American Edge Project:

National Security Policy

February 2021

/edge

AMERICAN EDGE PROJECT

/edge
AMERICAN EDGE PROJECT

American Edge Project: National Security Policy

February 2021

Introduction

The United States has traditionally used a mix of hard power, soft power, and smart power (a sensible blend of both hard and soft power) to advance its interests at home and abroad. With a new administration sworn into office, it is time to build the architecture for the deployment of U.S. digital power.

This new policy framework seeks to leverage two distinctly American assets: technological supremacy, and a network of allies, partners, and friends around the world that share a commitment to democratic principles. U.S digital power will empower American technology innovation and promote it globally as a way to defend our interests and advance our values in the competition between "techno-democracies" like the U.S., European Union (EU), Japan, and other democratic allies, and "techno-autocracies" like Russia and China. The global pandemic has rapidly sped up the integration of the internet as a common denominator in every aspect of economic and cultural society. If the U.S. loses its leadership role in technology, there will be long-term consequences for national security, the global economy, standard setting, and international norms.

This report will outline an initial framework to promote U.S. digital power to ensure the American technology industry maintains its edge on its international competitors. The "three pillars" for this framework are: protecting the ability to innovate, securing U.S. cyber and data, and advancing a democratic and open internet.

Pillar One: Protecting the Ability to Innovate

It is crucial for U.S. national and economic security that the U.S offers the most capable and cutting-edge technologies and services. While the U.S. maintains an advantage in emerging technologies such as artificial intelligence (AI) and semiconductors, it has lost what was once a comfortable lead to China, with many experts thinking China is a few years behind in these technologies. More troublingly, the U.S. has fallen behind China in technologies including facial and voice technology, 5G deployment, and the commercial drone market.[1] The Trump Administration laid the groundwork for overtaking the lead in 5G technology, and the new Biden Administration has indicated this will remain a priority issue. It is fortunate there is bipartisan agreement around the understanding that the country that leads in the global telecommunications deployment and in standard setting for new technologies will influence the international economic landscape in the decades to come.

[1] Cohen, Jared and Richard Fontaine. "Uniting the Techno-Democracies." *Foreign Affairs,* November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

Ensure U.S. Supremacy in the Race for 5G

Of critical importance to the United States in maintaining its technological leadership will be the successful deployment of 5G infrastructure. The past two years have seen the race to build out 5G networks emerge as a major pillar of the U.S.-China competition – and for good reason. On the one hand, the vast scope of 5G technologies, encompassing everything from connected home devices to autonomous vehicles, represents a huge opportunity for economic growth. On the other hand, the sheer volume of data that can be passed and stored on 5G networks creates clear repercussions for the security of digital communications.

Huawei, China's leader in international 5G deployment, has long drawn the concern of national security professionals and policymakers, particularly with regard to its close ties to the Chinese government and its military. Such links prompted the U.S. House Intelligence Committee to label Huawei as a major national security concern in 2012. More recently, the Trump Administration adopted a hardline stance against the global growth of Huawei, launching significant diplomatic and public relations campaigns that sought to dissuade U.S. allies and partners from cooperating with Chinese companies on 5G infrastructure deployment. In September 2020, the Trump Administration delivered a serious blow to Huawei when it barred the sale of any 5G chips to Huawei manufactured using U.S.-designed equipment.

Despite previous U.S. efforts, the incoming Biden Administration will face several challenges to countering China's well-established foothold in the global 5G market. One key issue is how to deal with older 4G and 3G Chinese telecommunications technology currently in use across the United States and allied nations. In June 2020, the Federal Communications Commission (FCC) labeled Huawei and ZTE as national security threats and issued a "rip and replace" order for all existing Chinese 4G and 3G technology. The FCC directive presented a major problem for many small wireless carriers that have long relied on low-cost telecommunications equipment from Huawei and ZTE to supply reliable high-speed internet to rural America. This has also put the FCC in a tight spot between its dual goals of securing U.S. networks and bridging the digital divide. Integrating new Chinese 5G technology would be more cost effective for these small carriers, therefore the Biden Administration will have to work with rural America to ensure that they retain access to quality U.S.-designed ICT.

