THE REAL COST OF 5G TECHNOLOGY: NATIONAL SECURITY IMPLICATIONS OF 5G IMPLEMENTATION AND IMPACT ON THE U.S.-CHINA RELATIONSHIP

Melissa L. Ken*

The development of 5G technology is one of the most important cybersecurity concerns facing the United States today. In order to combat this threat, the U.S. government must unify its domestic cyber-response efforts and increase its presence on the international stage in regard to this issue. This Article proposes specific domestic and international action plans to tackle the challenges presented by 5G. The most important proposals take steps to remedy the tensions between the United States and China by opening the Budapest Convention membership protocol as well as unifying the U.S. domestic cyber response and objectifying the U.S. digital supply chain standards rather than targeting specific entities. These steps will allow the United States to impose rigorous standards to protect American national security interests without increasing already high tensions with China.

*Major Melissa L. Ken, Judge Advocate General's Corps, U.S. Air Force; Assistant Professor at the United States Air Force Academy. The opinions and assertions expressed in this Article are those of the author and do not necessarily reflect the official policy or position of the United States Government, the Department of Defense, or the Department of the Air Force.

I. INTRODUCTION

On December 23, 2015, more than 200,000 Ukrainian citizens lost power in their homes and businesses.[1] Power was disconnected for about three hours. The source of the outage? Russian hackers, suspected to be backed by the Russian government itself.[2] Investigations determined that three electrical distribution control centers were remotely accessed and hackers proceeded to open breakers at approximately thirty distribution substations resulting in the loss of power.[3] This attack on Ukraine represents a growing threat to national critical infrastructure from cyberspace.[4] With the advent of Fifth Generation ("5G") technology, experts worry that the number ofcyberattacks and the threat to critical infrastructure will increase.[5] This new 5G technology represents the promise of faster data speeds, lower latency, and the ability to connect more devices at once than previous generations of technology.[6] However, a greater number of connections equals a greater number of entry points for malicious actors, particularly if those actors have the advantage of a built-in backdoor.[7]

---

[1] Donghui Park & Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power GridAttacks*, THE HENRY M. JACKSON SCH. OF INT'L STUD. (Oct. 11, 2017), https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

[2] *Compromise of a Power Grid in Eastern Ukraine*, COUNCIL ON FOREIGN RELS. (Dec. 2015), www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

[3] Park & Walstrom, *supra* note 1.

[4] *Id.* Vulnerabilities in networks and communication systems are fairly easy to exploit as there are minimal international norms and laws to address hacking and investigators are rarely able to track down specific individuals or even nations responsible for an attack. *Id.*

[5] Matthew Wall, *5G: 'A Cyber-Attack Could Stop the Country'*, BBC (Oct. 25, 2018), www.bbc.com/news/business-45952693.

[6] Sascha Segan, *What is 5?*, PC MAG. (Jan. 20, 2022), www.pcmag.com/news/what-is-5g.

[7] *Backdoor Computing Attacks*, MALWAREBYTES, www.malwarebytes.com/backdoor (last visited Mar. 12, 2021) ("A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access…Backdoors can be installed by software or hardware makers as a deliberate means of gaining access to their technology after the fact.").

Chinese companies, namely Huawei, control at least thirty-six percent of all 5G standard-essential patents, putting them firmly in control of 5G technology and requiring other nations to pay licensing fees or purchase equipment from Chinese manufacturers.[8] This high level of control over technology and manufacturing has raised serious national security concerns regarding the use of 5G technology. U.S. intelligence officials believe that Huawei built backdoors into their 5G hardware so it could obtain data from the networks they build and maintain.[9] This data could easily be shared with the Chinese government, especially given China's National Intelligence Law.[10]

This 5G technology represents an increased threat to U.S. national security and leaves the United States playing catch-up with Chinese technology and influence in the 5G development. The attempts to catch up to China have revealed several weaknesses in U.S. domestic structure regarding cybersecurity and technological developments.[11] The development of 5G has also exacerbated existing deficiencies in the international legal structure regarding cybercrime.[12]

In order to combat the security threats presented by 5G and ensure that the United States and its allies have an increased capacity to handle future technological developments, the United States must champion reforms to both international and domestic law and policy. On the international level,the United States must spearhead reforms to the Budapest Convention, the only international treaty regarding cybercrime. These reforms include amending the Convention's

[8] Dan Strumpf, *Where China Dominates in 5G Technology*, WALL ST. J. (Feb. 26, 2019),www.wsj.com/articles/where-china-dominates-in-5g-technology-11551236701.

[9] Julian E. Barnes, *White House Official Says Huawei Has Secret Back Door to Extract Data*, N.Y. TIMES, (Feb. 11,2020), www.nytimes.com/2020/02/11/us/politics/white-house-huawei-back-door.html.

[10] Arjun Kharpal, *Huawei says it Would Never Hand Data to China's Government: Experts Say it Wouldn't Have aChoice*, CNBC (Mar. 5, 2019), www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

[11] Tom Wheeler & David Simpson, *Why 5G Requires New Approaches to Cybersecurity,* BROOKINGS (Sept. 3, 2019), www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

[12] *Id.*

membership protocol to make it more inclusive and delaying the proposed additional protocol due to its overly broad information-sharing scheme. Also, the United States should increase its influence and participation in standard-setting organizations like the Third Generation Partnership Project ("3GPP") consortium and the International Telecommunications Union ("ITU").

On a domestic level, the United States must unify its domestic structure and response to cybercrime. The best way to achieve this unification is to utilize the existing Cybersecurity and Infrastructure Security Agency ("CISA") to streamline and simplify the nation's response to cyber incidents. This Article argues that creating a new National Cyber Director ("NCD") position is premature and could cause additional confusion. Instead, CISA should identify and remedy redundancies before Congress creates yet another new cyber-related position. Additionally, the United States must secure increased participation of private industry in combating cyber threats. This can be accomplished through mandatory reporting of data breaches and tax incentives to encourage corporations to adhere to existing federal standards of cyber hygiene and protection. Finally, the United States should secure and diversify its international digital supply chain through international programs such as the Blue Dot Network. This practice of setting objective standards will help alleviate international tensions, specifically with China, while still allowing the United States to protect its national security interests through rigorous quality control requirements.

Section II of this Article lays out the background of the 5G situation, including threats posed by 5G and China's growing influence in the developing technology as well as the currentdomestic and international response to cyber threats. Section II also describes the basic framework of China's perceptions of cyberspace. The concepts of cyber sovereignty and mutual strategic trust are particularly important to China's operations in this field.

