Sergeant Adam Dorian Wong, threat researcher with 136th Cybersecurity Unit, presents new topics of interest including artificial intelligence and vulnerability identification to Salvadoran cyber security unit in El Salvador, December 7, 2022 (U.S. Air National Guard/Victoria Nelson)

The New "Cyber" Space Race

Integrating the Private Sector Into U.S. Cyber Strategy

By Natalie R. Alen, Gregory M. Eaton, and Jaime L. Stieler

Lieutenant Natalie R. Alen, USMCR, is the Programs and Data Officer in Charge, Reserve Affairs Division, Manpower and Reserve Affairs. Captain Gregory M. Eaton, SC, USNR, is the Joint Directorate Chief, Defense Logistics Agency Distribution Joint Reserve Force. Colonel Jaime L. Stieler, USAF, is Director of Operations, 480th Intelligence, Surveillance, and Reconnaissance Wing.

Current Russian cyber warfare capability demonstrates that nation's growing sophistication with integrating cyberpower across the whole of society as a fully fledged instrument of national power. Russia's cyber activities have blended kinetic action with escalated information domain attacks to wage ongoing, low-intensity offensive campaigns that the U.S. military refers to as *hybrid warfare*. The Russian military's integration of cyber with other "patriotic" nonstate actors includes the use of hackers and criminal organizations suspected of being directly linked to or controlled by Russian security services. James Wirtz notes, "Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives."[1]

The impact of Russia's rise as a cyberpower and the Kremlin's use of cyber warfare as an instrument of power have not gone unnoticed by U.S. Government and military leaders. The questions remain, however: What can the United States learn from Russia, and how has the United States adapted its national strategy for cyberpower to this integrated, whole-of-society approach to international competition and conflict? In *Cyberpower and National Security*, Franklin Kramer, Stuart Starr, and Larry Wentz assert:

> *Cyberpower is now a fundamental fact of global life. In political, economic, and military affairs, information and information technology provide and support crucial elements of operational activities. U.S. national security efforts have begun to incorporate cyber into strategic calculations. Those efforts, however, are only a beginning. The critical conclusion . . . is that the United States must create an effective national and international strategic framework for the development and use of cyber as part of an overall national security strategy.*[2]

Members of 169th Cyber Protection Team and members of Armed Forces of Bosnia and Herzegovina conduct cyber adversarial exercises at Private Henry Costin Readiness Center in Laurel, Maryland, June 29, 2022 (U.S. Army National Guard/Tom Lamb)

While the U.S. Government works to decrease the Nation's vulnerability to cyber attacks by improving network security and resiliency, it is time to start integrating the private sector as part of a larger information domain strategy for developing U.S. cyber advantage. As the Kremlin becomes more sophisticated in developing and using cyber warfare, the United States must also be able to mobilize a whole-of-society approach to integrate private- and public-sector capabilities, including U.S. military expertise, to compete and win in this new era of great cyberpower competition. Still, private-sector resistance to information-sharing and collaboration with the U.S. Government remains an obstacle to implementing a successful national cyber strategy. To overcome this, government leaders should examine the last time the United States faced a new and emerging domain of international competition for creating a successful integrated public-private-military organization for exercising national power.

Origins of Russian Integrated Cyberpower

Russian cyber attacks, including distributed denial-of-service (DDoS) attacks and attacks on critical infrastructure and networks, have been widely reported in the press for many years. These attacks and intrusions by ostensible nonstate actors are suspected of being directed and controlled by the Kremlin. In 2007, Russia's Federal Security Service was believed to be behind DDoS attacks on banks, media outlets, and government bodies in Estonia, which may have constituted the first use of cyberwarfare as a coercive tool to exercise political influence.[3]

In 2008, Russian-affiliated groups, including the criminal gang known as the Russian Business Network, disrupted Georgian government communications, banks, transportation companies, and telecommunications providers in advance of a Russian ground invasion.[4] In addition, Russian "hacktivist" Web sites published lists of Georgian sites for other hackers to target, including instructions and downloadable malware.[5] Russia's Ministry of Defense subsequently created a formal branch responsible for information operations, effectively integrating military capabilities and nonstate actors under a whole-of-society umbrella for cyber and influence operations.

