffic, or Information Technology (IT) security breaches."[36] Finally, businesses are often reluctant to "let government onto private, commercial networks without a clear understanding of their shared interests and responsibilities."[37]

To break down this cycle of distrust between the federal government and private sectors, the *CISA Strategic Plan 2023–2025* Goal 3 (Operational Collaboration) wishes to establish a culture of "trusted, sustained, and effective partnerships between the government and the private sector" as a foundation "to protect the nation's critical infrastructure."[38] CISA also states that under *Strategic Plan 2023–2025*, the organization will "approach every partnership with humility, transparency, gratitude, and a firm resolution to add value wherever possible."[39] This is an ambitious goal for an organization that has been institutionally limited in its ability to carry out its mission fully. As the report clearly states in its findings:

> CISA has been institutionally limited in its ability to fully carry out this mission, hindered by inadequate facilities, insufficient resources, lack of buy-in from other federal departments and agencies, ambiguity from Congress on its role and position about other agencies, and inconsistent support to and integration with private-sector.[40]

Commerce Clause

Finally, the best example of cooperation that led to national domination occurs between the federal and state governments in the realm of the Commerce Clause. Throughout the nineteenth and twentieth centuries, the federal government battled with conditions regarding interpreting this clause. The action was based on the type of federalism to which the Supreme Court should adhere to. First was dual federalism. The court held that there were two separate spheres in which certain rights fell under state authority, and the remaining rights were under the national government's authority. During the periods when the court adhered to dual federalism, it generally ruled in favor of the state's rights. This contrasts with cooperative federalism, where states and the federal government are supposed to cooperate. However, such cooperation inevitably led to national domination, with the Supreme Court consistently ruling in favor of the national government during this period. A brief historical analysis will help illustrate how the court enabled the strengthening and growth of the federal government at the expense of state sovereignty.[41]

Every Commerce Clause analysis should begin with Gibbons v. Ogden (1824), involving a dispute between an individual who had a state-granted monopoly on its waters, and Gibbons, who claimed the right to travel on interstate waters pursuant to a federal license.[42] At issue in the dispute was whether

the state had concurrent powers to regulate interstate navigation. The Supreme Court ultimately held that the federal government had the right to regulate interstate commerce, which included navigation. While the holding of the case is important, how the court arrived at its opinion is noteworthy. Justice John Marshall announced that states could regulate intrastate travel, but interstate travel was the federal government's responsibility.[43] The court's ruling was thus adhering to a form of dual federalism, but one that favored the federal government.

The next era also adhered to dual federalism but favored the state governments. Dual federalism eras are essential as they permitted the state governments to retain sovereignty. After all, at the root of dual federalism eras is a recognition of equal powers between the federal and state governments. This can be seen in the second era of Commerce Clause jurisprudence following Gibbons, lasting from 1836 to 1937, and showed state government dominance with the court ruling consistently in favor of the states.

For example, in United States v. E. C. Knight Company (1896), the American Sugar Refining Company acquired E. C. Knight Company, among others, giving American Sugar Company nearly 98 percent control of the country's sugar production.[44] The United States attempted to nullify the acquisition because the sale amounted to a monopoly, thus constituting a trust. Therefore, the Sherman Anti-Trust Act (1890), passed pursuant to the Commerce Clause, was applied to prevent the sale. The Supreme Court ultimately held that while the Sherman Anti-Trust Act was valid, it did not apply in this case since E. C. Knight was only involved in manufacturing and production, which did not constitute commerce during this era.[45] This case displays dual federalism, with the court attempting to create a test in which manufacturing and production fell under the auspices of state regulation. In contrast, distribution across state lines was a matter of federal regulation.

This test and application of dual federalism were also seen in Hammer v. Dagenhart (1916), which involved child labor.[46] More specifically, Congress had passed an act prohibiting such labor. The court held that Congress could not regulate child labor since such work was only involved in producing and manufacturing materials, which did not constitute commerce. Again, the Supreme Court's ruling was preserving the sovereignty of states at the expense of federal power.

