Journal of Computer Sciences and Applications, 2019, Vol. 7, No. 1, 37-42
Available online at http://pubs.sciepub.com/jcsa/7/1/6
Published by Science and Education Publishing
DOI:10.12691/jcsa-7-1-6

Critical Infrastructure - Perspectives on the Role of Government in Cybersecurity

Mubarak Banisakher*, Marwan Omar, Wade Clare

Department of Computer Science, Saint Leo University, FL. USA
*Corresponding author: Mubarak.banisakher@saintleo.edu

Received June 05, 2019; Revised August 04, 2019; Accepted August 12, 2019

Abstract Since the end of the cold war era (1945 - 1989), the United States government (USG) has been gradually reduced, and in some cases eliminated direct support for the development of critical infrastructure. The reduction of public investment, and the subsequent transfer of critical infrastructure from public to private ownership, has significantly increased the risk not only to critical infrastructure, but to the entire nation. The use of non-isolated, public communication and information technology, without any contingency or emergency backups is a national disaster waiting to happen. The USG must vigorously support - both financially and through active management, policy and regulation - the creation of isolated, secure, and resilient communications and information technology infrastructures, that provide non-public redundancy, thereby ensuring that public communication and information technology failures, as a result of man-made attacks or natural events, do not result in catastrophic outcomes to not only other critical infrastructure sectors, but to the nation at large. This paper surveys historical and contemporary government roles in the development of critical infrastructure, particularly, communication and information technologies, and provides recommendations for how the US government can significantly improve the security and resilience of its current critical infrastructure systems.

Keywords: *critical infrastructure, communications, information technology, redundancy*

Cite This Article: Mubarak Banisakher, Marwan Omar, and Wade Clare, "Critical Infrastructure - Perspectives on the Role of Government in Cybersecurity." *Journal of Computer Sciences and Applications*, vol. 7, no. 1 (2019): 37-42. doi: 10.12691/jcsa-7-1-6.

1. Introduction

If one listens to, or reads the tweets of US politicians discussing cybersecurity and technology, it is obvious that the biggest security and technology issues facing Americans are 1) private companies like Twitter, Alphabet, and Facebook "violating the trust" of their users by selling aggregated data; and 2) private companies compromising users data through what has come to be known as data breaches. Based on the incessant drumbeat of the 24-hour news cycle, it would be easy to assume that all the cybersecurity problems begin and belong to the private sector (companies and individuals), and that all the solutions require varying types of federal, state, and local government oversight. Even without being constantly reminded of these facts daily, it's apparent to most that data breaches, dubious information collection and retention practices, and the potential of negative psychological and sociological impacts of technology are important topics. But, are they the most critical cybersecurity issues?

The National Institute of Standards and Technology (NIST) Special Publication 800-82 Revision 2 states that, "Critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies. An incident in one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures." [1] Put another way, critical infrastructure failures - especially in the areas of communications and information technology - have the potential for cascading and catastrophic impacts not limited to the specific sector to which they relate, but also across the broader critical infrastructure system of systems.

Yet, outside of a relatively small community of interest, there is little concern and even less discussion related to known or potential risks to US critical infrastructure. The fact is, critical infrastructure systems, particularly control systems - including supervisory control and data acquisition (SCADA) systems; distributed control systems (DCS); and programmable logic controllers (PLC) - are highly technical, and honestly, quite boring to the average person. However, these boring "systems of systems" are in fact the foundation of our American critical communication and information technology infrastructure. Without these systems there is no Twitter, Google, Instagram, or Facebook. In fact, without them there's no electrical power, water, financial, transportation or a variety of other systems that characterize the modern world.

While the loss or theft of one's passport or credit card number, the hacking of and e-mail or social media account, the loss of credentials, or a variety of other personal cybersecurity related events can be a stress-inducing,

embarrassing, and occasionally costly propositions - but, compared to a 5-day shutdown of the eastern United States' electrical grid, they are at most, inconsequential.

A recent paper produced by the US Air Force, Air University's Lemay Center [2] provided insight into a significant issue facing the United States, namely a range of substantial design and redundancy gaps in US critical communications and information technology (IT) infrastructure. While the paper addresses a range of threats and systems, of particular interest were discussions related to systems designed to provide the nation distributed, stable and consistent management of a variety of critical infrastructures. Threats against and the potentially catastrophic outcomes of successful attacks on these systems of systems were particularly and honestly quite disturbing. A review of these systems, potential vulnerabilities indicated that while the size and distribution of these systems are often sector (or entity) unique, virtually all rely on and are connected to public (i.e. commercial) communications and IT systems in some form or fashion.

