STIMSON

PRESIDENTIAL INBOX MEMO

Cyber Program

November 2024

Confront the Cybersecurity Challenge

Five policy priorities for an incoming U.S. administration

By Allison Pytlak

TOPLINE

Cybersecurity loomed large over the 2024 U.S. presidential election. At the same time, the online threat environment is evolving faster than policymakers can keep up with. From hacking operations to ransomware and spyware, U.S. government, businesses, and individuals are feeling the impact. Reducing risks and addressing threats requires leadership, vision, and partnerships. In today's globally connected society, cooperation is essential to navigating an increasingly interdependent world.

This policy memo suggests five priority areas for an incoming administration: critical infrastructure protection, enforcing accountability, improving internal coordination, digital solidarity, and building capacity.

THE PROBLEM

Cybersecurity is a growing threat to U.S. national security, highlighted during the 2024 election by cyber-attacks on critical infrastructure, foreign hacking operations, and the overwhelming influence of digital technologies on American lives. One pre-election survey showed that cybersecurity was among the top four most important foreign policy issues for voters, behind climate change, immigration, and terrorism.

Cyber should be important for voters—but also for an incoming administration. The cyber threat landscape is evolving faster than ever, and the impact of cyber operations on personal, national, and international security cannot be overstated.

ESSENTIAL CONTEXT

The digital security environment has changed considerably since President Trump's first term in office.

The cyber capabilities of states – including some U.S. adversaries like Iran – have become more sophisticated, sometimes converging with the activities of more 'traditional' cyber criminals. Cyber operations are playing a role in Russia's war on Ukraine and in Gaza, while Chinese hacking of Western critical infrastructure is intensifying. The vulnerability of U.S. critical infrastructure was highlighted through revelations about malicious activities, like those of Volt Typhoon, a state-sponsored actor based in China that has been accused of developing capabilities to disrupt critical communications infrastructure between the U.S. and Asia in future crises. Meanwhile, North Korean cyber actors have relied on offensive cyber capabilities to circumvent international sanctions and acquire illicit revenue by attacking commercial firms, international organizations, and other sectors.

Commercial spyware firms are arming state and non-state actors with the technologies to target U.S. interests, while also enabling surveillance and censorship against citizens and dissidents abroad.

Cybercrime is on the rise, with 2024 being a record year for cyber-enabled scams, ransomware attacks, and crime. Since 2021, the U.S. government has identified nearly 5,000 ransomware attacks totaling payments of about $3.1 billion USD. In the U.S., nearly 400 healthcare institutions were successfully hit by ransomware in 2024 alone. Online scams have also grown in scale and profitability in the last year. According to the FBI, losses due to investment scams surpassed all other online fraud types, accounting for more than $4.5 billion USD in losses in 2023.

Cybersecurity cannot be separated from the global digital ecosystem and keeping America secure against foreign and economic threats. There is a growing push from some states for "digital sovereignty," which champions a top-down, state-centric approach to data and internet governance that emphasizes domestic control of cyberspace including data, networks, and data centers. In response, the U.S. and its allies are advancing an approach of "digital solidarity" which stresses cooperation and a free and rights-respecting Internet to boost economic prosperity and technological innovation.

Despite a fast-moving and complex landscape, the U.S. and many of its allies have been making good strides to deter and respond to cyber incidents in recent years.

Internationally, the U.S. is leading an ever-growing alliance to counter ransomware and has been taking both unilateral and collective action against spyware vendors. It pursues accountability for hostile and malicious cyber activity through sanctions, attribution statements, and other tools in the diplomatic kit while also building up the defensive cyber capabilities of allies and partners.

In 2024, the U.S. published its first International Cyber Security and Digital Strategy which complements its national such strategies and demonstrates recent investment in cyber diplomacy. Important steps are being taken to improve the security of software and supply chains, such as by encouraging "secure by design" principles and through public-private partnership. A study assessing the viability of a uniformed service for cyber defense is underway, following other efforts to shore up the cyber defense capabilities of the U.S. military.

In his first term, President Trump demonstrated a mixed record on cyber issues. As president, he signed the first national cybersecurity strategy in 15 years, which became the basis for much of the US's current strong approach to cyber attribution and provides for the use of so-called offensive cyber capabilities and enhanced cyber defense and deterrence. His administration's efforts to check Chinese power included efforts around technology and cyber. However, Trump's public firing of then-director of the Cybersecurity and Infrastructure Security Agency (CISA) Christopher Krebs in the aftermath of the 2020 presidential election over claims of election fraud, coupled with other activities in online disinformation, have negatively affected what some might describe as a generally positive record on cyber issues.

Much is yet to be revealed about the incoming administration's policies and plans for cybersecurity and cybercrime. There is a lot of speculation about what level of continuity can be expected from the Biden administration and who will fill key roles. Cyber has traditionally been a mostly bipartisan issue, but each party brings a unique approach and priorities. The President-elect has expressed a very different view about the value of multilateralism to his predecessor, and his network of advisors and allies will likely bring shifts, as well. Tech leaders, for example, are already playing a larger and more active role. It is widely anticipated that existing initiatives on tech sector regulation and liability will be affected and rolled back, in favor of innovation over regulation. President-elect Trump also holds a different orientation toward historical U.S. adversaries like China, Iran, and Russia, as well as U.S. allies. These foreign policy dynamics will likely influence how the U.S. competes and cooperates in cyberspace. At its core, cyber is an extension and tool of geopolitics. Thus, cybersecurity and cybercrime will inherently be affected as relationships and dynamics change as a result of other policies.

