June 2020

country report

Konrad-Adenauer-Stiftung Office USA, Washington, D.C,

KONRAD ADENAUER STIFTUNG

Aspects of the Cybersecurity Ecosystem in the United States

Trends Before and During the Corona Pandemic

Dirk Hegen

The field of cybersecurity with all its complexities has been steadily gaining in importance over the last decade – and now, due to the Coronavirus-induced heightened dependency on digital infrastructure this process is further accelerated. This country report shows that cybersecurity has evolved into a key national security issue and gives an overview of certain aspects of the U.S. cybersecurity landscape, by tracing policy developments from before the Covid-19 pandemic as well as current legislative considerations.

It's All About Data

Today, humans produce more digital data than ever before. The "accumulated digital universe," or the total data generated globally in 2020, is estimated to be 44 zettabytes, or expressed more illustratively, 44,000,000,000,000,000,000,000 bytes.

On any given day, 500 million tweets and 294 billion emails are sent and 5 billion online searches are conducted worldwide. In 2017, the Pentagon collected 22 terabytes of data every day, while Google currently processes over 20 petabytes of data per day.

At present, accelerated through the Coronavirus pandemic, individual citizens and consumers, corporations and small and medium sized businesses (SME), civil society institutions, schools and the government increasingly rely on information and communications technology (ICT) to work, communicate, learn, pay and play.

This massive amount of private, public, business and governmental digital activity requires security, reliability and trust. In other words, cybersecurity as a public policy and national security issue is further gaining in importance.

Although an agreed-upon and uniform definition of cybersecurity is difficult to determine, cybersecurity entails the practice of protecting devices, systems, networks, and programs from (criminal to nation state) digital attacks aimed at accessing, stealing, manipulating, or destroying information.

Cybersecurity as a policy concern is a complex field, encompassing the areas of cybercrime, critical infrastructure (composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping), cyberconflict and warfare, violent extremism, network security, as well as encryption and privacy issues.

U.S. Cybersecurity in the Pre-Corona Era

Cybersecurity was already a key U.S. national security policy concern before the outbreak of the current Covid-19 pandemic, as ensuring the security of cyberspace is fundamental to protecting the U.S. economy and defense.

In addition to cybersecurity efforts at the state level - all 50 states now have chief information security officers (CISO) - there are numerous federal agencies with varying jurisdictions over cyberspace and with responsibilities to provide cybersecurity to the United States government, its businesses and people.

The maze of federal agencies, commissions, offices and departments are listed here as a reference and to illustrate the complexity of the cyber ecosystem:

- The Food and Drug Administration (FDA) manages cybersecurity risks of connected medical devices.
- The Federal Trade Commission (FTC) provides citizens with guidance on their digital interactions.
- The Federal Bureau of Investigation (FBI) investigates cyberattacks by criminals, adversaries, and terrorists.
- The U.S. Secret Service investigates cyber-enabled financial crimes.
- The Department of Justice's Cybersecurity Unit helps to shape cybersecurity legislation to protect U.S. computer networks and individual victims from cyberattacks.
- The Department of Homeland Security (DHS) builds the national capacity to defend against cyberattacks.
- The National Institute of Standards and Technology (NIST) Commission on Enhancing National Cybersecurity provides detailed short and long-term recommendations to strengthen cybersecurity in both the public and private sectors.
- The Department of Defense (DOD) Cyber Command coordinates cyberspace planning and operations to defend and advance national interests, while the DOD Cyber Crime Center (DC3) provides digital forensic services, cyber training and analysis.
- The Central Intelligence Agency (CIA) provides cybersecurity intelligence to U.S. policymakers.
- The National Security Agency (NSA) provides cybersecurity advisories, technical guidance, as well as threat assessments.
- The Office of the Director of National Intelligence Cyber Threat Intelligence Integration Center analyses foreign cyber threats to US national interests.
- The Federal Communications Commission (FCC) works to ensure the reliability and resiliency of the U.S. communications network.
- And, finally, the U.S. Department of State, "in partnership with other countries, is leading the U.S. government's efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."

This, not even exhaustive, list of federal institutions actively shaping the U.S. government cybersecurity capacity indicates great complexity, if not fragmentation, and potential obstacles to cross-departmental information sharing and cooperation, as well as problems with overall agility. According to a major reform effort currently underway, which is discussed below, the government structures and jurisdictional boundaries outlined above "fracture cyber policymaking processes, limit opportunities for government action, and impede cyber operations."