Stuckenberg, et al. (2018) served as another stark reminder that while personal data management and security - by both the user and trusted, semi-trusted, or untrusted third-parties - is important, it pales in comparison to the potentially disastrous outcomes related to systemic failures in current and proposed communication and IT critical infrastructure, whether because of man-made or natural catastrophe. Although not specifically focused on cybersecurity, and primarily concerned with potential roles and responsibilities of the US military - as an Air University paper should - it also encouraged thought about the roles and responsibilities of all three key players in both US critical infrastructure and cybersecurity, namely the individual, industry, and the government. It was the Lemay paper, and others like it that highlighted the need for a secure, hardened, resilient and redundant communication and IT infrastructures capable of supporting the system of systems which is currently known as US critical infrastructure.

While each of the three stakeholders has a part to play in the establishment, maintenance and protection of these critical infrastructures, this paper will focus on the role of the United States Government (USG). Through a survey of historical and current USG contributions and outcomes, this paper will endeavor to provide recommendations on the best way for the USG to effectively contribute to the development of secure and resilient critical infrastructures in both the physical and cyber domains.

2. Historical USG Contributions

Research and Development: The USG has a long history of contribution to not only scientific research but also the development of critical communications and IT infrastructure. Jokes about Vice President Al Gore creating the internet [3] aside, few serious students of communications and/or information technology question the critical role that the USG - in conjunction with individuals and industry - played in the development of today's modern communication infrastructure.

During the fifty years following World War II (1945 - 1995), the USG was directly involved the design, funding, and creation of not only communications and IT technology, but of most of what is currently labeled as US critical infrastructure. The end of World War II, and the entry of the United States of America (USA) and the Union of Soviet Socialist Republics (USSR) into the subsequent Cold War stimulated not only a plethora of divergent policy and political theories and arguments, but also inspired the development of literally thousands of USG funded, defense-related technologies.

As fear of nuclear and/or conventional attack by the USSR increased in the USA, the USG focused on the development of systems and processes that would support the defense of the nation and theoretically allow the USA to survive nuclear war. Through years of work, drills, and simulations, public and private infrastructure, capability, and capacity was identified and categorized in support of the nation's defense, and through this process, the theory of critical infrastructure was developed.

During the 20-year period between 1950 and 1970, literally hundreds of billions of dollars were invested in critical infrastructure, research, and related development programs [4]. It was during this period that initial investment was made into the interstate highway system, the space program, and several relatively small programs being managed under the Department of Defense's (DoD) Advanced Research Projects Agency's ARPANET network - programs which arguably led to the development of the current range of critical communication and IT infrastructure, including what we now call the internet [4]. As the previous paragraphs indicate, the idea of the USG being a key contributor to the design and development of critical infrastructure was not only accepted but expected. Critical infrastructure was considered a public good, and as such the primary provider was expected to be the United States government.

But, what was/is critical infrastructure? While a variety of different infrastructures have been included or removed over the years, the concept and supporting definition has changed little. The contemporary definition, and the one most often referred to in current discussions, policies and regulations is that stated in H.R.3162 (AKA the USA PATRIOT ACT), which states that critical infrastructure represents, "those 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." This definition (or a similar one) appears in virtually all historical and contemporary federal and state policy and regulatory documents reviewed for this paper.

Policy and Regulation: However, USG contribution was not only limited to the development of physical infrastructure. During this same period, the USG began investing heavily in national defense-related departments and agencies. These departments and agencies were designed to ensure Continuity of Government (CoG), with heavy focus on managing and communicating in a post-nuclear war scenario. Cold War era USG organizations and infrastructures, especially those designated as critical to the national defense or CoG, were designed to be secure, resilient and above all else, redundant.

The following organizations were the precursors of virtually all current USG critical infrastructure players and

understanding how they came into being - and the roles they were designed to play - will help us to better understand current challenges.

The National Communications System. President Kennedy established the National Communications System (NCS) via Presidential Memorandum on August 21, 1963 [6]. The NCS was established based on the recommendations of an interdepartmental committee, following communication failures during the Cuban Missile Crisis. Perhaps less than ironically, the creation of the NCS occurred almost simultaneously with the development of the Department of Defense's (DoD) Advanced Research Projects Agency's ARPANET network.