Section III addresses the challenges presented by current and future technological developments through the lens of international and domestic reforms. The proposed international reforms focus on amendments to the Budapest Convention and the pending Additional

Protocol. Section III also addresses the importance of standard-setting organizations and the importance of U.S. participation in those organizations. In regard to domestic reforms, this Article proposes changes to the U.S. cyber-response structure, targets improvements to the cybersecurity of private business in the United States, and proposes an objective, standards-based regulation of the digital supply chain.

II. BACKGROUND

This section provides an overview of the issues presented by 5G implementation and current responses. Subsection A provides background information on the threats of 5G implementation, including China's growing influence in the area as well as domestic risk management and supply chain security concerns. Subsection B discusses the current status of the major cyber responses from both an international and domestic perspective. Finally, Subsection C provides a brief explanation of China's perceptions of cyberspace, namely the concepts of cyber sovereignty and mutual strategic trust, and a brief overview of previous dialogues between the United States and China regarding cyberspace.

A. Threats of 5G Implementation

With the development and rollout of any new technology, there are challenges presented by the security of that technology and its implementation in society, the economy, and government. Roughly every ten years, tech companies develop and release the next generation ofmobile communication and technology.[13] The 3GPP is a consortium made up of seven separate international telecommunication standard-setting organizations that develop consensus-based technical specifications for wireless and networking technology, including 5G, to ensure global interoperability.[14] These

[13] *Feature Article: 5G Introduces New Benefits, Cybersecurity Risk*, DEP'T OF HOMELAND SEC. (Oct. 15, 2020), www.dhs.gov/science-and-technology/news/2020/10/15/feature-article-5g-introduces-new-benefits-cybersecurity-risks [hereinafter *Feature Article*].

[14] Guang Yang, *Who Are the Leading Players in 5G Standardization? An Assessment for 3GPP 5G Activities*, STRATEGY ANALYTICS (Mar. 16, 2020),

technical specifications are distributed through 3GPP Releases.[15] All 5G related specifications are contained in Release 15 and subsequent Releases.[16] Release 15, known as 5G Phase 1, was published in June 2019.[17]

Release 15 addressed several technical components of the 5G systems, including machine type communication ("MTC") and the Internet of Things ("IoT").[18] Specifications for MTC are extremely important as they allow devices to communicate and exchange information without human operation.[19] This MTC technology is the primary basis for self-driving cars and other automated machines.[20] The IoT is "basically connecting any device with an on and off switch to the Internet."[21] This technology enables users to control their thermostat, coffee maker, and other household devices from their

www.strategyanalytics.com/access-services/service-providers/networks-and-service-platforms/reports/report-detail/who-are-the-leading-players-in-5g-standardization-an-assessment-for-3gpp-5g-activities.

[15] *Releases*, 3GPP, www.3gpp.org/specifications/releases.

[16] *5G Evolution Across Three Major Releases*, 3GPP, www.3gpp.org/ftp/Information/presentations/presentations_2020/Poster_2020_MWC_v6_OPTIMIZED.pdf [hereinafter *Evolution Across Releases*].

[17] Although the first Release regarding 5G came in 2019, 5G technology has already been on a long evolutionary path starting as early as 2008 when the National Aeronautics and Space Administration helped launch the Machine-to-Machine Intelligence (M2Mi) Corp. *See* Bob O'Donnell, *The Evolution of 5G*, FORBES (Nov. 12, 2019), www.forbes.com/sites/bobodonnell/2019/11/12/the-evolution-of-5g/?sh=58b6cb2c278e; *see also* Michael Curie et al., *NASA Ames Partners with M2MI for Small Satellite Development*, NAT'L AERONAUTICS & SPACE ADMIN. (Apr. 24, 2008), www.nasa.gov/home/hqnews/2008/apr/HQ_08107_Ames_nanosat.html.

[18] *Evolution Across Releases*, *supra* note 16.

[19] Nurul Huda Mahmood et. al., *Machine Type Communications: Key Drivers and Enablers Towards the 6G Era*, SPRINGER OPEN (June 10, 2021), https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-021-02010-5. For more information regarding MTC, *see generally* Joachim Sachs et al., *Machine-Type Communication*, *in* 5GMOBILE AND WIRELESS COMMUNICATIONS TECHNOLOGY 77, 77-106 (Afif Osseiran et al. eds., 2016).

[20] Geoff Brown, *Machine-to-Machine Intelligence (M2Mi) Corp.*, NAT'L AERONAUTICS & SPACE ADMIN. (Sept. 14,2011), www.nasa.gov/centers/ames/researchpark/partners/industry/m2mi/.

[21] Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014), www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=5a4c73161d09.

cellphone.[22] These mobile IoT connections are growing at an incredible rate, and standards for this technology form the foundation of 5G development.[23]

Currently, 3GPP is working on Release 17 with Phase 2 of that Release frozen in mid-2021.[24] The Release 17 schedule was expanded allowing for maintenance and adjustment to previous release standards and specifications to increase the stability of the new technology.[25] Some aspects of Release 17 include determining specifications for satellite components in the 5G architecture and enhancing 5G location services.[26] The first package of Release 18, containing basics of Phase 4 of 5G technology, was released at the end of 2021.[27]

However, with the rollout of 5G technology, the United States faces challenges and security vulnerabilities on an unprecedented scale.[28] The abovementioned interconnectedness, i.e., the IoT, inherent in 5G utilization, results in a greater need for encryption and security of data as it flows from one point to another, but it presents other vulnerabilities as well. The Department of Homeland Security ("DHS") identified four discrete areas of risk and vulnerability related to developing 5G technology, which include the supply chain, 5G deployment, network security, and competition and choice.[29] The

[22] *Id.*

[23] Mobile Machine-to-Machine (M2M) connections are predicted to grow from 1.2 billion in 2018 to 4.4. billion by2023. Cisco, CISCO ANN. REP. (2018-2023) 12 (2020), www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

[24] "After freezing, a Release can have no further additional functions added. However…a considerable number ofrefinements and corrections can be expected for at least two years following this date." *Releases*, *supra* note 15; *Release* 17, 3GPP, www.3gpp.org/release-17.

[25] *Release 17 Timeline Agreed*, 3GPP (Dec. 14, 2020), www.3gpp.org/news-events/2145-rel-17_newtimeline.

[26] *Id.*

[27] *Release* 17, *supra* note 24.

[28] Shane Fonyi, *Overview of 5G Security and Vulnerabilities*, 5 CYBER DEF. REV. 117, 122-23 (2020).