Federal Cyber and Defense Strategies

In 2018, two major strategic adjustments were made to U.S. cybersecurity policy: the White House's National Cyber Strategy and the quadrennial National Defense Strategy. The former states that: "ensuring the security of cyberspace is fundamental. Cyberspace is an integral component of all facets of American life, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities. America created the Internet and shared it with the world. Now, we must make sure to secure and preserve cyberspace for future generations."

The umbrella National Defense Strategy (NDS) also describes cyber security as a warfighting domain, by assessing that "today, every domain is contested—air, land, sea, space, and cyberspace." The NDS also contains investments in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. It aims to enable the U.S. to "provide attribution while defending against and holding accountable state or non-state actors during cyberattacks."

Based on these strategies, in November 2018, the Cybersecurity and Infrastructure Security Agency (CISA) was launched under the umbrella of the Department of Homeland Security (DHS). Its mission is to "lead the national effort to understand and manage cyber and physical risk to our critical infrastructure and work towards a secure and resilient critical infrastructure for the American people." To that end, CISA coordinates security and resilience efforts with public and private partnerships and provides technical assistance to all levels of government, including state and local, as well as to infrastructure operators nationwide.

A 2019 GAO report titled "Ensuring the Cybersecurity of the Nation" recommends that federal agencies and other entities take "urgent actions to implement a comprehensive cybersecurity strategy, perform effective oversight, secure federal systems, and protect cyber critical infrastructure, privacy, and sensitive data."

5G

Another development unfolding over the last several years, is the increasing geopolitical power competition with the United States and China vying for regional and global influence, especially in the field of information and communications technology, such as artificial intelligence, cybersecurity and 5G. 5G technology is widely regarded to have the potential to fundamentally transform society, by connecting not just people but the Internet of Things (IoT), while also requiring new 5G-specific cybersecurity strategies.

The Administration has responded to developments in 5G technology with a May 2019 Executive Order, which declared a national emergency regarding the risks associated with information and communications technology and related services supply chains. The order prohibits the purchase or use of any communications technology produced by entities controlled by "a foreign adversary" and likely to create an "undue risk of sabotage" of U.S. communications systems or "catastrophic effects" to U.S. infrastructure.

Subsequently, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) identified over one hundred persons or organizations connected to Chinese company Huawei, a global leader in 5G technology in their so-called Entity List. For Huawei, being on this list means that a specific license is required for the export, re-export, or transfer of any of its product. But Huawei aside, 5G in itself will continue to pose new security concerns for the United States.

Cyber Workforce

There is also increasing international competition for cyber talent highlighting the need for the education, retention, and expansion of the cyber workforce. In this context the White House issued another Executive Order in May 2019, supporting the development of cybersecurity skills in the U.S. workforce.

The Economic Impact of Cybercrime

During the last decade, the economic impact of cybercrime has risen progressively. A global report that focuses on the significant impact that cybercrime has on economies worldwide concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year. Common cases of cybercrime involve business email compromises (BEC), the loss of intellectual property, online fraud, financial crimes and manipulation, phishing and ransomware, often targeting seniors. In early 2020, the FBI has released the Internet Crime Complaint Center (IC3) "2019 Internet Crime Report." For that year, both individuals and businesses filed over 450,000 cybercrime complaints, with an estimated economic loss of more than $3.5 billion.

Finally, since the 2016 U.S. presidential elections, there is a growing emphasis on state-actor cyber interference in U.S. elections. In the election's aftermath, the CIA, FBI, and National Security Agency jointly stated with "high confidence" that the Russian government conducted a sophisticated campaign to influence this election through cyberattacks. Already pre-Corona, the U.S. worked on strengthening election cybersecurity and responding to cyber-enabled disinformation campaigns aimed at dividing citizens and discrediting democracy. The Coronavirus has put the state-run election infrastructures under more pressure and state budgets in enormous difficulties. Even popular culture is taking note of the issue, as evidenced by an HBO documentary film on the weaknesses of certain voting technologies.

Cybersecurity Trends in the Covid-19 Pandemic

As mentioned earlier, the coronavirus pandemic has further accelerated the transition from the analog world to the digital domain. As a response to the virus, socially-distanced telework, telemedicine, remote learning, growth in online purchasing and the now ubiquitous virtual meetings on digital meeting platforms have skyrocketed.

Corporate earning developments help illustrate this digital exodus. San Jose, California-based Zoom Video Communications' stock, as of June, has already tripled in 2020 and Zoom posted quarterly revenues of $328.2 million, up 169% compared to last year. For the 2021 fiscal year, Zoom predicts total revenues of about $1.8 billion.