China is also well positioned to dominate the 5G space in regions outside of the United States. In 2015, the Chinese government launched its Digital Silk Road (DSR), an arm of the larger Belt and Road Initiative (BRI), in order to help developing countries improve their telecommunications networks, cloud-computing infrastructure or AI technology. As of April 2020, more than 30 countries had signed Demand Side Response (DSR)-specific Memorandums of Understand (MOUs) with China, including countries in the Middle East (Egypt and Saudi Arabia), Europe (the United Kingdom (UK) and Poland), Latin America (Peru and Cuba), and Africa (the African Union).[2] The United States has achieved only limited success in trying

[2] Triolo, Paul, and Kevin Allison. "The Digital Silk Road: Expanding China's Digital Footprint." *Eurasia Group*, 8 Apr. 2020, www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint-1.pdf.

to persuade major partners to block access to Chinese 5G infrastructure. For example, in January 2020, the UK announced that it would allow limited access to Huawei for development of 5G networks, but later released plans to fully remove Huawei's 5G technology from UK networks by 2027.[3]

The growing spread of Chinese-developed 5G technologies is of specific concern for global supply chains. Next generation "Internet of Things" (IOT) technologies and automated factories will rely on 5G infrastructure to operate. The country that is able to deploy the majority of global supply chain 5G technology will also be the one that is able to harness (or exploit) the data and intellectual property (IP) generated from these devices. Therefore, a global supply chain dominated by Chinese-manufactured 5G infrastructure would put U.S. and U.S.-partner markets at grave risk. Moreover, as was apparent during the development of 4G technology, the country that is first to market with new technological advancements is also the one that wins the lion's share of the economic growth associated with those technologies. While the United States led with many of the advancements that ultimately became 4G, Huawei is currently the global leader in patents for 5G technology, while ZTE holds the third most 5G patents among global ICT companies.[4] The incoming Biden Administration will have to step up U.S. leadership on these issues if it wants to defend against the threats and capitalize on the opportunities of 5G technology.

Increase U.S. Leadership on Influential International Standard Setting Bodies

Another area in which the United States needs to regain a leadership role is in standards setting for emerging technologies, namely 5G and AI, and norms for policies surrounding data protection, surveillance, and international patent reform. In recent years the United States has pulled back from international standards settings organizations, such as the United Nations' (UN) International Telecommunication Union (ITU), which is currently being chaired by China's Houlin Zhao. Through ITU and related groups, China is attempting to rewrite the rule book on disruptive technologies as it attempts to expand its techno-autocracy model around the globe.

As we have seen with several U.S. technology giants, exporting new U.S. technology abroad is a significant and efficient way to promote American values and culture. These technologies reflect U.S. values of excellence via market competition, as well as the market possibilities available by maintaining a free, secure and open internet. By virtue of leading in technology services, the U.S. can shape the guidelines for how technologies are used abroad. Losing the innovation edge to techno-autocracies, however, would

[3] Payne, Sebastian. "UK to Ban Installation of Huawei 5G Equipment from September." *Financial Times*, 30 Nov. 2020, www.ft.com/content/c8e7ee9a-4661-4890-a41a-6a7b59f1caba.

[3] Apelblat, Mose. "EU Auditors on 5G: Economic Potential and Security Risks." *The Brussels Times*, 13 Jan. 2021,

[4] "Global Number of 5G Patents Filed by Major Company 2020." *Statista*, 24 Nov. 2020, www.statista.com/statistics/1117922/global-number-of-5g-patents-filed-by-major-company/.

mean losing the ability to set international standards on new and emerging technology. The end result in this scenario is a U.S. that is in a disadvantaged economic position and has less power to influence geopolitical matters.