Moscow's malign cyber activities are ongoing, and their proven approach to advancing the Kremlin's interests using cyberwarfare as an instrument of national power presents a significant challenge to the United States in great cyberpower competition.

Lessons from the Kremlin

Perhaps the most important lesson to learn from Russia's use of integrated cyberwarfare is not technical, but organizational: the use of a single coordinating authority to effectively integrate Russian state, military, and nonstate actor capabilities across the full spectrum of information operations. According to CNA, Russian military theorists do not even use the term *cyberwarfare*.[6] Instead, cyber operations are considered part of the broader term *information warfare*, which Moscow views as a means for

> *enabling the state to dominate the information landscape . . . and is to be employed as part of a whole of government effort, along with other, more traditional, weapons of information warfare that would be familiar to any student of Russian or Soviet military doctrine, including disinformation operations,* [psychological operations], *electronic warfare, and political subversion*.[7]

This viewpoint is echoed by author Yavor Raychev, who highlights key differences in the concepts of cyberwarfare in Russian and American politico-military thought.[8] According to Raychev, Americans view cyberwarfare as a part of modern hybrid war, which blends conventional warfare, irregular warfare, and cyberwarfare.[9] But as Raychev points out, "In the Russian tradition, before the disintegration of [the Soviet Union], 'hybrid war' referred rather to *political and information operations*."[10] This raises the question of what the U.S. Government's strategic approach should be to integrate the information domain as an instrument of cyberpower, incorporating U.S. military and private-sector capabilities.

Current U.S. Cyber Strategy and Public-Private Partnerships

Public-private partnerships between industry and the U.S. Government around cyber protection and initiatives began during the Bill Clinton administration, and they continue to expand.[11] Whereas the Russian military has employed criminal nonstate actors to augment and execute its cyber capabilities, the United States has leveraged the talent and expertise of respected U.S.-based firms to collaborate on cybersecurity for critical infrastructure in the public and private sectors. The 2018 National Cyber Strategy calls for "technical advancements and administrative efficiency across the Federal Government and the private sector" to secure cyberspace.[12] Similarly, the 2018 Department of Defense (DOD) Cyber Strategy identifies the need to increase the resilience of U.S. critical infrastructure through interagency and private-sector partnerships.[13] The Department of Homeland Security (DHS) leads this effort through the Cybersecurity and Infrastructure Security Agency (CISA) to build stronger defense and resilience through public-private partnerships.[14] For example, CISA oversees information-sharing programs, such as sector-specific Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). These nonprofit, member-driven organizations have been formed by private-sector critical infrastructure owners to gather, analyze, and disseminate cyber threat information between government and industry in order to promote better cybersecurity information-sharing and enhance collaboration and information-sharing among the private sector.[15]

While these partnerships have succeeded in improving U.S. cyber defenses, there are calls for greater integration between government and private-sector corporations to further develop

U.S. cyber capabilities for the private, civil, and defense sectors. For the past several years, General Paul Nakasone, commander of U.S. Cyber Command (USCYBERCOM) and director of the National Security Agency (NSA), has actively pursued partnerships with technology companies, emphasizing that the private sector and Silicon Valley are at the forefront of innovative thinking.[16]

Former USCYBERCOM commander and NSA director Admiral Mike Rogers argues that the United States is not taking an optimal approach when it comes to government and private-sector relations. Currently, we are collaborating in a manner wherein the public and private sectors are internally focused and inform one another if something relevant is discovered. Admiral Rogers advocates that the United States should move beyond collaboration and into integration, where the government and private sector work together around the clock on cybersecurity in a mutually beneficial partnership.[17] Integrated partnerships between the government and private-sector tech companies signal momentum toward strengthening alliances and attracting new partnerships, one of the strategic lines of effort in the 2018 DOD Cyber Strategy.[18]

The strategy calls for greater sharing of information among allies and other key partners to enhance the effectiveness of collective cyber operations and to build trusted private-sector partnerships. While the strategy promotes information-sharing, concerns remain over the speed with which information is shared and declassified for use. In a memorandum to the Director of National Intelligence, several combatant commanders raised concerns about the inability to share and circulate overly classified intelligence regarding adversary behaviors and receiving intelligence too late.[19] The memo depicts significant challenges in information-sharing with the interagency, allies, and key partners. If the United States aims to advance government and private-sector partnerships to leverage the innovations of Silicon Valley, the speed and scope of information being shared will require a more progressive approach.