In general, tech stocks have fared better than most other sectors during the coronavirus pandemic as newly-remote workers have come to rely more heavily on online services. Facebook, Apple, Amazon and Microsoft all hit new all-time trading highs in early June. Microsoft has seen strong demand for cloud services and reported that its remote-working Teams platform now has 75 million daily active users.

Big tech companies also seem to benefit from providing services for the government, such as contact tracing apps and cloud services. In the latter field, Amazon and Microsoft are in a legal dispute over a $10 billion defense contract (JEDI), while Google Cloud in May announced a deal

with the U.S. Defence Innovation Unit (DIU), a division of the DOD to build a multi-cloud management platform to detect and protect against cyber threats.

The damage created by COVID-19, might also provide incentives for governments and public health experts to put less emphasis on cybersecurity and privacy concerns in favor of technological capabilities that promise results in preventing and controlling life-and-death emergencies.

Yet, the exponential user-growth and profit development for technology companies cannot overshadow that the pandemic further amplified cyber threats and cybersecurity breaches. In early April, for instance, 500,000 Zoom account credentials were stolen and subsequently offered on the dark web.

Meanwhile, larger-scale, nation state-linked attacks also continued during the pandemic, often making use of the fear and insecurities it created. In May 2020, for instance, U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. coronavirus vaccine research. In April 2020, U.S. officials alleged an increase in attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human Services. The U.S. government responded with guidance and official alerts.

Overall, the Coronavirus induced a heightened dependency on digital infrastructure and concerns intensified that cyberattacks could cause widespread infrastructure failures that take entire cities offline, obstruct healthcare providers, public systems and networks and strongly impact national and global security.

Congressional Responses

According to Senator Angus King of Maine (I), testifying at a May 13th virtual cybersecurity Senate hearing, the current Covid-19 pandemic had "showed us how vulnerable" the United States was with respect to cyberspace.

Together with Representative Mike Gallagher of Wisconsin (R), King co-chairs the so-called Cyberspace Solarium Commission (CSC), chartered by the 2019 National Defense Authorization Act (NDAA) and named after President Eisenhower's Project Solarium, a 1950's effort to create a unified cold war strategy. The Commissions' declared aim is to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber-attacks of significant consequences."

Somewhat unfortunate for the Commission, its finished report was presented to the public on March 11, 2020 – a mere two days before the United States had begun to implement the unprecedented, Coronavirus-induced nationwide lock-downs.

Nevertheless, Senator King's sobering statement echoes a view maintaining that the current pandemic further highlighted a pre-existing need to increase investment into U.S. cybersecurity. And indeed, many U.S. think tanks and academic institutions have pointed out that the process of digitalization and automation in general, and that fast-paced developments in Artificial Intelligence, machine learning, neural networks and quantum computing in particular have increased the total cyber-attack surface available to criminal or even nation state-level actors.

The CSC's report addresses these concerns with multiple recommendations and several top leaders of other national commissions signed a joint letter on May 4th, urging Members of Congress to implement CSC's cyber workforce recommendations.

Generally the CSC seeks to "shape behavior" by working with allies and partners to promote responsible behavior in cyberspace, "deny benefits" to adversaries, and to "impose costs" by retaliating against malicious actors in cyberspace. The recommendations are made in six arenas: reforming government, strengthening norms, promoting resilience, operationalizing work with the private sector, and using military power.

More specifically, the CSC recommends a U.S. policy of "layered deterrence" - combining strong military capability with international engagement and a greater resilience at home, stating that the United States ought to build a coalition of democracies to impose penalties on those who infringe upon agreed cyber norms. This multilateral aspect was also echoed by LTG (Ret.) Ben Hodges, former Commanding General of the U.S. Army in Europe at a recent KAS event, when he stated that he would like to "see the U.S. rather lead than leave" arenas of international cooperation, such as the information space.

The prime legislative vehicle for the CSC recommendations is the fiscal year 2021 National Defense Authorization Act (NDAA) currently debated in the Senate. Some analysts contend that U.S. lawmakers' appetite to pass laws in this space might be accelerated by the pandemic and that the crisis presents an opportunity to establish a more balanced national cyber strategy with prudent risk management, contingency planning and enhanced resilience.

Yet, it remains to be seen to which degree and in which timeframe the U.S. will be able to improve its cybersecurity ecosystem, while being confronted with the effects of an unprecedented health, economic and social crisis.

Konrad-Adenauer-Stiftung e. V.

Dirk Hegen
Project Manager KAS Office USA
European and International Cooperation
www.kas.de/usa

dirk.hegen@kas.de