We can see this play out in real time with emerging technologies like facial recognition, an area in which China currently maintains an innovation edge. The standards for this new technology have not yet been agreed upon by leading democracies, and in the meantime China is already using the technology for surveillance purposes, including most problematically on Uighurs in Xinjiang.[5] This is notable given that the Trump Administration's final major action on China policy was declaring that Beijing's actions in Xinjiang constituted a "genocide". During his confirmation hearing to be Secretary of State, Tony Blinken indicated the Biden Administration would continue this aspect of the Trump Administration's China policy. This could prompt other nations to follow suit.[6] But without consensus around standards for technology such as facial recognition, techno-democracies are unable to prevent this technology from being used to oppress people in China or in an estimated 18 other countries that use Chinese surveillance systems.[7] Calls for a boycott or a venue change of the 2024 Winter Olympics in response to the treatment of the Uighurs are increasing and will be a telling metric in terms of international attitudes toward China.

Standard setting should be a collaborative venture with other democracies that share U.S. values, as well as the U.S. private sector. Fortunately the world's leading democracies have a long history of cooperation on issues that intersect international norms and economies. Standard setting remains one of many areas of collaboration for techno-democracies as they work to ensure democratic values are reflected in the technologies being exported around the world. The U.S. should prioritize working with allies to influence the global guidelines for major technologies such as AI, 5G, semiconductors, quantum computing, and facial recognition. Key in this effort will be sharing information amongst allies, particularly about supply chain risks, cyber and cloud security, as well as strategies to combat intellectual property theft.[8]

The U.S. should also work closely with countries in the EU on advancing standards that balance the protection of data privacy with the free flow of data across borders. Though there are differences of opinion about specific standards for data protection and surveillance technologies, the U.S. and EU ultimately share far more common ground when it comes to privacy concerns than they do with techno-autocracies. It is these shared democratic standards that should be reflected in international digital norms. President Biden took advantage of a February 2021 speech to the Munich Security Council to raise this

[5] Cohen, Jared and Richard Fontaine. "Uniting the Techno-Democracies." *Foreign Affairs,* November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

[6] Wong, Edward and Chris Buckley. "U.S. Says China's Repression of Uighurs Is 'Genocide'." *The New York Times,* 19 Jan. 2021, https://www.nytimes.com/2021/01/19/us/politics/trump-china-xinjiang.html.

[7] Brown, Megan and Dr. Andrea Little Limbargo. "TechLash and National Security: The Need for U.S. Leadership on Privacy and Security." *National Security Institute*, July 2020, https://nationalsecurity.gmu.edu/techlash-and-national-security-the-need-for-u-s-leadership-on-privacy-and-security/.

[8] Cohen, Jared and Richard Fontaine. "Uniting the Techno-Democracies." *Foreign Affairs,* November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

issue and begin the discussion with allies about a common China strategy. Future engagements with democratic allies will provide an opportunity to expand on this effort. An article in *Foreign Affairs* by Jared Cohen and Richard Fontaine explores the idea of creating a "T-12" grouping of leading techno-democracies and proposes an agenda along these lines.[9]

In addition to partnering with democracies, the U.S. government should work closely with the U.S. private sector to coordinate participation on standard setting bodies, especially those led by industry. For example, the Third Generation Partnership Project (3GPP) is the standard setting body for 5G and is a collaborative body that combines seven telecommunications standard development organizations.[10] Compared to government-led groups like the International Telecommunication Union that focus primarily on regulations, 3GPP working groups debate and determine technical standards and proper security mechanisms for global mobile communications. Working groups are composed of company representatives who meet regularly to discuss current concerns as well as long-term implications for global telecommunications. With U.S. technology experts in leadership positions at groups like 3GPP, we can ensure the platform is being used to promote American technology standards and values when setting guidelines and security standards for technology that will drive the global economy for the next several decades.

Regardless of whether government or industry officials lead international standard bodies, the U.S. government must work in close alignment with the private sector to ensure they are in agreement on major priorities regarding technology standards. The Department of Defense (DOD) made this observation in its 2020 5G Implementation Plan. In addition to engaging with 3GPP, DOD highlighted the Alliance for Telecommunications Industry Solutions (ATIS) and the Institute for Electrical & Electronics Engineers (IEEE) as standard setting bodies shaping 5G planning through both advocacy and technical contributions.[11] While the U.S. does not want to adopt the techno-autocratic approach of government interfering in domestic business planning, there is room to grow in improving the channels of communication between the U.S. government and technology industry on standard setting priorities.