POLICY RECOMMENDATIONS

Amid a sea of speculation, here are five areas for the incoming administration to focus on:

Protect critical infrastructure. Cybersecurity is, at its foundation, focused on keeping assets secure and resilient. This protection is most important for the infrastructure that we depend on for clean water, electricity, energy, medical care, education, banking, finance, and communication, among others. Cybersecurity threats to critical infrastructure are a strategic risk to national security, economic prosperity, and public health and safety -- as numerous high-profile operations in recent years have shown.

CISA plays a central role in protecting such infrastructure and networks against increasingly complex cyber threats. CISA is currently experiencing pushback from certain industries around the limits of its mandate and incident reporting, and it faces an uncertain future if certain proposals found in the Project 2025 plan see formal adoption. The Agency has done important and effective work since its establishment and must be adequately funded and supported to meet the cyber threats of tomorrow. Clarifying its responsibilities and streamlining its efforts with that of other agencies, and across different industries, will be necessary, however. So too will be recognizing that not all critical infrastructures experience the same risks or have the same resourcing to meet threats. There is a role for regulation in all of this, even if that is not the preference of the new administration; strengthening the public-private partnerships that reduce risk through information sharing and incident reporting also needs attention

Promote and enforce cyber accountability. The online threat environment necessitates robust accountability mechanisms that effectively deter and dissuade adversaries. Accountability mechanisms, both positive and negative, need to be promoted *and* robustly enforced, including through cooperation with allies and likeminded partners. Doing so can draw on multiple tools of statecraft, ranging from the imposition of consequences such as diplomatic isolation, economic sanctions, and counter-cyber operations, to actions that incentivize compliance and build capacity.

The U.S. has pursued accountability in various ways through its strategies and, increasingly, through its actions. This enforcement of accountability should be continued. For example, the recommendations of the International Counter Ransomware Initiative need to be implemented, and the coalition broadened. The new administration should work with allies to strengthen methods for attributing responsibility for cyber operations that violate international law or behavioral norms. Collective and unilateral efforts such as existing blacklists that rein in the proliferation and misuse of commercial spyware and its producers should not be forgotten. The new

administration is not expected to prioritize digital rights concerns around spyware. However, the national security threats posed by an under-regulated spyware industry should be a key priority for U.S. policymakers.

Improve domestic and interagency cooperation. As cyber threats diversify and multiply, so too have U.S. response mechanisms. The result is an assortment of mandates, policies, and regulations that often exist in siloes or, at an extreme, may undercut or undermine one another.

Clarifying how different offices and agencies relate to one another, auditing existing regulations for gaps and inconsistencies, and creating an interagency task force are a few ways in which roles and regulations could be better streamlined. The Office of the National Cyber Director could be elevated to oversee such coordination, for example. And while "big picture" coordination and streamlining is essential, this cooperation should be done in a way that sets up a framework for more focused interagency and domestic coordination to address specific cyber threats or risks in targeted ways as needed (i.e. cybercrime scam operations and online fraud and ransomware require differentiated responses)

Strengthen American security through global cyber cooperation. The growing emphasis in the U.S. on digital solidarity as a check against a digital sovereignty approach is an important aspect of foreign policy and technological innovation, and for defending human rights online. Technological innovation is increasingly intwined with geopolitical competition and security. The digital economy depends on the free flow of data and interoperability.

The digital sovereignty concept has therefore been a helpful way to tackle these concerns, to advance U.S. interests, and even to serve as a bridge in U.S. relations with allies like Canada and the European Union, who sometimes have different approaches to privacy and data rights. Cyber security risks are transboundary and so is the infrastructure that underpins the Internet, and the U.S. cannot tackle these threats alone. The new administration would be wise to continue to pursue digital solidarity for all of the above reasons, but it should do so in a way that is rooted in established U.S. values and principles of freedom and human rights. Otherwise, actions taken in the name of technological innovation and protecting the digital economy could be seen simply as a tool for targeting adversaries or creating double standards for U.S. corporations and government agencies. That would ultimately undermine and harm U.S. interests and partnerships.

Build capacity for cyber defense and resilience today—and tomorrow. Cyber presents dynamic and evolving risks that require continuous investment in cyber capacity building, in all aspects. Future cyber risks will be more sophisticated—AI or

quantum computing can render today's defenses obsolete, for example, and while cloud environments generally bring greater security, they also introduce new risks that are not yet fully understood or accounted for. The cybersecurity of satellites and outer space systems is increasingly a priority, as is securing the physical security of undersea cables, as recent events have shown.

The current shortage of skilled cybersecurity professionals in the U.S. needs to be addressed through educational and upskilling efforts in partnership with the private sector. Public awareness raising campaigns can improve cyber hygiene at the level of individuals and prevent future financial loss or the theft of personal information or reduce the effectiveness of foreign influence campaigns. Digital and cyber capacity-building for partners and allies will have a direct and positive impact on international cyber stability and overall security of the United States. A whole-of-society approach is needed to build this culture of cybersecurity. In return, improved and integrated cybersecurity practices can expect to pay dividends on American defense, resilience, and economic priorities.