Big Tech, the U.S. Military, and the Information Domain

In the United States, most cyber architecture, operations, and expertise reside in the civilian marketplace.[20] Despite this, the current U.S. approach to cyber operations does not effectively integrate private-sector expertise. To compete successfully against Russia's authoritarian system, a balanced whole-of-society approach is needed that is both reflective of our democratic values and effective against our adversaries. As noted by Raychev, "It can be concluded that the Western view on cyberwar is predominantly military-focused and technocratic. It views cyberwar in the broader context of cyber conflict as a modern form of fighting, but hardly grasps its social dimensions."[21] While experts can disagree with Raychev on the U.S. Government's understanding of the full context of cyber interactions, it is evident that gaps exist between this military view of cyber operations and the untapped civilian resources that do not integrate well with the military-minded approach.

Joint Publication (JP) 5-0, *Joint Planning*, codified the Chairman of the Joint Chiefs of Staff's recognition that successful use of military power in support of U.S. interests is coordinated closely with the other three instruments of national power: diplomatic, informational, and economic.[22] Interagency coordination among what is known as the "3Ds"—diplomatic, development, and defense establishments for planning and conducting operations—is a critical element of U.S. engagement policy and success. Exploring the concept of greater integrated public-private partnerships in the information domain through interagency coordination has increased applicability to the new era of cyber competition and operations.

The principles of interagency cooperation are outlined in military doctrine such as JP 5-0, and the National Security Council continues to facilitate the "mutual understanding and cooperation" necessary to achieve unity of effort in wielding all instruments of national power.[23] However, big tech firms have been reluctant to fully collaborate with the U.S. Government on cyber issues. This inhibits a unity of effort between public- and private-sector entities for use of, and protection within, the cyber realm. As noted by Darko Trifunović
, leading tech corporations exposed by the Edward Snowden leaks as engaging in U.S. cyberpower missions reacted by distancing themselves from "political subordination or participation in the national distribution of cyber war."[24] In addition, some private-sector firms have turned away from national cybersecurity protection programs and have opted to look for alternate solutions of their own to provide cyber protection. According to the Carnegie Endowment for International Peace, "the more resourceful and sophisticated private sector entities are scaling up their own efforts to address cyber threats. In addition to a range of security measures, many have turned increasingly to the risk challenging mechanism offered by cyber insurance policies. Yet the cyber insurance coverage presently available provides only a limited, uncertain, and ad hoc solution."[25]

The stand-up of CISA in 2018 as an independent Federal agency under DHS, similar to the Federal Emergency Management Agency, was an attempt by the U.S. Government at creating a single organization responsible for integrating cybersecurity across the Federal civilian agencies and to provide for greater public-private cooperation on protecting critical infrastructure networks.[26] Since its inception, however, CISA has been widely criticized by privacy advocates and big tech companies, such as Apple and Amazon, for allowing data to be shared with other companies and the U.S. Government.[27] An internal DHS Office of the Inspector General report concluded that improvements in data-sharing are still needed.[28] A May 12, 2021, executive order on improving the Nation's cybersecurity was aimed at addressing the need for greater information-sharing among departments and agencies and the private sector, but issues still remain between CISA and the private sector over privacy and collaboration.[29]

Participants analyze metadata to identify any suspicious activity on network during 2-week cyber exercise Tacet Venari, at Ramstein Air Base, Germany, May 12, 2022 (U.S. Air Force/Jared Lovett)