[9] The T-12 countries are the United States, France, Germany, Japan, the United Kingdom, Australia, Canada, South Korea, Finland, Sweden, India and Israel. Cohen, Jared and Richard Fontaine. "Uniting the Techno-Democracies." *Foreign Affairs,* November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

[10] https://www.5gamericas.org/wp-content/uploads/2021/01/InDesign-3GPP-Rel-16-17-2021.pdf.

[11] Department of Defense. https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf

Pillar Two: Securing U.S. Technology, Networks, and Data Through Enhanced Cybersecurity

Integral to digital power at home and abroad is the ability to secure the cyber networks of American citizens, businesses, and government agencies. The recent SolarWinds hack is a reminder of the persistent and sophisticated nature of cyber threats. America's commitment to infrastructure integrity, the strongest possible cybersecurity protections, and privacy stand in sharp contrast to the internet infrastructure of techno-autocracies in which data protections are nonexistent and there is a risk of data being harvested for Chinese AI algorithms. The U.S. technology industry will be instrumental in the effort to detect and deter future cyber threats as part of a broader effort to advance U.S. digital power that upholds the privacy of U.S. citizens data through secure networks and cyber protections.

Incentivize U.S. Industry to Maintain Edge on Cyber Protections Against Techno-Autocracies

There are two primary drivers of risk when it comes to defending against cyberattacks. One is the number of complex tools available and the number of adversaries – including non-nation states – who can access them. The second is the interconnectivity of systems, which has exponentially increased during the global pandemic as people and businesses all over the world increasingly turn to technology to support remote operations. The radical increase in the number of devices connected to the internet – which has risen from around seven billion in 2011 to above 25 billion today – has dramatically increased the "threat surface" available to adversaries.

The conflation of these factors means once an adversary is able to access a private cyber network, they are able to obtain more data and potentially cause more damage than ever before. Countries such as Russia, China, North Korea and Iran are eager to exploit such access to seize U.S. intellectual property, including sensitive military capabilities and future innovations.[12] This can be used to improve their own military power or possibly identify vulnerabilities in American defense capabilities. In a worst-case scenario, an adversary nation could leverage existing access into U.S. networks to disrupt or even shut down American communications or critical infrastructure services. Americans need to look no further than the February 2021 cyberattack of the water systems in Oldsmar, Florida to see how quickly a hacker can attempt to directly harm the safety of Americans. In the case of the Oldsmar attack, a hacker was able to successfully increase the levels of chemicals in a water reservoir that supplied water to nearly 15,000

[12] Thompson, Loren B. "Why U.S. National Security Requires a Robust, Innovative Technology Sector." *Lexington Institute,* October 2020, https://www.lexingtoninstitute.org/wp-content/uploads/2020/10/100820-WHY-U.S.-NATIONAL-SECURITY-REQUIRES-A-ROBUST-INNOVATIVE-TECHNOLOGY-SECTOR-002.pdf.

residents.[13] Fortunately the attack was reversed before anyone was harmed, but the fact a hacker was able to access the systems in the first place is symptomatic of broader concerns about the vulnerability of sensitive industrial systems. No individual actor has been apprehended in connection with the attack, but it could certainly be considered a harbinger of threats to come.

With techno-autocracies reliant on cyber espionage to improve their own technologies and military prowess, the power to protect private networks is essential for U.S. national security and technological supremacy. Key to this effort is the empowerment of a competitive and innovative cybersecurity industry. In the case of the recent SolarWinds hack, a nation state – likely Russia – gained access to U.S. public and private servers through unfair advantage. However, U.S. cyber firms identified and publicized the intrusion, allowing the U.S. government to take measures to limit the impact of the hack. U.S. industry then supported the U.S. government in determining the scope and methods of the attack. Were it not for the innovation in the private sector, a foreign state might still be unknowingly expanding its presence on private U.S. networks.