[29] The issues with supply chain as well as competition and choice (interoperability and standards development) arediscussed more in depth later in this paper. 5G

deployment of 5G presents new obstacles as the 5G spectrum requires more base stations than previous generation technology.[30] Because 5G utilizes the full spectrum of radio frequencies, 5G signals do not carry as far as their 4G predecessors, especially in cities.[31] This will require the deployment of more networks and base stations, which increases the risk of manipulation and disruption of that equipment.[32]

Threats to network security of 5G networks create a greater need for defenses and comprehensive standards to prevent cyberattacks. There are three primary known vulnerabilitiesin 5G standards, which organizations, like 3GPP, are attempting to mitigate through their standardsetting process. The three security principles are confidentiality, integrity, and availability.[33] Each principle is vulnerable to different types of known threats and cyberattacks used to target previous generations of technology.[34] For example, in the area of confidentiality, 5G systems have demonstrated vulnerabilities to Authentication and Key Agreement attacks, which allow hackers to determine a subject's location and activities by establishing a fake base station that the subject's device uses to access the 5G network.[35] This

deployment and network security are briefly addressed in this background section. *Feature Article*, *supra* note 13.

[30] O'Donnell, *supra* note 17.

[31] Previous 4G signals technology utilized the low end of the radio spectrum. Waves at that level are able to pass through most materials and travel long distances resulting in the use of large cellular towers to cover large geographic areas. Since 5G uses the whole spectrum, 5G equipment must carry high frequency signals which improve speed, but have a much lower ability to penetrate walls and other materials like 4G spectrum requirementsresulting in the need for a greater number of smaller cellular base stations covering less area. CISA, OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES 3 (2019), www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

[32] *Feature Article*, *supra* note 13.

[33] Confidentiality requires that sensitive data not be released to unauthorized parties. Integrity ensures that data maintains its accuracy and consistency from end point to end point without being manipulated by environmental factors or malicious actors. Availability indicates that all information systems will be functional and accessible at alltimes. Fonyi, *supra* note 28, at 126-28.

[34] *Id.* at 125-29 (describing further details on different vulnerabilities and types of attacks).

[35] *Id.* at 127.

type of attack obviously compromises the subject's privacy and could be used to disastrous effect if employed by an enemy against any ongoing military and covert operations.

Another, more familiar, type of cyberattack is known as a distributed denial of service attack ("DDOS"). A DDOS attack is when cyber attackers make it impossible for a network service to be delivered by preventing access to services, devices, applications, and transactions.[36] These attacks are typically conducted by overwhelming and crashing a server with requests for data or services.[37] In October 2016, Mirai botnet used a DDOS attack on an internet infrastructure service provider to infect more than 100,000 IoT devices and disrupted services like Amazon, Netflix, and Twitter.[38] While this type of attack was fairly common on previous generation systems, the increased use of botnets as well as the nature of 5G and the IoT will make DDOS attacks "much more devasting and potentially easier to orchestrate."[39]

In addition to the technological risks, 5G poses risks to U.S. national security and has already altered the United States' relationships and interactions with foreign nations such as China. China has a vested interest in the future of 5G, which has put it at odds with the United States and several of U.S. allies. This tension largely stems from the U.S. ban on the Chinese company Huawei, which has heavily invested in 5G infrastructure and technology around the globe.[40]

As explored below, Chinese companies have played a greater role in international standard-setting organizations and have

[36] Josh Fruhlinger, *DDoS Explained: How Distributed Denial of Service Attacks are Evolving*, CSO ONLINE (Feb.12, 2021), www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html.

[37] DDOS attacks can also occur through protocol or network-layer attacks as well as application-layer attacks. *Id.*

[38] *DDos Attack That Disrupted Internet was Largest of Its Kind in History, Experts Say,* THE GUARDIAN, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, (last visited Mar. 1, 2022)

[39] Fonyi, *supra* note 28, at 129.

[40] Sean Keane, *Huawei Ban Timeline: Chinese Company's CFO to Testify in Extradition Case*, CNET (Oct. 27,2020), www.cnet.com/news/huawei-cfo-trial-begins-in-canada/.

increased their influence in the development of this newtechnology. Additionally, China's National Intelligence Law has raised questions regarding Huawei's ability to provide secure 5G to its customers. On the domestic side of the 5G rollout, the United States has promulgated legislature and executive orders regarding 5G, particularly focusing on risk management and securing the digital supply chain.

1. China's Growing Influence

Huawei is a major Chinese tech company and has been a prominent player in the global market for years. The company was founded in 1987 and operates in more than 170 countries.[41] According to its website, Huawei's "mission is to bring digital to every person, home and organization for a fully connected, intelligent world."[42] Huawei's products are utilized around the globe, and the company is the second-largest smartphone supplier,[43] although the products are "virtually invisible" in the United States.[44] Huawei has been involved in building both the global 3G and 4G networks.[45]

In 2009, Huawei was still virtually unknown outside of China; however, the Swedish phone company TeliaSonera employed Huawei to build its 4G network in Oslo, Norway.[46] Huawei's successful completion of this contract led to other contracting opportunities in Europe, which put Huawei on an upward trajectory in global

[41] *Our Company*, HUAWEI, www.huawei.com/us/corporate-information (last visited Jan. 7, 2021).
[42] *Id.*
[43] Tim Bowler, *Huawei: Why Is It being Banned from the UK's 5G Network?* BBC (July 14, 2020),www.bbc.com/news/newsbeat-47041341.
[44] Sean Keane, *Huawei Ban Timeline: Detained CFO Makes Deal with US Justice Department,* CNET (Sept. 30, 2021), www.cnet.com/tech/services-and-software/huawei-ban-timeline-detained-cfo-makes-deal-with-us-justice-department/.
[45] Nawied Jabarkhyl, *We Abide by Laws of 170 Countries: Huawei tells UK it can be Trusted with 5G Network*, CGTN (June 9, 2020), newseu.cgtn.com/news/2020-06-09/-We-abide-by-laws-of-170-countries-Huawei-makes-its-case-for-UK-s-5G-Ra6mf33RrG/index.html.
[46] Keith Johnson & Elias Groll, *The Improbable Rise of Huawei,* FOREIGN POL'Y (Apr. 3, 2019), foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.

technological infrastructure.[47] Despite anearly reputation for cheap hardware, Huawei engaged in its own research and development to create reliable equipment available at low prices.[48] Due to the growing strength of Huawei, coupled with Ericsson and Nokia's dominance in the wireless networking industry, U.S. companies were absorbed by foreign counterparts and the industry collapsed in the United States.[49] Instead, U.S. companies focused on developing the software to accompany the infrastructure and hardware developed by others.[50]

Huawei's influence continued to grow due to those early contracts in Europe and support from the Chinese government. While Huawei denies receiving direct state aid, the Chinese government was Huawei's first customer, and it is undeniable that Chinese policy protected Huawei from foreign competition within China.[51] These protections at home enabled Huawei to grow domestically and put it in a favorable position to expand overseas, which it did in 2009. Huawei's founder and CEO, Ren Zhengfei, admitted that without China's policy of protecting nationally owned companies, "Huawei would no longer exist."[52]

Naturally, Huawei is attempting to continue and increase its influence with the 5G rollout. The company has already signed more than forty commercial 5G contracts with nations around the world, including countries in Europe, the Middle East, and Asia.[53] Huawei

---

[47] *Id.*

[48] Brian Fung, *How China's Huawei Took the Lead Over U.S. Companies in 5G Technology,* WASH. POST (Apr. 10, 2019), www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/.