A Digital Arm for U.S. Cyber Integration

A potential solution for integrating the private sector into U.S. cyberpower strategy could be adding a fourth pillar—*digital*—to the 3Ds for protecting U.S. national security in the information domain. A new fourth "D" could serve to broker cyber information and innovation from big tech companies with the cyber defense and operations capabilities of the government and the U.S. military while still preserving the independence of the private sector. Akin to how the U.S. Agency for International Development operates as lead for the *development* arm of the 3Ds of U.S. foreign policy, an independent, civilian-led agency could drive U.S. cyber interests and economic prosperity in the information domain by using partnerships and investments that protect critical infrastructures. A new D agency could also serve as a conduit for Federal research and development in cyber technology and technology transfer programs. A similar model of public-private partnerships was adopted during the Cold War period with the creation of agencies such as the National Science Foundation and the Defense Advanced Research Projects Agency. Federal funding for research and development resulted in the creation of new scientific and technical capabilities leading to the establishment of new industries, benefiting both the Federal Government and the private sector.[30] A similar leading digital pillar of government would not only sustain investment and innovation in the information domain but also strengthen the other instruments of national power and provide the organizing energy needed to maximize U.S. public-private coordination in great cyberpower competition with Russia.

The concept of a truly integrated fourth D, or digital arm, would also require the ability to ensure separation between civilian and military activities within the competition continuum.[31] As demonstrated in the 2018 petition by 4,000 Google employees who demanded "a clear policy stating that neither Google nor its contractors will ever build warfare technology," many within the U.S. cyber technology field are uncomfortable with working toward a U.S. cyber advantage if it means working in direct support of DOD objectives.[32] Furthermore, controversy remains over the law of armed conflict principle of *distinction* as applied to civilians participating in direct hostilities in the information domain.[33] A digital arm of what would become the 4Ds would need to provide the necessary privacy, oversight, and coordination among all U.S. cyber technology activities. At the same time, it also should build clear distinctions between civilian capabilities and government or military objectives and position the United States to better engage in an open whole-of-society approach to compete against Russia and other nation-states in the information domain. Such an organization further would need authority to develop incentives for private-sector firms to overcome privacy and data-sharing concerns, such as grants, limited liability protections, and access to cybersecurity research, to name a few.[34]

Sergeant Ian McConnell, cyber warfare operator for Defensive Cyberspace Operations–Internal Defensive Measures, 8th Communication Battalion, works on his network hacking plans during Cyber Yankee 22, on Camp Nett, Niantic, Connecticut, June 13, 2022 (U.S. Marine Corps/Ashley Corbo)

Integrating the Information Domain

Establishment of a fourth D organization to integrate government and private-sector activities while keeping civilian and military objectives separate is needed for achieving unity of effort in the era of great cyberpower competition. According to one article:

> *Governments have a unique capacity to facilitate information sharing and engagement. Doing so would help rebuild the relationships among the innovation triangle—the public sector, private industry, and academia—and would encourage mutual understanding, a necessary step for breaking down the cultural barriers that restrict collaboration between government and high-tech firms.*[35]

Fortunately, a template for this very type of organization was designed by the U.S. Government more than 60 years ago in response to another national security domain challenge stemming from Russia. In 1957, the Soviet Union launched its first satellite—Sputnik. This triggered what came to be known as the space race and drove the need for the United States to rapidly mobilize both government and private-sector capabilities into the space domain.[36] The National Aeronautics and Space Administration (NASA) was thus created in 1958 and continues to oversee America's space program, integrating civilian and military capabilities. The National Aeronautics and Space Act, the legislation that created NASA, "allow[ed] the agency to enter into contracts with industry and educational institutions and call[ed] for the widest possible practicable and appropriate dissemination of information."[37] Quoting directly from the original act, Sec. 103, paragraph b:

> *The Congress further declares that such activities* [aeronautical and space] *shall be the responsibility of, and shall be directed by, a civilian agency exercising control over aeronautical and space activities sponsored by the United States, except . . . activities peculiar to or primarily associated with the development of weapons systems, military operations, or defense of the United States.*[38]

This type of legislation and organizational arrangement echoes the calls by General Nakasone and Admiral Rogers for providing greater integration and information-sharing with the private sector in the information domain, while separating the private sector from any military cyber activities conducted by USCYBERCOM or other DOD entities.