The SolarWinds case shows that a robust private sector is integral toward keeping U.S. cyber networks protected against ongoing threats from foreign actors. To support ongoing innovation, the U.S. should incentivize the private sector to maintain its cutting-edge cyber practices so that it can continue to innovate to protect the nation from future cyberattacks. The Department of Defense acknowledged this in its 2018 Cyber Strategy, which included a pillar on "Promoting American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation." [14] Strong national cybersecurity will help protect intellectual property from espionage, theft, and manipulation in American research institutions and corporations, which are under near constant attack from nations including Russia, China, and Iran. A thriving domestic cybersecurity industry will also help ensure that companies that hold sensitive information relating to the COVID-19 vaccine and vaccine distribution aren't improperly compromised by foreign nations.

Strengthen U.S. Government Response to Cyber Attacks

Years before news about SolarWinds became public knowledge, the U.S. Congress identified the risk of a major cyberattack and established the Cyberspace Solarium Commission (CSC) to "develop consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."[15] As the nation looks for ways to prevent future attacks like SolarWinds, it can consult the

[13] Kevin Collier. "Lye-poisoning attack in Florida shows cybersecurity gaps in water systems." *NBC News*, 9 Feb. 2021, https://www.nbcnews.com/tech/security/lye-poisoning-attack-florida-shows-cybersecurity-gaps-water-systems-n1257173.

[14] U.S. Department of Defense. "DOD's Cyber Strategy: 5 Things to Know." 2 October 2018, https://www.defense.gov/Explore/Features/story/Article/1648425/dods-cyber-strategy-5-things-to-know/.

[15] U.S. Cyberspace Solarium Commission. "Cyberspace Solarium Commission Report." March 2020, https://www.solarium.gov.

recommendations already debated and authorized by the CSC. Of the initial 80 recommendations, 25 were incorporated into the FY2021 National Defense Authorization Act (NDAA). Several others appear particularly prescient following SolarWinds and are worth revisiting by Congress as it takes steps to improve the nation's cybersecurity.

One CSC recommendation of relevance following the SolarWinds hack is to codify a "Cyber State of Distress" to ensure the government has adequate resources to respond to a cyber incident.[16] Similar to how the Federal Emergency Management Agency (FEMA) can order more resources in the event of a natural disaster, this initiative would trigger new resources through a "Cyber Responses and Recovery Fund" to enable the government to quickly assess damages and recover from a cyber incident.

The CSC also endorsed having relevant U.S. agencies like Cybersecurity and Infrastructure Security Agency (CISA) share information and analysis with industry on threats of shared concern, including supply chain security and cyber threats. Information sharing helps build a situational awareness of current and future threats. This situational awareness can be leveraged to identify intelligence gaps or areas of vulnerability so that the U.S. government and private sector can take preemptive actions to remain one step ahead in the ever-changing cyber threat field. By maintaining a strategic channel of communication with U.S. cyber firms, information sharing can also help inform best practices to constantly raise the bar on protecting U.S. data and networks.

Another important issue the report addresses is the relationship between cybersecurity and encryption. While CSC experts were unable to reach a consensus on the balance between "maximum encryption" and "mandatory lawful access to devices," the report acknowledges that across the government and the private sector there is broad consensus on "the importance of strong encryption" as a cornerstone of data security.[17] Experts believe this applies to both data in motion and data at rest. Senior national security leaders have stated that the technology is especially valuable in protecting U.S. data against adversary nations that continuously attempt to hack into U.S. networks to steal IP on emerging technologies critical to the American economy and national security. The use of end to end encryption by some U.S. companies helps ensure their IP and users' data is kept as secure as possible. In contrast, companies based in techno-autocracies are often required to share user data directly with their governments for nefarious purposes.