[49] At the beginning of the wireless age, U.S. companies, like Motorola and Lucent, attempted to dominate the wireless networking industry. It became difficult for these companies to keep up with their European counterpartsdue to the common European standard for wireless communication that did not exist in North America. This common standard gave European companies like Nokia a larger market and enabled them to take primacy in the wireless networking market. *Id.*

[50] Scott Andes & Mark Muro, *Software: America's Hidden Manufacturing Advantage*, BROOKINGS (Feb. 25, 2014), www.brookings.edu/blog/the-avenue/2014/02/25/software-americas-hidden-manufacturing- advantage/.

[51] Johnson & Groll, *supra* note 46.

[52] *Id.*

[53] Reality Check Team, *Huawei: Which Countries are Block its 5G Technology?*, BBC (May 18, 2019), www.bbc.com/news/world-48309132.

has also pointed its massive research and development capabilities toward 5G technology, resulting in Huawei and other Chinese companies owning thirty-six percent of all 5G standard-essential patents compared to U.S. company Qualcomm's fourteen percent share of 5G patents.[54] However, Huawei has come under international scrutiny for its perceived legal obligations under China's recently passed National Intelligence Law. The backlash from this law caused several nations to ban, or severely limit, Huawei's role in their 5G rollout.[55]

a. China's National Intelligence Law

In 2017, China's National Intelligence Law passed as part of a larger legislative plan to revitalize and strengthen China's national security.[56] Article 7 of the National Intelligence Law requires that "all organizations and citizens shall support, assist and cooperate with national intelligence efforts . . . and shall protect national intelligence work secrets they are aware of."[57] Article 8 states that intelligence efforts pursuant to this law "shall respect and protect human rights, and shall preserve the lawful rights and interests of individualsand organizations."[58]

---

[54] "The Chinese 5G patents cover technology associated with everything from 5G handset componentry to base stations and driverless-car technology." This number of patents is more than double the number of comparable 4Gpatents controlled by Chinese companies. Strumpf, *supra* note 8.

[55] Nations that have banned Huawei technology include the United States, Australia, and the United Kingdom. Othernations that have cancelled Huawei contracts or chosen competitors include Italy and New Zealand. *See The Definitive List of Where Every Country Stands on Huawei*, NS TECH (July 29, 2020), www.offshore-technology.com/tech/the-definitive-list-of-where-every-country-stands-on-huawei/.

[56] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017), www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[57] Guójiā Qíngbào Fǎ (国家情报法) [National Intelligence Law] (promulgated by the Standing Comm. Nat'lPeople's Cong., June 27, 2017), ch. 1, art. 8, *translated in* www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/ (last visited Apr. 14, 2021).

[58] *Id.* at ch. I, art. 8.

The text of this law raises concerns that Chinese companies, such as Huawei, are requiredto assist the Chinese government in their intelligence gathering operations.[59] Given the amount of access Huawei has to the 5G network and technology, the United States and other nations areconcerned that Huawei will be required to use its 5G access to provide intelligence to China in accordance with the National Intelligence Law.[60] Theoretically, China could have access to all 5G communications involving Huawei technology.

Huawei and China's government have both repeatedly asserted that Huawei's overseas components are not required to assist with intelligence gathering.[61] They argue that this position is supported by Article 8 of the National Intelligence Law, which preserves the lawful rights and interests of organizations. Huawei CEO Ren stated that his company will "never participate in espionage, and . . . we absolutely never install backdoors. Even if we were required by Chinese law, we would firmly reject that."[62]

Despite these assurances, the United States has called for a global ban on Huawei technology.[63] To this end, the United States has added Huawei to its Entity List.[64] The Entity List is published by the Department of Commerce, Bureau of Industry and Security. The Entity List is comprised of foreign persons, businesses, and organizations that are "subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items."[65] The original purpose of the Entity list was "to inform the public of entities

[59] Kharpal, *supra* note 10.
[60] *Id.*
[61] Yuan Ying, *Is Huawei Compelled by Chinese Law to Help with Espionage?*, FIN. TIMES (Mar. 4, 2019),www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0.
[62] Kharpal, *supra* note 10.
[63] Justin Sherman, *Is the U.S. Winning Its Campaign Against Huawei?*, LAWFARE (Aug. 12, 2020),www.lawfareblog.com/us-winning-its-campaign-against-huawei.
[64] Huawei has been placed on the Entity List, not due to cybersecurity issues related to 5G, but because of Huawei'sindictment for violating export laws regarding trade with Iran. Addition of Entities to the Entity List, 84 Fed. Reg. 22, 961 (May 21, 2019) (codified at 15 C.F.R. Pt. 740) [hereinafter Addition to Entity List].
[65] Entity List, BUREAU OF INDUS. & SEC., www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list (last visited Jan. 7, 2021).

who have engaged in activities that could result in an increased risk of the diversion . . . [of] items to weapons of mass destruction programs . . . [but has] expanded to activities . . . contrary to U.S. national security and/or foreign policy interests."[66] However, placing Huawei (and other Chinese technology companies) on the Entity List resulted in unintended consequences for the development of global 5G standards, including limiting U.S. companies' abilities to participate in international standard-setting organizations.

b. International Standard Setting Organizations

Standard-setting organizations ensure "interoperability between networks and devices."[67] The success of these organizations is evidenced in the deployment of the world's 4G network, which allows consumers to utilize their devices almost anywhere in the world.[68] For the purposes of 5G development, the most important standard-setting organizations are 3GPP and the ITU. There are more than 600 member-organizations in 3GPP working together to establish consensus-based, unified technical specifications for services and networking 5G systems.[69] The ITU is an agency of the United Nations ("UN"), which allocates global radio spectrum and satellite orbits while also developing technical standards to ensure networks and technologies can interconnect.[70]

These two standard-setting organizations each play a critical role in the interoperability and development of 5G technology. The ITU attempts to ensure that all nations allocate the same spectrum range for 5G while 3GPP establishes technical specifications on every 5G system from network access security, core network functions, and

---

[66] *Id.*

[67] *5G Policy Primer: The Global Standards Process is Robust and Effective in Advancing U.S. Goals*, AT&T (Jan.2020), policyforum.att.com/wp-content/uploads/2020/08/5G-Standards-Whitepaper-March-2020.pdf [hereinafter AT&T Policy Primer].