The NCS was tasked to, ""Assist the President, the National Security Staff, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in: (1) the exercise of the telecommunications functions and responsibilities, and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack & recovery and reconstitution." [6] In short, the NCS was tasked to provide the Executive expert advice ensuring the continuity of the entire range of communications during periods of national crisis.

Over the next 40 years the role of the NCS would continue to expand within the DoD universe, eventually encompassing advice and oversite of US communication, as well as management of the radio spectrum, National Security and Emergency Preparedness (NS/EP) systems and the National Coordinating Center (NCC), which was a subordinate agency tasked with the monitoring of emergency communication systems [7].

In 2003 the NCS was transferred from DoD to the Department of Homeland Security (DHS) [8], where it continued to morph during the post-9/11 national security reorganization, until it was finally disbanded and strangely reverse-absorbed into the National Coordinating Center (NCC) by Executive Order 13618 in 2012 [9].

While the NCS has become a footnote in the US government communication's history, the process used to establish it (a post-crisis committee recommendation following critical government failures), and its vague mission statement (which allowed creeping role expansion over decades), are disturbingly like the formation and mission statements of present day USG cybersecurity organizations.

National Coordinating Center (NCC). The NCC's was originally designed to supplement the capabilities of the NCS, specifically "…in the initiation, coordination, restoration and reconstitution of national security or emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency [10]. Over time this organization continued to expand its role, eventually being designated by the White House in 2000, as the Information Sharing and Analysis Center for Telecommunications.

Federal Computer Incident Response Center (FedCIRC) and the United States Computer Emergency Readiness Team (US-CERT). Following a rash of cyber-attacks, FedCIRC was created by the US Congress in 2000. The organization was tasked to coordinate and support cyber information sharing between the various components of the USG. FedCIRC fell under the oversite and control of the General Services Administration (GSA) until 2002, when it was transferred to the Department of Homeland Security (DHS) and renamed US-CERT. The organization's original taskings gradually changed over time as well, from coordination and information sharing in 2000 to, "Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities. Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations. Responding to incidents and analyzing data about emerging cyber threats. Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture." in 2016 [11].

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT was established by DHS as the "operational arm" of the Control Systems Security Program (CSSP), which had been established by DHS in 2004. The role of ICS-CERT, and ostensibly CSSP was to support information exchange; training and exercises; risk and vulnerability assessments; data synthesis and analysis; operational planning and coordination; watch operations; and incident response and recovery. As was the case with NCS and NCC, ICS-CERT absorbed CSSP in 2012. In 2017, as part of a general DHS realignment, ICS-CERT was rolled into the National Cybersecurity and Communications Integration Center Industrial Control Systems (NCC ICS) [12].

3. Review of Contemporary USG Contributions

The Department of Homeland Security (DHS). DHS was established in with the passage of Public Law 107-296), on November 25, 2002. DHS was comprised of 22 different federal departments and agencies, see Figure 1 [13], and was tasked to oversee and coordinate, "…a comprehensive national strategy to safeguard the country against terrorism and respond to any future attacks." [14]. Under its current "Safeguard and Secure Cyberspace" role, DHS "…works to analyze and reduce cyber threats and vulnerabilities; distribute threat warnings; and coordinate the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe."

Between the years 2012 and 2017, DHS consolidated the organizational structure, personal, resources and authorities of the NCS, NCC, US-CERT and ICS-CERT into the National Cybersecurity and Communications Integration Center (NCCIC), with the mission to, "reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center." On November 16, 2018, roughly a year after the last DHS consolidation (ICS/US-CERT), President Trump signed the Cybersecurity and Infrastructure Security Agency Act (CISAA) of 2018, which brought about significant changes to the National Protection and

Programs Directorate (NPPD) in addition to establishing the Cybersecurity and Infrastructure Security Agency (CISA). The NPPD was task organized into Federal Protective Services (FPS), Office of Biometric Identity Management (OBIM), Office of Cyber and Infrastructure Analysis (OCIA), Office of Cybersecurity and Communications (CS&C), Office of Infrastructure Protection (IP) [15].