The Cyberspace Solarium Commission released a report following the inauguration of President Biden to offer a digital blueprint for the new administration.[18] Similar to its initial report, a common theme throughout the blueprint was the recommendation to bolster partnerships with the private sector,

[16] U.S. Cyberspace Solarium Commission. "Cyberspace Solarium Commission Report." March 2020, https://www.solarium.gov.
[17] U.S. Cyberspace Solarium Commission. "Cyberspace Solarium Commission Report." March 2020, https://www.solarium.gov.
[18] U.S. Cyberspace Solarium Commission. "Cyberspace Solarium Commission White Paper #5: Transition Book for the Incoming Biden Administration." January 2021, https://www.solarium.gov/public-communications/transition-book.

understanding that empowering American technology will strengthen the preparedness of the federal government against a future Solar Winds-style attack. The promise of future American innovation is dependent on ensuring strong cybersecurity standards today.

Looking ahead, the CSC report recommends greater scrutiny of the opportunities and risks posed by quantum computing.[19] Given the impact this emerging technology could have on the decryption of sensitive communications, the public and private sectors should work together to ensure research and investments in quantum computing are part of the U.S.'s short-term cybersecurity strategy.

Pillar Three: Advancing a Democratic and Open Internet

One of America's greatest allies in the tech race against techno-autocracies is the U.S. technology industry and the massive research and development (R&D) investments made by technology companies to maintain an edge in key emerging technologies. U.S. tech companies promote freedom of speech, non-censorship, and the value of an open internet. The most efficient way to share and maintain these U.S. values is through U.S. technologies used abroad. To export U.S. digital power, the government must partner with the private sector and incentivize domestic innovation to help empower the U.S. tech industry to continue to thrive at home and around the world.

Encourage Policies Abroad that Reverse Harmful Data Localization Laws

The U.S. technology industry has produced consistent economic growth in the U.S., but the adoption of U.S. technology and the values inherent in such technologies have been instrumental in improving lives far beyond American borders. The open and democratic nature of the global internet has unlocked extraordinary innovation and explosive growth around the globe. Fundamental to this development has been the free flow of data across global borders.

With China's rising influence, however, some nations have gravitated toward adoption of China's restrictive and censored approach to an internet model. These nations include Vietnam, Singapore, Russia, and – perhaps most concerningly – India, the world's largest democracy. India's Parliament is currently considering a Personal Data Protection bill that would enforce a policy of data localization, in which a country silos its data within its borders to gain more control over it.

If India continues to pursue the closed internet model favored by techno-autocracies like China, a third of the world's population will have its internet data and privacy compromised by data localization policies.

[19] U.S. Cyberspace Solarium Commission. "Cyberspace Solarium Commission Report." March 2020, https://www.solarium.gov.

Central tenets of this model include a high level of government surveillance, lack of data privacy and security, and censorship of content considered politically threatening. Should this trend extend to other developing nations in South American, Asia, and Africa, it could lead to a fracturing of the global internet as we know it. This would have national security and economic consequences far beyond the immediate borders of any one country.

U.S. tech companies cannot compete as effectively when they are excessively obstructed by restrictive data laws. This is a direct challenge to today's internet, which is accessible to all people and diverse points of view. China, meanwhile, is less threatened by these policies since their companies are often subsidized by the Chinese government, enabling them to offset the costs of building local storage centers in countries in which China wants to expand its presence. This gives Chinese tech companies a substantive advantage in competing with U.S. companies in nations where data localization laws are being adopted. Over the long term, this increases the likelihood that citizens in these nations will use Chinese technology services in place of the U.S. ones currently available to them – unless there is a concerted effort by techno-democracies to fight the spread of a closed internet model.

Empower the Private Sector as "Ambassadors" for U.S. Values Abroad

The latest technological developments show that innovation in emerging technologies such as AI, semiconductors, 5G, quantum computing, and facial recognition is driven by commercial vendors rather than the U.S. government. The Department of Defense is no longer uniquely positioned to anticipate future technologies and resulting threats, unless it works alongside the U.S. technology industry to do so.