[68] *Id.*

[69] Yang, *supra* note 14.

[70] *About International Telecommunication Union (ITU)*, ITU, www.itu.int/en/about/Pages/default.aspx (lastvisited Jan. 9, 2021).

satellite components in the5G architecture.[71] One important example of a 3GPP specification involves channel coding. Channel coding mitigates the effect of errors in a communication link caused by interference or device impairments.[72] Huawei developed a novel method for correcting these errors called polar coding, patented the technology, and submitted it to 3GPP to become the standard for 5G systems. In 2016, 3GPP adopted Huawei's polar coding as standard for 5G, thus giving Huawei ownership over a critical 5G technology.[73]

This type of patent control and setting of technical standards is critical to China's efforts to control the future of 5G.[74] "When you invest like that in the standardization process . . . you end upseeing a significant portion of the essential intellectual property being in your hands."[75] As a privately owned company, Huawei is not required to disclose licensing revenue; however, Qualcomm, an important U.S. semiconductor company, reported that it generated more than twenty percent of its total income from licensing fees in 2018.[76] Thus, setting global standards through 3GPP and other organizations results in control over that technology and a higher market share of 5G.[77]

China has already taken large steps and increased their influence in organizations like 3GPP. Thus, it is essential that U.S. companies, like Intel and Qualcomm, the only two U.S. companies who currently regularly contribute to 3GPP, continue and increase their efforts to contribute to standard-setting by increasing their own

[71] For a more robust list of 3GPP standards, *see* Evolution Across Releases, *supra* note 16; *see also* Janne Peisa et al., *5G Evolution: 3GPP Releases 16 & 17 Overview*, ERICSSON TECH. REV. (Feb. 2020), available at www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-nr-evolution.
[72] Alan Carlton, *How Polar Codes Work*, COMPUTERWORLD (Sept. 28, 2018), www.computerworld.com/article/3228804/how-polar-codes-work.html.
[73] Josh Chin et al., *The 5G Race: China and U.S. Battle to Control World's Fastest Wireless Internet*, WALL ST. J.(Sept. 9, 2018), www.wsj.com/articles/the-5g-race-china-and-u-s-battle-to-control-worlds-fastest-wireless-internet-1536516373.
[74] "China's bid to steer the 5G future depends heavily on setting technical standards the rest of the world will have tofollow – and pay royalties and licensing fees to use. It has played an aggressive role in the international telecom industry collective that sets global standards." *Id.*
[75] Strumpf, *supra* note 8.
[76] *Id.*
[77] Johnson & Groll, *supra* note 46.

research and development programs.[78] Without U.S. influence in 3GPP, these international standards will continue to favor Chinese technology and intellectual property resulting in U.S. dependence on those Chinese companies to maintain globally interoperable technology. Dominance in 5G technology will also lead to dominance in 6G, 7G, and even 8G, or at least a significant head start.[79]

As previously mentioned, the U.S. Department of Commerce placed Huawei and its affiliates on the Entity List.[80] This action had the intended consequence of severely restrictingHuawei's operations, but it also had the unintended consequence of preventing U.S. companies from engaging in standard-setting organizations, such as 3GPP. In order for companies to meaningfully participate in 3GPP, companies must be able to share limited portions of their technology, which enables 3GPP to write the technical specifications allowing networks and devices to communicate.[81]

After Huawei's inclusion on the Entity List, U.S. companies feared that sharing information during a 3GPP meeting would cause them to violate federal export control laws as they would be sharing U.S. technology with a company without an export license.[82] As such, many U.S. companies stopped contributing to 3GPP and requested clarification from the federal government regarding Huawei's designation and its consequences.[83] The Department of Commerce amended the applicable sections of the Export Administration Regulations (EAR) to specifically authorize U.S. companies to release information to Huawei, despite the lack of a license, if the release is "made for the purpose of contributing to the revision or development

[78] *Id.*
[79] Chin et al., *supra* note 73.
[80] Addition to Entity List, *supra* note 64.
[81] Ari Schwartz, *Standards Bodies are Under Friendly Fire in the War on Huawei*, LAWFARE (May 5, 2020),www.lawfareblog.com/standards-bodies-are-under-friendly-fire-war-huawei.
[82] *Id.*
[83] Yixiang Xu, *O-Ran, 3GPP, and R&D Fund: The U.S. May Finally Have a Winning Strategy for the 5GCompetition*, AM. INST. FOR CONTEMP. GERMAN STUD. (May 7, 2020), www.aicgs.org/2020/05/o-ran-3gpp-and-rd-fund-the-u-s-may-finally-have-a-winning-strategy-for-the-5g-competition/.

of a 'standard' in a 'standards organization.'"[84] However, it took approximately thirteen months for the Department of Commerce to amend the EAR to allow U.S. companies to participate in standard-setting organizations.

China is a leading participant in international standards regarding 5G technology.[85] In 2019, China submitted the most technical documents to the ITU wired communications specifications commission, which constituted a larger contribution than the next three contributors combined.[86] Additionally, since December 2016, Huawei submitted more than 6,000 of the almost 30,000 5G-related proposals received by 3GPP.[87] The combination of China working with the ITU and Huawei's influence in 3GPP creates a very real threat that China's domestic standards will become international standards, thus allowing China to dominate the global 5G market.[88]

2. Domestic Risk Management and Supply Chain Security

Risk management standards form the foundation of 5G infrastructure and hardware. While the future of "5G is the conversion to a mostly all-software network," the immediate concern lies in the potential vulnerabilities of the hardware and infrastructure.[89] The future of 5G (and even 6G) depends on the reliability and security of infrastructure decisions regarding the acquisition and deployment of 5G technologies that are being made right now. Attempting to secure and reaffirm its traditional position as the global technological leader, the United States promulgated several pieces of legislation and executive action regarding 5G. In March 2020, then-President Donald Trump issued the National Strategy to Secure 5G, which constitutes a culmination of most of the United States' efforts to create a cohesive