The court's interpretation of the Commerce Clause and its use of dual federalism changed in 1937. This change was primarily due to the credible threat of court expansion from President Franklin D. Roosevelt in response to the court's continual rulings upholding state's rights and knocking down pieces of Roosevelt's New Deal legislation. Roosevelt's court-packing plan did not come to fruition, as one of the justices on the court began to switch his vote, ruling in favor of the New Deal legislation. This would usher in a period of cooperative federalism, in which the federal government was to "cooperate" with the state governments.[47] However, what resulted from the implementation of coopera-

tive federalism was national domination. This can mainly be seen in cases for the third era of the Commerce Clause, which lasted from 1937 to 1995. During this era, the Supreme Court would consistently rule in favor of the federal government.

Several cases are illustrative of federal domination during this era. The first is NLRB v. Jones and Laughlin Steel Corp. (1937), where the Supreme Court examined the constitutionality of the National Labor Relations Act passed pursuant to the Commerce Clause.[48] Recall that production and manufacturing did not constitute commerce in the prior era and hence could not be regulated by Congress. However, the court began examining the aggregate effect on commerce in this era. It therefore looked to the total impact of what was to be regulated and no longer just looked at production and manufacturing. Ultimately, the Supreme Court upheld the act and ruled in favor of the federal government.

This case was followed by United States v. Darby (1941), involving the constitutionality of the Fair Labor Standards Act of 1938 (FLSA).[49] Again, the issue involved goods produced in one state but shipped across state lines. While this issue appeared to have been resolved in the prior era, the court reexamined it and explicitly overruled Hammer v. Dagenhart. The court finally discarded the production/distribution rule it had utilized in the previous period and held that the FLSA was constitutional.

Two final cases show federal domination during the cooperative era. However, these cases are unique in that the link between what was being regulated and the Commerce Clause was arguably tenuous. For example, the first of these cases was Heart of Atlanta Motel v. United States (1964), involving the constitutionality of the 1964 Civil Rights Act.[50] The particular provision at issue, in this case, prohibited racial discrimination in areas affecting public accommodation. In Heart of Atlanta Motel, the motel essentially argued that they were not engaged in interstate commerce, even though they placed advertisements in national magazines and billboards and received most of their guests from out of state. Nevertheless, the court held that the act was valid and the Commerce Clause could be used to regulate racial discrimination. This was an expansive interpretation of the Commerce Clause.

However, the most expansive interpretation that favored the federal government during this era can be seen in the case of Wickard v. Filburn (1942).[51] In Wickard, the 1933 Agricultural Adjustment Act limited the wheat farmers could grow. Filburn grew several acres of wheat for consumption on his farm, more than the amount allowed under the act. The court held that the act was valid even though it seemingly regulated intrastate consumption. To justify its opinion, the court avoided analyzing the case by looking at Filburn's wheat consumption. Instead, the court considered the potential effects of all the individuals growing home wheat and how that could affect the overall market. Thus, the court considered the aggregate impact from all individuals violating the act and held that this constituted commerce.

The cases during this era make it clear that cooperative federalism leads

to national domination. In every case considered during this time frame, the Supreme Court upheld Congress's right to enact the legislation under the Commerce Clause. However, the results during the final Commerce Clause era (1995–present) are mixed at best. Some cases favor federal rights, while others favor states' rights. These mixed results are likely due to a court that grew more conservative and hence more in favor of states' rights. This revival of states' rights leads one to wonder whether the court reverted to dual federalism.

A few cases will illustrate this point. The first is perhaps the most important, as it was the first case where the conservative court overturned a congressional statute based on the Commerce Clause. The case, Lopez v. United States (1995), involved the Gun-Free School Zones Act of 1990, in which a high school student brought a gun to school and was charged with violating the act.[52] The student, Lopez, argued that Congress had exceeded its authority under the Commerce Clause in passing the act. The court agreed, holding that regulating guns on campuses did not amount to commerce.