CISA's mission was to lead, "the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow" [16]. In support of this mission, the CISAA organized CISA into three divisions: Cybersecurity, Infrastructure Security and Emergency Communications [16] - effectively completing the 50-year consolidation of numerous departments and agencies centers, teams, and systems under one - in this case DHS - directorate. Although the CISA mission statement seems clear and concise, one must ask what general terms like, "defend" and "secure" will mean when the mission statement task analysis is complete.

Summary. While the US government is still involved in supporting a variety of R&D efforts, a review of recently published, unclassified documents seems to indicate that the USG has refocused its primary cybersecurity and critical infrastructure efforts on assisting partners through communication, coordination, policy, and regulation.

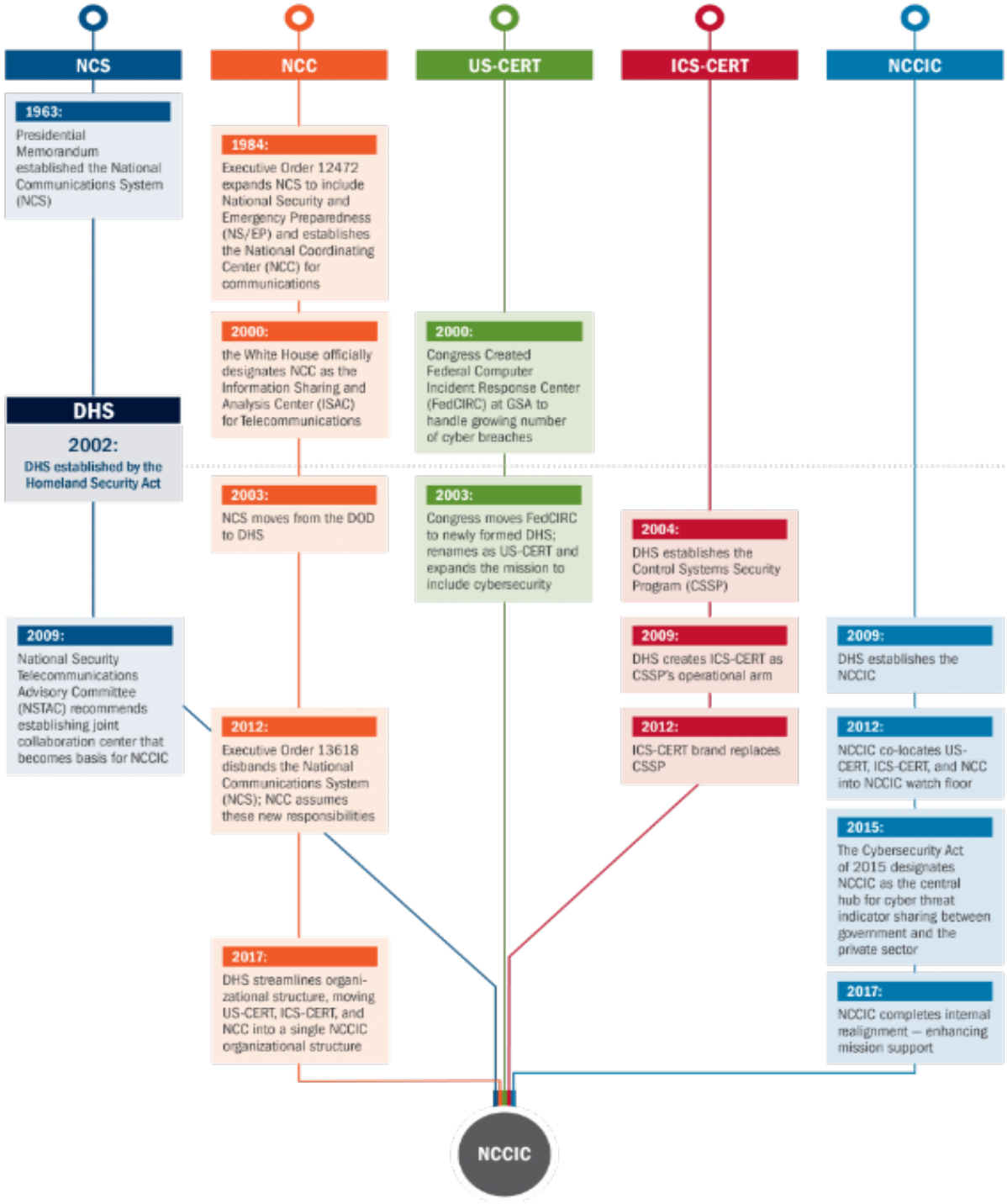

Figure 1. DHS comprised of 22 different federal departments and agencies

4. Discussion and Analysis

As previously stated, the US government remains involved in communication and information technology R&D efforts but appears to be organizing / reorganizing its agencies and departments towards supporting and coordinating roles, as opposed to a more active role in the development, deployment, and maintenance of physical and virtual critical infrastructure systems.