[84] Release of "Technology" to Certain Entities on the Entity List in the Context of Standards Organizations, 85 Fed.Reg. 36, 719 (June 18, 2020) (codified at 15 C.F.R. Pt. 744, 772).
[85] Hideaki Ryugen & Hiroyuki Akiyama, *China Leads the Way on Global Standards for 5G and Beyond*, FIN. TIMES(Aug. 4, 2020), www.ft.com/content/858d81bd-c42c-404d-b30d-0be32a097f1c.
[86] Those contributors are South Korea, the United States, and Japan. *Id.*
[87] Yang, *supra* note 14.
[88] Ryugen & Akiyama, *supra* note 85.
[89] Wheeler & Simpson, *supra* note 11.

plan regarding 5G deployment and security.[90] The National Strategy to Secure 5G targets four main components of America's 5G plan. The components are (1) facilitating a domestic 5G rollout; (2) assessing risks to 5G infrastructure; (3) addressing those identified risks; and (4) promoting responsible global development and deployment.[91] The Strategy relies on inter-agency cooperation and private sector cooperation to identify risks to the 5G infrastructure.[92] To address those risks, the Strategy relies heavily on the Federal Acquisition Security Council ("FASC") and the authority granted by Executive Order 13873 on Securing the Information and Communications Technology and Services Supply Chain.[93]

In December 2018, Congress passed the Strengthening and Enhancing Cyber-capabilitiesby Utilizing Risk Exposure ("SECURE") Technology Act.[94] The most important provision of theSECURE Technology Act is Title II, known as the Federal Acquisition Supply Chain Security Act.[95] This provision established the FASC to identify and recommend supply chain risk management standards, guidelines, and practices for executive agencies.[96] Essentially, the FASC can control which technologies are used by the federal government to ensure government computer system security. However, the Office of Management and Budget only recently published its interim final rule governing the FASC's procedures and processes.[97] It is important to note that non-federal, U.S. entities are not required to share supply chain risk information with the FASC.

On May 15, 2019, then-President Trump issued an Executive Order to secure the information and communications technology and services ("ICTS") supply chain.[98] In this Executive Order, the

[90] *National Strategy to Secure 5G of the United States of America*, WHITE HOUSE (Mar. 2020),hsdl.org/?view&did=835776.
[91] *Id.* at 1.
[92] *Id.* at 3.
[93] *Id.* at 4-5.
[94] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No.115-390 (2018).
[95] *Id.* at § 101.
[96] *Id.* at § 201.
[97] 41 C.F.R. § 201 (2020).
[98] Exec. Order No. 13,873, 84 Fed. Reg. 22689 (May 15, 2019).

President invoked his authority pursuant to the International Emergency Economic Powers Act to declare a national emergency. In doing so, the President found that maintaining an open investment climate in the ICTS arena must be balanced against the criticalnational security threats posed by technological developments. In furtherance of finding this balance, the President authorized the Secretary of Commerce (in consultation with other departments and agencies), to prohibit ICTS transactions involving foreign adversaries that pose an "undue risk" or "unacceptable risk" to national security.[99]

Pursuant to the Executive Order on securing the ICTS supply chain, the Secretary of Commerce was instructed to issue regulations within 150 days establishing the procedures for reviewing these transactions.[100] The Department of Commerce issued a proposed rule, which laid out procedures for reviewing transactions on a case-by-case basis.[101] On December 23, 2019, the Department of Commerce extended the comment period for the proposed rule until January 10, 2020.[102] However, the Secretary of Commerce has not issued a final rule regarding these procedures.[103]

In addition to the FASC and Executive Order to secure the ICTS supply chain, the federalgovernment also relies on the 2019 National Defense Authorization Act ("NDAA") to help secure its computer systems.[104] The 2019 NDAA specifically prohibits government agencies from using technology produced by Huawei (among others).[105] Another section of the NDAA, which went into force in August 2020, prohibits government agencies from contracting

[99] *Id.* at § 1(a)(ii)(A)-(C).
[100] *Id.* at Sec. 2(b).
[101] 15 C.F.R. § 7 (2019).
[102] *Id.* (as amended on Dec. 23, 2019).
[103] *Commerce Department Issues Interim Rule to Secure the ICTS Supply Chain,* U.S. Dep't of Com., 2017-2021.commerce.gov/news/press-releases/2021/01/commerce-department-issues-interim-rule-secure-icts-supply-chain.html (last visited Feb. 8, 2022) (Announcing an interim final rule and the final rule will consider additional comments. The final rule has not yet been promulgated).
[104] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong. (2018) (enacted)[hereinafter McCain NDAA].
[105] *Id.* at §§ 889(a)(1)(A) and (f)(3)(A).

with entities that use Huawei technology "as a substantial or essential component of any system, or as critical technology as part of any system."[106] Again, the 2019 NDAA only regulates activities by government agencies and the military; private corporations are not impacted by this legislation.

It is likely that the resolution of many of these issues have been delayed by the onset of the 2019 novel coronavirus ("COVID-19"), which brought the U.S. government to a grinding halt in many areas. To that effect, CISA has published an analysis report regarding the impact of COVID-19 on the ICTS supply chain and how to build a more resilient supply chain for the future.[107] All these efforts are a governmental attempt to ensure that the United States remains on the forefront of developing technology and equipment.

B. Current Status of Cyber Response

1. Budapest Convention

In 1997, the Council of Europe ("CoE") assembled a committee of experts on crime in cyberspace. The CoE tasked this committee with drafting a document laying out procedures for addressing the growing issue of cybercrime.[108] This draft document laid the foundation for the Convention on Cybercrime (hereinafter "the Budapest Convention" or "the Convention"). After extensive revisions and an opportunity for the public to review the draft document, the final draftof the Budapest Convention was opened for signature in 2001 and came into force in 2004.[109]

---

[106] *Id.* at § 889(a)(1)(B).

[107] *Building A More Resilient ICT Supply Chain: Lessons Learned During the COVID-19 Pandemic*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY (Nov. 2020), www.cisa.gov/sites/default/files/publications/lessons-learned-during-covid-19-pandemic_508_2.pdf.

[108] COUNCIL OF EUROPE, EXPLANATORY REP. TO THE CONVENTION ON CYBERCRIME 3-4 (Nov. 23, 2001), rm.coe.int/16800cce5b.

[109] *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUROPE, www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (last visited Jan. 4, 2021).