A similar outcome was reached in United States v. Morrison (2000) involving the 1994 Violence Against Women Act.[53] Congress had again passed the act under the Commerce Clause, as it was argued that if you aggregate all the instances of domestic violence, many women would be unable to work during the year, which would impact the overall economy. The conservative court held that this was too tenuous of a connection and that crime cannot be aggregated to make commerce.

However, despite these two previous cases, the court did rule in favor of the government once during this era. This is mainly seen in Raich v. Gonzales (2005), in which individuals grew marijuana for their consumption.[54] In reaching their decision, the court cited Wickard and noted that home consumption of marijuana affected the overall economy of the primarily illegal product.

The mixed results obtained from the prior three cases are significant as they show the court needs help interpreting the Commerce Clause and justifying its decision. In other words, the court is trying to figure out which form of federalism it adopts and how to balance the delicate relationship between federal and state governments. For present purposes, what is important is that during the cooperative federalism phase, when the governments were supposed to cooperate, the federal government dominated the field.[55] This is like the expected outcome of the cooperation as envisioned in the *Solarium Report*. Based on the precedents established in the historical overview, one should be cautious in advocating cybersecurity changes that may alter the government's balance with the private sector. While there may be certain advantages to the federal government taking the lead in cybersecurity, the potential loser may be the private sector and the states.

Overall, as these precedents show, the relationship between the federal and state governments is tenuous. Nevertheless, the relationship between these governments is always in play, as the federal government consistently attempts to dominate the states. It is only during cooperative times that this becomes pos-

sible. Therefore, state governments and the private sector should be wary of any proposals of cooperation.

Is Cooperation Constitutional?

While the three previous sections outlined precisely how cooperation could lead to the potential nationalization of cybersecurity, some may wonder whether the proposals presented in the *Solarium Report* are constitutional. After all, constitutional questions can be expected when the balance of power between the governments and the private sector shifts.

The primary constitutional concern regarding the report involves the proposed cooperation between states and the federal government in election security. More particularly, the report recommends providing grants to states that require the states to match 30 percent of funds to protect federal elections from cyber threats. Brian T. Yeh examined the federal government's limitations to imposing conditions on grant funds.[56] These limitations are primarily found in South Dakota v. Dole (1987), which held that according to the Spending Clause, legislation must be in pursuit of the "general welfare."[57] In addition, Yeh noted that the Dole Court held that

> any conditions attached to the receipt of federal funds must: (1) be unambiguously established so that recipients can knowingly accept or reject them; (2) be germane to the federal interest in the particular national projects or programs to which the money is directed; (3) not violate other provisions of the Constitution such as the First Amendment or the Due Process or Takings Clauses of the Fifth Amendment; and (4) not cross the line from enticement to impermissible coercion, such that states have no real choice but to accept the funding and enact or administer a federal regulatory program.[58]

The fourth provision that could apply to the cybersecurity context involves coercion. The court has addressed coercion with the Taxing and Spending Clause in the Dole case and NFIB v. Sebelius (2012).[59]

In Dole, the federal government wanted to raise the drinking age to 21. However, states are typically in charge of such age requirements. Therefore, the federal government attached conditions to the receipt of federal highway money, prohibiting some of the funding from going to any state that failed to comply. The court ultimately held in favor of the federal government since it did not take away all funding but only threatened to take a small percentage of it.[60]

Dole can be contrasted with Sebelius, which involved the constitutionality of the 2010 Affordable Care Act. While there were multiple issues in the case, the most applicable one involved Medicaid expansion. More particularly, the federal government threatened the states with the complete loss of all Medicaid if they did not comply with the new proposed health care law. Unlike in Dole, the court ruled that the federal government had gone too far this time and that their actions amounted to coercion and were thus unconstitutional.[61]

Regarding the *Solarium Report*, it is recommended that the federal government help secure the state's election apparatus, with the states responsible for 30 percent of the costs. The constitutional issue is whether such a proposal is like Dole or Sebelius. In other words, is depriving states of a grant because of a 30 percent funding requirement constitute coercion like in Sebelius, or is it more consistent with Dole since it is not a complete threat of deprivation of federal funds? After all, only a small percentage was withheld in Dole, which was deemed constitutional, while a complete deprivation in Sebelius was deemed unconstitutional. This case is likely like Dole, but it should be noted that the constitutionality of such a provision is questionable.[62]

