Stanford | Cyber Policy Center
Freeman Spogli Institute

ADDITIONAL PRIORITIES

STANFORD CYBER POLICY CENTER

Kelly Born

ADDITIONAL PRIORITIES

New and emerging technologies promise to be amongst the most influential forces of this century and will transform every aspect of our public and private lives. The policies developed to govern these new technologies will play a pivotal role in shaping our global future. The incoming administration and Congress is encouraged to make significant headway by considering the recommendations included by the authors highlighted here.

At the same time, a range of important issues are necessarily left unaddressed in this report, but are too significant to fail to mention. The following section on Additional Priorities highlights other areas requiring urgent attention from federal policymakers. These priorities are covered thoughtfully in related publications, including the Aspen Cybersecurity Group's **A National Cybersecurity Agenda for Resilient Digital Infrastructure** and the German Marshall Fund's **#Tech2021 - Ideas for Digital Democracy**, while these and many more urgent needs are addressed in the **March 2020 Cyber Solarium Commission Report**.

- **Education and Workforce:** The **prior** **two** administrations have highlighted that the nation's cybersecurity workforce is a "strategic asset" suffering from a persistent supply shortage: employers in the United States alone report over **520,000** open cybersecurity roles. The field is both under-staffed, and much less diverse than it should be. To address this, policymakers and the field writ large must increase awareness of cybersecurity as a potential career path, improve relevant education and skill development, and support the public and private sector in improving their practices to ensure better representation from underrepresented groups.
- **Protecting the Public Core:** The public core point to the core elements that enable the Internet to function, and that create extraordinary public value. It is comprised of the primary rules,

processes, protocols and infrastructure that allow Internet operability, including packet routing and forwarding, naming and numbering systems, cryptographic means of security and identity, etc. When these central elements of the public core were created, the need for strong security features was less clear. It is now too late to supplant many of these elements with more secure substitutes. Instead, many argue that protecting the public core will require the development of **new universal norms** as a basis for responsible behavior, as suggested by the Global Commission on the Stability of Cyberspace in 2018 on which the Cyber Center's Marietje Schaake served. Development of such norms will require global collaboration between state and non-state actors, as well as with the private companies and international nonprofits that manage most aspects of the public core.

- **Cybersecurity Metrics:** It has been widely noted that the U.S. government lacks even the most basic data about the frequency and severity of cyber attacks, the most prevalent security failures, and the most successful interventions impeding attempted attacks, as well as data or research indicating the return-on-investment for security measures taken. These gaps make it difficult to incentivize better government and private sector risk management. Experts have recommended that the government must, most urgently: develop a Bureau of Cyber Statistics, as **recommended** by the U.S. Cyberspace Solarium Commission; begin to collect a limited set of basic data; and begin to assess the cost-effectiveness of competing cybersecurity frameworks.

- **Supply Chain Security:** Most new technologies include hardware and software components sourced from multiple vendors, with additional potential vulnerabilities introduced during assembly and routine updating. To address this, experts have proposed a wide range of interventions including: reforming the federal acquisition process; improving transparency, including the potential introduction of "ingredients lists" indicating software and hardware components integrated into new technologies, and new device labeling regimes; mandating risk analysis; creating "critical technology testing centers"

as recommended by the U.S. Cyberspace Solarium; increasing competition amongst producers; and transferring some liability for supply-chain risk to the primary vendors responsible for integrating complete products and systems.

- **Public-Private Sector Collaboration:** In cyberspace the private sector, rather than the government, is often the primary actor. In order to either proactively disrupt threats before harm occurs, or better respond to and recover from cyber events, the U.S. government must better communicate with the private sector regarding emerging threats, and establish mechanisms for better operational cross-sector collaboration. Experts have noted that doing so will require the creation of new roles within federal government, new incentives for law enforcement (who are currently rewarded more for prosecution of crimes than for disruption of crimes before they occur), revisions to legal barriers that inhibit government-private sector coordination, and more.

- **Predictive AI and Algorithmic Bias:** Predictive analytics tools use algorithms and machine learning, informed by historical data, to predict the likelihood of future outcomes. Their use in the private sector, by companies like Amazon to recommend future purchases, has been seen as (relatively) innocuous. However, these tools have been increasingly deployed in the public sector, with **demonstrated biases** in terms of race, age and gender when informing **housing loan decisions**, **prison sentencing and parole eligibility**, and more. To address these concerns, experts have suggested: mandating government disclosure of all predictive analytics tools in use by government, and their impacts; requiring audits of decision-making algorithms before they are adopted; issuing guidelines for assessing algorithms during the government procurement process; and Congressional designation of **regulatory sandboxes and safe harbors** for predictive technologies. Congress has also introduced several relevant acts, including the Facial Recognition and Biometric Technology Moratorium Act of 2020, and the No Biometric Barriers to Housing Act and Algorithmic Accountability Act of 2019.