The Budapest Convention is currently the only binding international agreement regarding cybercrime.[110] Sixty-five states, including twenty-one non-CoE states, such as the United States,have ratified the Convention.[111] For a state to become a member of the Budapest Convention, a state must be invited by a Contracting State;[112] there must be "unanimous consent of the Contracting States" to accept the invitee;[113] and, if the invitee is a non-CoE member, it must accept the invitation within five years.[114]

The Convention's primary purpose is to establish "a common criminal policy aimed at the protection of society against cybercrime."[115] The Convention requires signatory states to adopt legislation at the domestic level criminalizing certain computer-related offenses[116] and establish general principles for mutual legal assistance and international cooperation.[117] However, the Convention has been criticized for being too Western in nature and origin because more than fifty percent of the contracting states are CoE members and the United Statesis one of the few non-CoE members that has any significant voice in the drafting of the Convention.[118] Additionally, due to varying interests and priorities of the original signatory nations, many argue that the Convention is too broad in its definitions of

[110] *Id.*

[111] Ratifying nations include forty-four Council of Europe member nations and twenty-one non-member nations. *Id.*

[112] Convention on Cybercrime, art. 37(1), Nov. 23, 2001, T.I.A.S. No. 13, 174, 2296 U.N.T.S. 167 (Jan. 7, 2004) [hereinafter Budapest Convention].

[113] *Id.*

[114] Currently there are eight non-CoE nations with pending invitations to join the Budapest Convention. *See Non- members States of the Council of Europe*, COUNCIL OF EUROPE, rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22 (last visited Jan. 4, 2021).

[115] Budapest Convention, *supra* note 112, at Preamble.

[116] *Id.* at arts. 2-13.

[117] *Id.* at arts. 23-28.

[118] Initially the United States was merely an observer to the negotiations, but the Council of Europe eventually requested that the United States participate in the negotiations thus giving the United States more input in the actualdrafting of the treaty. Sara L. Marler, *The Convention on Cyber-Crime: Should the United States Ratify*, 37 NEW ENG. L. REV. 183, 198 (2002).

certain cybercrimes and does not do enough to protect privacy rights of individuals.[119]

Despite accusations of being too Western and a failure, the Convention serves as a baseline for cyber strategies all over the world.[120] Given that there is no globally accepted definition of cybercrime, the Budapest Convention has managed to create a system where nations with different legal systems and traditions have agreed on basic criminal activities that constitute cybercrime.[121] The Convention itself is backed by the Cybercrime Convention Committee ("T- CY"), which assesses parties' implementation of the Convention, as well as the Cybercrime Programme Office ("C-PROC"), which builds the worldwide capacity of sates to implement the Convention.[122] Thus, Convention members are held to Convention standards by the T-CY while the C-PROC develops and encourages new countries to adopt the Convention or, at least, base its own cybercrime model around the Convention's principles.[123]

a. Proposed Additional Protocol

It has been fifteen years since the Budapest Convention has been updated.[124] However, the substantive procedural elements have

---

[119] NEIL BOISTER, AN INTRODUCTION TO TRANSNATIONAL CRIMINAL LAW 189-96 (2nd ed. 2018).

[120] Alexander Seger, *Enhanced Cooperation on Cybercrime: A Case for a Protocol to the Budapest Convention*, ITALIAN INST. FOR INT'L POL. STUD. (July 16, 2018), www.ispionline.it/en/pubblicazione/enhanced- cooperation-cybercrime-case-protocol-budapest-convention-20964.

[121] MARY GREER & TARA MOBARAKI, A.B.A., RULE OF LAW APPROACHES TO VIRTUAL THREATS 10 (2019).

[122] Seger, *supra* note 120.

[123] Alexander Seger, *The Budapest Convention on Cybercrime: A Framework for Capacity Building*, GFCE (July12, 2016), thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/.

[124] Additional Protocol I (AP I) entered into force on March 1, 2006. This first additional protocol addressed the criminalization of racist and xenophobic acts committed in cyberspace. Thirty-two of the sixty-five Contracting States have ratified AP I. The United States has not ratified this protocol. *See Chart of Signatures and Ratificationsof Treaty 189*, COUNCIL OF EUROPE, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=h59sZJAT (last visited Jan. 4, 2021).

not been touched since the Convention was originally drafted. Responding to the need for updates to the Convention, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol ("AP II").[125] AP II consists of the following elements: more efficient mutual legal assistance; increased direct cooperation; extended transborder searches; and increased rule of law and data protection safeguards.[126] These changes are intended to ensure that the Convention remains relevant and addresses the developments in cyberspace and cybercrime since the Convention's drafting. There are two provisions within AP II which merit specific discussion. Those provisions are Article Seven and Article Eight.

Article Seven is entitled "Disclosure of Subscriber Information." The text of Article Seven requires that contracting states promulgate legislature that allows "its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party . . . where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings."[127] The explanatory report, which accompanies the text of AP II, explains that this provision will allow law enforcement to request the "subscriber's identity, postal or geographical address, telephone or other access number, billing and payment information" and states that a request pursuant to this paragraph "may include certain Internet Protocol ("IP") address information—for example, the IP address used at the time when an account was created, the most

[125] *Second Additional Protocol to the Cybercrime Convention Adopted by the Committee of Ministers of the Council of Europe*, Council of Europe (Nov. 17, 2021) www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe.

[126] Counsel of Europe, *Discussion Guide for Consultations with Civil Society, Data Protection Authorities and Industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime* 3 (Sept. 18, 2019), rm.coe.int/t-cy-2019-28-pdp-consultations-paper-v1c/168097fe1f.

[127] Counsel of Europe, Cybercrime Convention Committee: Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence (Nov. 17, 2021), at art. 7.1 [hereinafter AP II].

recent log-on IP address or the log-on IP addresses used at a specific time."[128]

Article Eight is entitled "Giving Effect to Orders from Another Party for Expedited Production of Subscriber Information and Traffic Data." The text of this Article requires that Contracting States implement legislature compelling service providers within their domestic jurisdiction "to produce specified and stored subscriber information" upon receiving an order from a requesting nation.[129] Essentially, this provision enables law enforcement to go directly to a service provider and compel that service provider to disclose the requested information without the involvement of the service provider's host nation.

b. Proposed Russia-China Cyber Treaty

Since 2011, China and Russia have made annual proposals to the UN General Assembly regarding information security and cybercrime.[130] Most of these proposals have stalleddue to a lack of global support. However, on January 13, 2015, China and Russia's proposal to the UN General Assembly started to gain traction in the global community.[131] This proposal led to the creation of an intergovernmental expert group tasked with writing a report on the current status of global cybercrime.[132] It ultimately resulted in the adoption of another draft document entitled "Countering the use of