While there are a variety of different opinions about where this transition will lead, most agree that the United States' "victory" in the Cold War significantly impacted the perceptions about the roles and responsibilities of the USG in critical infrastructure development and deployment. While investment in a range of critical - and undeniably costly - infrastructure projects was strongly supported by most Americans in the post-World War II and Cold War eras, support for funding, even for maintenance and sustainment of established infrastructure is far secure now. A 2009 report by the National Academy of Sciences stated that the USG's historical investment in the "design, construction, and operation of critical infrastructure systems—water, wastewater, energy, transportation, and telecommunications—has not been matched with the funds necessary to keep these systems in good condition or to upgrade them to meet the demands of a growing and shifting population" [17].

Another likely reason for this transition is the fact that 85 - 90 percent of the nation's currently identified critical infrastructures are privately owned and operated [1]. Combine this private ownership with the fact that development, deployment, and maintenance of physical and virtual critical infrastructure systems require substantial, long-term financial investment (i.e. increased federal budget and supporting taxation), and the reasoning behind the apparent present-day transition of the USG from active creator and maintainer of infrastructure to a more limited, and cheaper coordinator role begins to make more sense.

While some in government might argue that nothing has really changed, and that the USG is actively pursuing the funding, development and deployment of critical infrastructure systems, the facts seem to indicate a multi-decade sea change in the perception of US government critical infrastructure roles and responsibilities. As a recent NIST paper indicated, "The most successful method for securing an ICS is to gather industry recommended practices and engage in a proactive, collaborative effort between management, the controls engineer and operator, the IT organization, and a trusted automation advisor" [1].

While collaboration in cybersecurity and the security of critical infrastructure is undeniably important, the likelihood that a reassessment of USG - and others - roles and responsibilities would improve that "most successful method" seems likely.

As indicated in this papers introduction, the USG, as one of three stakeholders in the US cybersecurity equation, has a critical role to play in the future of cybersecurity and its integration into critical infrastructure systems. Figure 2 shows the common system topology. Most US critical communications and IT infrastructure is owned by private entities - including multinational corporations, super-empowered individuals, and in some cases, competing nation states. While an argument can be made that this simply reflects the global nature of our modern economy, it ignores the potential risk associated with the facts, as well as a variety of constitutional obligations relative to commerce and national defense.

Constitutional role of government aside, it is still difficult to justify surrendering control of "systems and assets 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…" to the previously identified third-party actors, regardless of the desire of politicians or potential cost savings associated with outsourcing critical infrastructure communication and IT systems. While undoubtable cheaper, the question remains whether private entities will ever be willing to invest the billions (possibly trillions) of dollars necessary to develop redundant and survivable systems. The basic business principle of return on investment (ROI) and recent historical review of investment would seem to indicate that the likely answer would be "No." Private companies exist to make profit and expecting them to actively address what is often viewed as unlikely, if potentially catastrophic risk, is unreasonable. Figure 3 shows the proposed system topology.

5. Conclusion

The USG should immediately realign its primary cybersecurity efforts from coordination to that of an active creator and maintainer of infrastructure. Initial investment should be focused on the development, construction, and maintenance of redundant and isolated critical infrastructure systems of systems, as seen below.