This section is essential in the report as it highlights a substantial constitutional question. While the constitutionality is questionable, nationalistic recommendations should not hinge on whether cooperation should be constitutional. While the report strives to maintain election security, there are other possible means to do so than forcing states to match federal funds that would be less constitutionally suspect. This includes matching funds at a lesser rate or true cooperation between the federal government and the states.

Implications

The fact that 85 percent of the critical infrastructure the government relies on is in private hands and controlled by private investors is a concern for a highly interconnected and wired nation. The United States' critical infrastructure "provides national critical functions that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on the Nation's security, economy, and public health and safety."[63] Critical infrastructure today faces increasingly new risks and challenges moving forward. Our modern way of life in an interconnected and highly wired world depends on confidentiality, integrity, and availability, also called the CIA Triad of data. Furthermore, the United States "is facing adversary nation-states, extremists, and criminals leveraging emerging technologies to an unprecedented degree. Authoritarian states seek to control every aspect of life in their societies and export this style of government, in which surveillance trumps liberty, to the rest of the world."[64] Finally, TOCs and cyber criminals are migrating toward the "crime-as-a-service" model in which threat groups purchase and exchange malicious code on the dark web.[65]

Recommendations

1. The U.S. government and the private sector must create a new social contract of shared responsibility to secure the nation's cyberspace, recognizing each other as partners to diminish the distrust between the private sector and the government.
2. Information sharing between the federal government and the private sector rather than operating in silos and keeping secrets from each other to diminish the distrust.

3. The matching amount states are required to give for election security should be reduced to ensure constitutionality; and
4. Increased workforce recruitment and talent acquisition and management

Workforce recruitment and talent acquisition will be a challenge to the U.S. government. The U.S. government needs to be able to protect its critical infrastructure with a crucial civilian workforce. Dr. Raj Iyer, Army chief information officer (CIO) at the U.S. Army Europe and Africa 2022 Cybersecurity Summit, held on 29 July 2022, pointed out that finding the right people is one of his biggest challenges as an Army CIO. He emphasized "the importance of filling the cyber talent gap and that the Army plans to address this perennial challenge by rolling out the Department of Defense Cyber Excepted Service, a new talent model for the civilian cyber workforce, this year. The service will take advantage of every available tool to recruit and retain the cyber workforce."[66] Unfortunately, one of the tools not available to the Army is the high compensation package provided by the private sector to cybersecurity professionals. For example, "positions includ[e] cybersecurity analyst, information security analyst, and penetration tester, and annual median salaries ranging from $75,000 to more than $100,000."[67]

Conclusion

Humans created the cyber ecosystem on which the nation relies; therefore, it is susceptible to vulnerabilities. Furthermore, this system is more than simply the technology that comprises it. It also comprises people, processes, and organizations that plug into the technology and the data they combine to produce complex products.[68] Overall, as reviewed throughout this article, the report has made several key recommendations that continue the trend of nationalizing cybersecurity. This trend was placed in a historical context through the creation of the Department of Homeland Security and CISA. In addition, the historical overview of the Commerce Clause explains how the federal government, through the lens of cooperative federalism, became dominant over states' rights. The report assumes the federal government's dominance is explicit, while it claims to seek cooperation and, in many instances, the recommendations arguably trample on state and individual rights. In other words, consistent with the Commerce Clause and the nationalization of our government, complete adoption of the report could lead toward the nationalization of cybersecurity.