Extreme Makeover: CISA Edition

At its creation, CISA may have been imagined as a NASA-like solution; however, in its initial 4 years of existence, it has yet to capture the public imagination or energize the private sector in the same way as NASA did. Early challenges with managing data privacy and data-sharing have undercut CISA's effectiveness in fully integrating the private sector into U.S. cyber strategy. For CISA to become the digital organization to integrate government and private-sector efforts across cyber, it would benefit from following the same path as NASA.

A first step would be decoupling CISA from DHS to give the agency more operational independence and to increase the agency's visibility and public profile as the U.S. Government's face, or digital arm, for cyber security. Former head of CISA, Christopher Krebs, has publicly advocated for CISA breaking out from DHS and becoming a standalone agency to give the private-sector and other stakeholders a clearly visible "front door" for working with the government to combat cyber threats.[39]

Second, CISA should be invested with greater budget authorities for sponsoring cyber research and development and for incentivizing private-sector participation through contracting and grants. Although CISA currently oversees industry forums for sharing information on protecting critical infrastructure, such as the ISACs and ISAOs, participation and membership are strictly voluntary, and CISA offers only programmatic support. A new fiscally empowered CISA could continue to manage and leverage these existing relationships while being able to incentivize greater participation through access to grant programs and research and development funding.

Finally, a newly independent and rebranded CISA could serve as a "cyber center of excellence" by collecting and promulgating cyber information, cyber expertise, and best practices from government, academia, and the private sector, while keeping offensive cyber objectives separated. This reimagined CISA could serve as a magnet for developing U.S. cyber talent by not only increasing its existing training offerings but also creating internships, sabbatical opportunities, research assistantships, and funded executive-in-residence programs with tech companies to accelerate the growth of cyber talent both for the U.S. Government and industry. Rotational assignment opportunities with other governmental agencies and the military departments could also serve to "cross-pollinate" talent and build professional networks needed to achieve the unity of effort required for great cyberpower competition.

Today, much of the U.S. cyber talent and capabilities reside in the private sector. A successful national cyberpower strategy must be able to integrate these resources, as Russia has effectively demonstrated, while maintaining our uniquely American character. An organized and flexible integration of government and private-sector tech capabilities in the United States requires an approach that facilitates information-sharing and unity of effort in support of national interests while at the same time protecting privacy concerns and maintaining the freedom of association foundational to American values. The reinvention of CISA into a NASA-like organization responsible for integrating public- and private-sector activities on the development and use of cyber provides the potential means for establishing a unity of effort between the government and the private sector. This would allow the U.S. Government to employ a whole-of-society approach while ensuring private-sector cyber tech companies can maintain separation from direct hostilities within the information domain. **JFQ**

Notes

[1] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 31, available at <https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf>.

[2] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: NDU Press, 2009).

[3] Michael Connell and Sarah Vogler, *Review of Russia's Approach to Cyber Warfare* (Arlington, VA: CNA, September 2016), 13, available at <https://apps.dtic.mil/sti/pdfs/AD1019062.pdf>.

[4] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008; Connell and Vogler, *Review of Russia's Approach to Cyber Warfare*, 18.

[5] Connell and Vogler, *Review of Russia's Approach to Cyber Warfare*, 17.

[6] Ibid., 3.

[7] Ibid.

[8] Yavor Raychev, "Cyberwar in Russian and U.S.A. Military-Political Thought: A Comparative View," *Information & Security: An International Journal* 43, no. 3 (2019), 354.

[9] Ibid., 351.

[10] Ibid., 349. Emphasis added.

[11] Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (2016), 43–62.

[12] *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 21, 2018).

[13] *Department of Defense Cyber Strategy* (Washington, DC: Department of Defense [DOD], September 2018).

[14] "Protecting Critical Infrastructure," Cybersecurity and Infrastructure Security Agency (CISA), September 7, 2021, available at <https://www.cisa.gov/protecting-critical-infrastructure>.

[15] "Information Sharing and Awareness," CISA, February 16, 2022, available at <https://www.cisa.gov/information-sharing-and-awareness>.

[16] Mark Pomerleau, "U.S. Cyber Command's Top General Makes Case for Partnering With Tech Firms," *C4ISRNET*, August 25, 2020, available at <https://www.c4isrnet.com/cyber/2020/08/25/us-cyber-commands-top-general-makes-case-for-partnering-with-tech-firms/>.