When it comes to promoting U.S. values abroad, America's most ubiquitous diplomats are often its tech companies that offer their services to people and business all around the world, from the largest cities to the most remote corners of the globe. As stated in a recent opinion piece by Admiral Jim Stavridis and Fran Townsend, "The private sector is where American technological advancements have always flourished. We must do everything we can to bolster this industry, encourage competition and allow easy adoption of private sector innovations by the Pentagon and the U.S. intelligence community."[20]

A growing obstacle to the U.S. technology industry and its influence abroad is the concerted effort by China to build a self-reliant tech industry. This is part of a broader international effort to reclaim advantages in what has traditionally been a distinctly American asset. Over the long-term, China's emphasis on a domestic market will make it increasingly difficult for U.S. companies to operate in China, including major U.S. companies that already have a presence. This will have impacts beyond the bottom line of those individual companies.

[20] Stavridis, Jim and Frances Townsend. "US tech at risk of falling behind threatening our global interests." *Military Times,* 28 October 2020, https://www.militarytimes.com/opinion/commentary/2020/10/28/us-tech-at-risk-of-falling-behind-threatening-our-global-interests/.

For example, the Chinese are investing in efforts to displace U.S. strength in chip-making, which has worrying implications for global supply chains. The same chips that power iPhones and laptops can be used for sensitive military communications and equipment.[21] Both Defense Secretary Lloyd Austin and Treasury Secretary Janet Yellen addressed the strategic significance of the domestic semiconductor industry in their confirmation hearings, tying the issue to supply chain security and technological leadership.[22] The White House has also pledged a broad supply-chain review of critical goods and an executive order to address the growing shortages of semiconductors.

All of this reflects an understanding that the continued dominance of U.S. digital power is reliant on the strength of our domestic semiconductor industry. It remains to be seen if this understanding will translate into federal investments that would help the U.S. maintain an edge in this technology, both in domestic manufacturing and in influencing strong security standards for microchips abroad. Investments in incentivizing domestic production for microchips will help ensure the U.S. semiconductor industry continues to lead the world in development of a technology essential to future innovation.

Another obstacle facing U.S. technology companies is the growing call for regulation both at home and around the world. Regulation to intentionally weaken the U.S. technology industry will make it that much more difficult for the techno-democracies to maintain an advantage in the long-term race for technological supremacy – especially since Chinese competitors face no such obstacles from their government. Ongoing debate surrounding updating privacy and data laws should not distract from the mission shared by techno-democracies and their private sector partners to promote technologies abroad that reflect democratic principles.

Conclusion

In the spring of 2020, President Biden wrote in a piece for *Foreign Affairs* stating that "to win the competition for the future against China or anyone else, the United States must sharpen its innovative edge and unite the economic might of democracies around the world".[23] This reflects an understanding that the work of promoting U.S. digital power must be done in the broader context of working with our allies and the private sector, and that if the U.S. does not model and enforce an innovative digital framework, it risks losing its edge to techno-autocracies.

[21] Thompson, Loren B. "Why U.S. National Security Requires a Robust, Innovative Technology Sector." *Lexington Institute,* October 2020, https://www.lexingtoninstitute.org/wp-content/uploads/2020/10/100820-WHY-U.S.-NATIONAL-SECURITY-REQUIRES-A-ROBUST-INNOVATIVE-TECHNOLOGY-SECTOR-002.pdf.

[22] Fried, Ina. "Why Intel's troubles should concern us all." *Axios*, 1 Feb. 2021, https://www.axios.com/intel-outsourcing-chip-manufacturing-competitiveness-f6fb76e6-ee15-4409-8f45-704d4b137ec2.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top.

[23] Biden, Joseph R. "Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump." *Foreign Affairs*, March/April 2020, https://www.foreignaffairs.com/print/node/1125464.

President Biden has no shortage of emergencies that will consume his first months as president. But within his first year in office, the president should issue a national framework for U.S. technology policy with a focus on national security. The goal of policy should be to identify and prioritize ways the U.S. can maintain a long-term advantage in existing and emerging technologies against threats posed by nations like Russia, China, Iran, and North Korea. The framework will require collaboration across the federal government, and in partnership with the private sector, especially on data protection and cybersecurity issues.