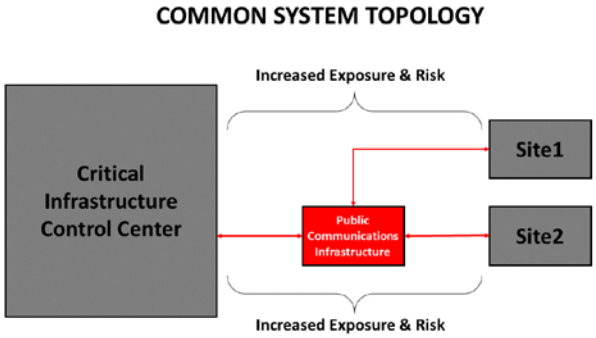

Figure 2. Common System topology

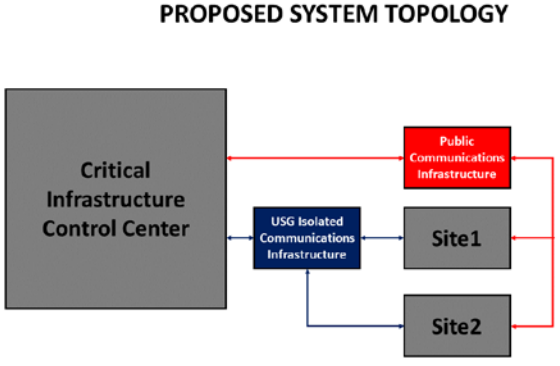

Figure 3. Proposed System topology

Critical infrastructure systems should not be reliant on the currently accepted mix of commercial, public communications and information technology infrastructure. While the risk associated with the farming out the actual critical infrastructure to private entities can be mitigated through constant vetting of business organizations, no-notice inspections, other active regulation, security of shared communication and information linking technology infrastructure - both physical and virtual - remains open to continuous attack. Isolating these links significantly improves their security, and only the USG has the resources and inherited responsibility to develop, construct and maintain the system of systems necessary to mitigate and/or defeat the real-world risks critical infrastructure faces.

While there are no silver bullets in cybersecurity of critical infrastructure for that matter, the development of an isolated, secure, and resilient USG managed communication and information technology system which supports the function of survivability of US critical infrastructure is an excellent first step. And while the cost may initially appear prohibitive, the cost of failure would be catastrophic.

References

[1] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, "Special Publication 800-82 Revision 2," National Institute of Standards and Technology, Gaithersburg, 2015.

[2] D. Stuckenberg, R. J. Woolsey and D. DeMaio, "2018 Report - Electromagnetic Defense Task Force," Air University, Maxwell Air Force Base, 2018.

[3] D. Mikkelson, "Al Gore: 'I Invented the Internet'," 5 September 2016. [Online]. Available: https://www.snopes.com/fact-check/internet-of-lies/.

[4] J. Erickson, "Top 10 U.S. Government Investments in 20th Century American Competitiveness," 6 January 2012. [Online]. Available: https://www.americanprogress.org/issues/economy/reports/2012/01/06/10930/top-10-u-s-government-investments-in-20th-century-american-competitiveness/.

[5] J. Sensenbrenner, "H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," 23 October 2001. [Online]. Available: https://www.congress.gov/bill/107th-congress/house-bill/3162/text.

[6] The Federal Register, "National Communications System," 2018. [Online]. Available: https://www.federalregister.gov/agencies/national-communications-system.

[7] US-CERT, "The National Coordinating Center for Communications (NCC)," [Online]. Available: https://www.us-cert.gov/nccic/ncc-watch.

[8] S. Barrett, "National Communications System Joins Homeland Security Department," 10 March 2003. [Online]. Available: http://archive.defense.gov/news/newsarticle.aspx?id=29323.

[9] P. B. Obama, "Executive Order -- Assignment of National Security and Emergency Preparedness Communications Functions," 6 July 2012. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-.

[10] R. Reagan, "Executive Order 12472," 15 August 2016. [Online]. Available: https://www.archives.gov/federal-register/codification/executive-order/12472.html.

[11] US-CERT, "US-CERT Description Document - RFC 2350," 30 September 2016. [Online]. Available: https://www.us-cert.gov/sites/default/files/rfc2350/US-CERT_RFC2350.txt.

[12] ICS-CERT, "About Us," [Online]. Available: https://ics-cert.us-cert.gov/about-us.

[13] DHS, "Who Joined DHS," 15 September 2015. [Online]. Available: https://www.dhs.gov/who-joined-dhs.

[14] DHS, "Creation DHS," 24 September 2015. [Online]. Available: https://www.dhs.gov/creation-department-homeland-security.

[15] DHS, "NPPD at a glance," 2018. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf.

[16] DHS, "CISA," 2018. [Online]. Available: https://www.dhs.gov/CISA .

[17] National Research Council, "Sustainable Critical Infrastructure Systems, A Framework for Meeting 21st Century Imperatives," National Academy of Sciences, Washington D.C., 2009.