[17] Ryder Ashcraft, "Admiral Mike Rogers, USN (Ret.)," *DOD Reads: What Are You Reading?* podcast, April 26, 2021, available at <https://anchor.fm/dodreads/episodes/Admiral-Mike-Rogers--USN-Ret-eubfn6>.

[18] *Department of Defense Cyber Strategy.*

[19] Betsy Woodruff Swan and Bryan Bender, "Spy Chiefs Look to Declassify Intel After Rare Plea from 4-Star Commanders," *Politico*, April 26, 2021, available at <https://www.politico.com/news/2021/04/26/spy-chiefs-information-war-russia-china-484723>.

[20] Max Smeets, "U.S. Cyber Strategy of Persistent Engagement and Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security* 35, no. 3 (2020), 450.

[21] Raychev, "Cyberwar in Russian and U.S.A. Military-Political Thought," 353.

[22] Joint Publication 5, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), xv, available at <https://irp.fas.org/doddir/dod/jp5_0.pdf>.

[23] Ibid., I-24.

[24] Darko Trifunović and Zoran Bjelica, "Cyber War—Trends and Technologies," *National Security and the Future* 21, no. 3 (2021), 76, available at <https://doi.org/10.37458/nstf.21.3.2>.

[25] Ariel E. Levite, Scott Kannry, and Wyatt Hoffman, *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance* (Washington, DC: Carnegie Endowment for International Peace, October 2018), available at <https://carnegieendowment.org/files/cyber_insurance_formatted_final_web.pdf>.

[26] Cynthia Brumfield, "What Is the CISA? How the New Federal Agency Protects Critical Infrastructure," *CSO Online*, July 1, 2019, available at <https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html>.

[27] Graeme Caldwell, "Why You Should Be Concerned About the Cybersecurity Information Sharing Act," *TechCrunch*, February 7, 2016, available at <https://techcrunch.com/2016/02/07/why-you-should-be-concerned-about-cisa/>.

[28] Jordan Smith, "CISA Aims to Improve Cyber Threat Data Sharing Problem," *MeriTalk*, October 9, 2020, available at <https://www.meritalk.com/articles/cisa-aims-to-improve-cyber-threat-data-sharing-program/>.

[29] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

[30] David H. McCormick, Charles E. Luftig, and James M. Cunningham, "Economic Might, National Security, and the Future of American Statecraft," *Texas National Security Review* 3, no. 3 (Summer 2020), 56, available at <https://tnsr.org/2020/05/economic-might-national-security-future-american-statecraft/>.

[31] Joint Doctrine Note 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), 2–3, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.

[32] Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times*, April 4, 2018.

[33] David Wallace, Shane Reeves, and Trent Powell, "Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines," *Harvard National Security Journal* 12 (2021), 186, available at <https://harvardnsj.org/wp-content/uploads/sites/13/2021/02/HNSJ-Vol-12-Wallace-Reeves-and-Powell-Direct-Participation-in-Hostilities-in-the-Age-of-Cyber.pdf>.

[34] Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," Department of Homeland Security, August 6, 2013, available at <https://www.dhs.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework>.

[35] McCormick, Luftig, and Cunningham, "Economic Might, National Security, and the Future of American Statecraft," 58.

[36] "The Birth of NASA," National Aeronautics and Space Administration, March 28, 2008, available at <https://www.nasa.gov/exploration/whyweexplore/Why_We_29.html>.

[37] W.D. Kay, *Defining NASA: The Historical Debate Over the Agency's Mission* (Albany: State University of New York Press, 2005), 6.

[38] *National Aeronautics and Space Act of 1958*, H.R. 12875, Pub. L. 85-568, 85th Cong., 2nd sess., July 29, 1958, available at <https://history.nasa.gov/spaceact.html>.

[39] Suzanne Smalley, "Ex-CISA Chief Krebs Advocates for Standalone Cyber Agency. Experts Say That's Impractical," *Cyberscoop*, August 12, 2022, available at <https://www.cyberscoop.com/cybersecurity-experts-say-cisa-cannot-stand-alone/>.