In conclusion, one may wonder what the results of such nationalization are and whether it is positive or negative for the United States. One positive aspect of nationalization would be uniformity in cybersecurity. There is no need for the potential of 50 state responses to a particular cyber threat. In addition, a swifter response from the federal government may issue if nationalization occurred in the field. However, as noted throughout this article, nationalization has potentially adverse consequences. One example involves trampling states'

rights, especially in the election field. While the report has noble goals, forcing state participation may be unconstitutional. Furthermore, the relationship between the federal government and the private sector may need further analysis. Nationalization may also lead to forced participation in this relationship, which may lead to new constitutional challenges in the future.

Endnotes

1. *United States of America Cyberspace Solarium Commission Report* (Washington, DC: Cyberspace Solarium Commission, 2020), hereafter *Solarium Report*.
2. *Solarium Report*, 23.
3. *Solarium Report*, 58.
4. *Solarium Report*, 59.
5. *National Response Plan* (Washington, DC: U.S. Department of Homeland Security, 2004), 64.
6. *Solarium Report*, 100.
7. *Solarium Report*, 101.
8. "Election Infrastructure Insider Threat Mitigation Guide," Cybersecurity & Infrastructure Security Agency, accessed 17 April 2023.
9. *Solarium Report*, 68.
10. *Solarium Report*, 67–68.
11. *Solarium Report*, 80–82.
12. *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2022), 23.
13. *Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2021). *Phishing* is a scam in which the perpetrator sends out legitimate-looking email to phish for personal and financial information from the recipient; *vishing* is a social engineering activity over the telephone system, most often using features facilitated by Voice over Internet Protocol (VoIP), to gain unauthorized access to sensitive data; *smishing* is the fraudulent practice of sending text messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords or credit card numbers; and *pharming* is the fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one to obtain personal information such as passwords, account numbers, etc. For more definitions of current cybersecurity terms, see Adam Gordon, ed., *Official ISC² Guide to the CISSP® CBK®*, 4th ed. (Boca Raton, FL: CRC Press, 2015).
14. James J. F. Forest, *Digital Influence Mercenaries: Profits and Power through Information Warfare* (Annapolis, MD: Naval Institute Press, 2022).
15. "Meta Bans 'Cyber-Mercenaries' that Targeted 50,000 People," Al Jazeera, 17 December 2021.
16. James Carafana, "Homeland Defense and Homeland Security: Distinctions and Difference," in *Introduction to Homeland Defense and Defense Support of Civil Authorities: The U.S. Military's Role to Support and Defend*, ed. Bert B. Tussing and Robert McCreight (Boca Raton, FL: CRC Press, 2015).
17. Homeland Security Act of 2002, Pub. L. No. 107-296 (2002).
18. "Creation of the Department of Homeland Security," Department of Homeland Security, 3 June 2022.
19. "Creation of the Department of Homeland Security."
20. *The DHS Strategic Plan: Fiscal Years 2020–2024* (Washington, DC: Department of Homeland Security, n.d.).
21. "Creation of the Department of Homeland Security."
22. William M. Oliver, Nancy E. Marion, and Joshua B. Hill, *Introduction to Homeland Security: Policy, Organization and Administration*, 2d ed. (Burlington, MA: Jones & Barlett Learning, 2021), 75.