The Biden Administration should work closely with like-minded allies like the EU, our Five Eyes partners, and Japan to ensure techno-democracies collectively support the democratic principles inherent in a U.S. digital framework. Any grievances with individual technology companies should not distract from the broader goal of uniting against techno-autocracies seeking to export a more closed and censored internet model. Strategic trade agreements present one such opportunity to advance national security goals, including digital standards or protected data transfers.

A U.S. technology framework should also explore proportionate responses to cyber threats. The phrase "Big Tech" is often used derisively, but the advantages of being a larger company is having more resources to defend against cyberattacks and other digital threats, as well as to proactively develop products that help all industries defend themselves. However, no matter how big "Big Tech" is, it's no match against the full power of aggressive nation-states. While industry can support governments in helping to detect and prevent cyber threats, the response to successful attacks fall to the federal government. One way to deter particularly damaging cyber operations is to ensure nation states such as Russia and Iran are made aware that the U.S. is prepared to respond to cyberattacks as it would respond to traditional military threats, including with targeted sanctions. If done in coordination with other techno-democracies, a digital framework would be a means to formalize that, for example, an attack on one country's national election is not just an attack on that specific country, but an attack on core democratic systems. In a digital world, this sort of attack is far more likely than traditional military action, and yet there is no official framework outlining how techno-democracies could collectively deter such actions through the threat of a unified response.

The Chinese government has already made it clear in its 5 Year Plan (5YP) that technological independence and self-reliance will be cornerstones of its development strategy. Therefore, it will be just as important for the Biden Administration to develop its own clear strategy for protecting America's technological edge. The Biden Administration should engage with a bipartisan coalition in Congress on this framework, especially given the bipartisan consensus on the rising threat of China.

Concurrently, the Biden Administration should follow through with its campaign promise that R&D investments will be the "cornerstone" of his presidency.[24] As part of his "Made in All of America" plan

[24] Biden, Joseph R. "Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump." *Foreign Affairs,* March/April 2020, https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again.

during the campaign, President Biden pledged a new $300 billion investment into R&D and breakthrough technologies.[25] The Biden Administration should continue to work with Congress on ensuring funding is available for rural carriers to replace existing Chinese 4G and 3G infrastructure, which would pave the way for installation of U.S.-designed 5G infrastructure. The Biden Administration should also ensure full funding for legislation, such as the USA Telecommunications Act. These bills seek to spur investment in U.S. companies for 5G deployment in the United States as well as a multilateral fund, which provides grants to our allies in more developing nations to help support their buildout using trusted vendor equipment.

Over the last several generations, technology innovation has driven productivity, invented millions of new jobs, and made the United States the wealthiest nation in the world. As the nation continues to fight a global pandemic, the technology industry remains a consistent growth area for the U.S. economy and the job market. It also offers services to maintain regular order in the short-term and a path to thrive as a nation in the decades ahead. Policies that forfeit the U.S. competitive edge to foreign entities put the safety, privacy, and economic prosperity of Americans at risk. A smart regulatory and policy approach is needed both at home and abroad, but the stakes are too high to adopt practices that unnecessarily hamper a U.S. industry so intertwined with the future of American prosperity and security.

###

[25] https://joebiden.com/made-in-america/

The national security policy framework was published by the American Edge Project along with the following contributing authors:

- **Admiral James Stavridis**, USN (Ret.) former Supreme Allied Commander at the North Atlantic Treaty Organization (NATO), commander of U.S. Southern Command and American Edge Project National Security Advisory Board Co-Chair
- **Frances Townsend**, former White House Counterterrorism and Homeland Security Advisor and American Edge Project National Security Advisory Board Co-Chair
- **Michael Allen**, managing director, Beacon Global Strategies
- **Jeremy Bash**, founder and managing director, Beacon Global Strategies
- **Kaitlyn Garman,** senior associate, Beacon Global Strategies
- **Jamil Jaffer**, founder and executive director, National Security Institute
- **Stephen Rodriguez**, founder, One Defense