23. "Secure Cyberspace and Critical Infrastructure," Department of Homeland Security, accessed 12 May 2023.
24. *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report* (Washington, DC: Government Accountability Office, 2009).
25. *Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency Management* (Washington, DC: Federal Emergency Management Agency, 2011).
26. *Solarium Report*, 16.
27. *Solarium Report*, 17.
28. The Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278 (2018).
29. *CISA Strategic Plan, 2023–2025* (Washington, DC: Cybersecurity and Infrastructure Security Agency, 2022), 3.
30. *CISA Strategic Plan 2023–2025*, 5.
31. *CISA Strategic Plan 2023–2025*, 5.
32. *CISA Strategic Plan 2023–2025*, 6.
33. "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency, accessed 18 April 2023. The 16 critical infrastructure sectors are: chemical sector; communication sector; dams sector; emergency services sector; financial services sector; government facilities sector; information technology sector; transportation systems sector; commercial facilities sector; critical manufacturing sector; defense industrial base sector; energy sector; food and agriculture sector; health care and public health sector; nuclear reactors, materials, and waster sector; and water and wastewater systems sector.
34. *CISA Strategic Plan 2023–2025*, 17.
35. *Solarium Report*, 16.
36. Bert B. Tussing et al., *Contested Deployment: A US Army War College Center for Strategic Leadership Integrated Research Project* (Carlisle, PA: Army War College Press, 2022), 114.
37. *Solarium Report*, 16.
38. *CISA Strategic Plan 2023–2025*.
39. *CISA Strategic Plan 2023–2025*, 23.
40. *Solarium Report*, 105.
41. For more discussion regarding the different types of federalism and resulting power if the federal government, see Theodore J. Lowi et al., *American Government: Power and Purpose*, 16th ed. (New York: W. W. Norton, 2021), 81–93.
42. Gibbons v. Ogden, 22 U.S. 1 (1824).
43. David M. O'Brien, *Constitutional Law and Politics*, vol. 1, *Struggles for Power and Governmental Accountability*, 10th ed. (New York: W. W. Norton, 2017), 519, 533.
44. United States v. E. C. Knight Co., 156 U.S. 1 (1895).
45. O'Brien, *Constitutional Law and Politics*, vol. 1, 539, 543–45.
46. Hammer v. Dagenhart, 247 U.S. 251 (1918).
47. For more discussion regarding the change in federalism, see Lowi et al., *American*, 81–93. For more background and discussion regarding 1937 and the threats toward the court, see O'Brien, *Constitutional Law and Politics*, vol. 1, 553–54.
48. NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1 (1937).
49. United States v. Darby, 312 U.S. 100 (1941).
50. Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241 (1964).
51. Wickard v. Filburn, 317 U.S. 111 (1942).
52. United States v. Lopez, 514 U.S. 549 (1995).
53. United States v. Morrison, 529 U.S. 598 (2000).
54. Gonzales v. Raich, 545 U.S. 1 (2005).
55. For more discussion regarding the Commerce Clause and different types of federalism, see Lowi et al., *American Government*, 81–93. For more background and discussion of the cases previously cited, see David M. O'Brien and Gordon Silverstein *Constitutional Law and Politics*, vol. 1, *Struggles for Power and Governmental Accountability*, 11th ed. (New York: W. W. Norton, 2020), 549–645.

56. Brian T. Yeh, *The Federal Government's Authority to Impose Conditions on Grant Funds* (Washington, DC: Congressional Research Service, 2017).
57. South Dakota v. Dole, 483 U.S. 203 (1987).
58. Yeh, *The Federal Government's Authority to Impose Conditions on Grant Funds*.
59. National Federation of Independent Business v. Sebelius, 567 U.S. 519 (2012).
60. O'Brien, *Constitutional Law and Politics*, vol. 1, 636–38.
61. O'Brien, *Constitutional Law and Politics*, vol. 1, 639–48.
62. One may attempt to distinguish Dole and Sebelius from our current situation, since in those cases the states had a preexisting grant that was threatened to be reduced or extinguished. In this case, states merely have an option to participate in the election security program and arguably will not necessarily suffer a reduction or extinguishment of funds. Yet, the states are still suffering from a potential loss of participation in a critical program based on not matching federal funds. Thus, not participating in a grant program is still viewed as a loss or extinguishment of said program.
63. "National Critical Functions," Cybersecurity and Infrastructure Security Agency, accessed 12 May 2023.
64. *Solarium Report*, 19.
65. Keman Huang, Michael Siegel, and Stuart Madnick, "Cybercrime-as-a-Service: Identifying Control Points to Disrupt" (working paper CISL#2017-17, MIT Sloan School of Management, November 2017), 13.
66. Sun Vega, "Army CIO speaks at Army Europe and Africa 2022 Cybersecurity Summit," Army.mil, 10 August 2022.
67. Steve Morgan, "Cyber Jobs Report: 3.5 Million Openings by 2025," *Cybercrimes Magazine*, 14 April 2023.
68. *Solarium Report*, 71.