[128] AP II, *supra* note 127, at ¶ 93.
[129] AP II, *supra* note 127, at art. 8.1(a).
[130] Mark A. Barrera, The Achievable Multinational Cyber Treaty: Strengthening Our Nation's Critical Infrastructure, AIR UNIV. (2017), media.defense.gov/2017/Jun/19/2001764798/-1/-1/0/CPP_0003_BARRERA_MULTINATIONAL_CYBER_TREATY.PDF.
[131] Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, Uzbekistan to the U.N.,Letter dated Jan. 9, 2015 from the Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan addressed to the Secretary-General, U.N. Doc. A/69/723 (Jan. 13, 2015) [hereinafter Russia-China Proposal].
[132] The report is expected sometime in 2020. *See* Meetings Coverage and Press Release, General Assembly, GeneralAssembly Approves $3.07 Billion Programme Budget as It Adopts 22 Resolutions, GA/12235 (Dec. 27, 2019), www.un.org/press/en/2019/ga12235.doc.htm [hereinafter UN Press Release].

information and communication technologies for criminal purposes" and the creation of an open-ended ad hoc intergovernmental committee of experts to explore the creation of an international convention regarding cybercrime.[133]

The success of this proposal indicates a global shift in attitude regarding the purpose and treatment of the Internet. The United States and most Western nations believe the Internet should be open, free, and secure—a platform for free speech and the exchange of ideas.[134] However, the current Russia-China proposal focuses more on internet censorship and cyber sovereignty (a concept which will be explained more in depth in Subsection C).[135] The United States staunchly opposed this resolution believing that it "would stifle global anti-cybercrime efforts" and that it was premature to launch a committee exploring a new convention before the appointed panel of experts produced their report on the status of global cybercrime.[136]

2. Domestic Structure and Law

Cyberspace offers a vast array of capabilities and issues that are addressed by an equallyvast array of government agencies and departments. While preventing and prosecuting cybercrime are typically the most visible aspects of the field, another area of importance includes the development of partnerships with private corporations to counter cyber threats.

a. Federal Organization

Similar to the field of cybersecurity and cyberspace itself, the U.S. agencies and departments tasked to handle cybersecurity are, themselves, growing and developing. There are at least eight federal departments as well as several law enforcement agencies that each play

[133] *Id.*
[134] Joyce Hakmeh & Allison Peters, *A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open,Free, and Secure Internet*, COUNCIL OF FOREIGN REL. (Jan. 13, 2020), www.cfr.org/blog/new-un- cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.
[135] *See* discussion *infra* Section II.C.
[136] UN Press Release, *supra* note 132.

a significant role in cybercrime investigation, prosecution, and enforcement.[137] Not only are there a variety of agencies dealing with different aspects of cybersecurity, but there is also a veritable army of congressional committees and subcommittees claiming jurisdiction over cybersecurity policy.[138]

In an attempt to unite the capabilities and operations of each agency, then-President Obama created the position of cybersecurity coordinator.[139] The cybersecurity coordinator sat on the National Security Council and acted as a focal point for the nation's cyber efforts. With so many agencies and programs involving the cyber domain, the cybersecurity coordinator was tasked with developing a new comprehensive cyber strategy; organizing a unified response to future cyber incidents; and strengthening public-private partnerships.[140] In order to properly respond to a cyberattack, the cybersecurity coordinator facilitated communication between cyber-related agencies and created an action plan to mitigate the damage after a large-scale attack. However, in 2018, National Security Advisor Bolton eliminated the cybersecurity coordinator position, claiming that the position was redundant and that other agencies were already performing the same or similar functions.[141] Many experts criticized this move and claimed that it downplayed the importance of cybersecurity in the U.S. national security plan andresponse.[142]

---

[137] Brandon Gaskew, *Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget*, THIRD WAY (Feb. 21, 2019), thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement- architecture-and-budget.

[138] There are approximately eighty Congressional entities involved in forming cybersecurity policy. Simon Handler,*Cybersecurity and the 117th Congress*, ATL. COUN. (Oct. 12, 2020), www.atlanticcouncil.org/blogs/new-atlanticist/cybersecurity-and-the-117th-congress/.

[139] Macon Phillips, *Introducing the New Cybersecurity Coordinator*, WHITE HOUSE (Dec. 12, 2009),obamawhitehouse.archives.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator.

[140] Eric Chabrow, *Reports: Schmidt Tapped as Cybersecurity Coordinator*, Gov. Info. SEC. GOV. INFO. (Dec. 21, 2009), www.govinfosecurity.com/reports-schmidt-tapped-as-cybersecurity-coordinator-a-2021.

[141] Nicole Perlroth & David E. Sanger, *White House Eliminates Cybersecurity Coordinator Role*, N.Y. TIMES (May15, 2018), www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html.

[142] *Id.*

Shortly after the elimination of the cybersecurity coordinator position, Congress passed the CISA Act.[143] The Act, signed into law on November 16, 2018, reorganized existing programs within the DHS to create CISA.[144] Previously, DHS's National Protection and Programs Directorate was responsible for reducing and eliminating threats to U.S. critical infrastructure, both physical and cyber.[145] However, after hackers stole records regarding approximately twenty-two million current, former, and aspiring government employees from the Office of Personnel Management ("OPM"), legislators realized that the cybersecurity in the federal government needed a serious reevaluation.[146]

While CISA is just beginning to grow into its role, the new director claimed that the lack of a cybersecurity coordinator has not hindered U.S. cyber deterrence efforts and asserted that the absence of the position does not mean that there is no coordination of U.S. cyber efforts.[147] In fact, CISA's mission is to "lead the National effort to understand and manage cyber and physical risk to our critical infrastructure."[148] Congress has tasked CISA with coordinating security as well as building the national capacity to defend against cyberattacks; this includes safeguarding federal government cyber assets (such as the records lost in the OPM hack).[149]

---

[143] Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law No. 115-278 [hereinafter CISA Act of 2018].
[144] H.R. Rep No. 115-454, at 2 (2017) ("The bill realigns the current NPPD structure so it can more effectively carry out the existing authorities provided in law…").
[145] NPPD at a Glance, Department of Homeland Security, Feb. 13, 2018 available at www.cisa.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf (last accessed Feb. 8, 2022).
[146] Zachary Figueroa, *Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for CentralizedCybersecurity Infrastructure*, 24 CATH. U. J. L. & TECH. 433, 436-37 (2016).
[147] Jack Corrigan, *Lawmakers Urge new National Security Adviser to Restore White House Cyber Coordinator*, NEXTGOV (Sept. 19, 2019), www.nextgov.com/cybersecurity/2019/09/lawmakers-urge-new-national-security-adviser-restore-white-house-cyber-coordinator/160008/.
[148] *About CISA*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, www.cisa.gov/about-cisa (last visited Oct. 30, 2020).
[149] CISA Act of 2018, *supra* note 143, at § 2202(e)(1).

In addition to creating CISA, Congress established the Cyberspace Solarium Commissionwith the 2019 NDAA. The purpose of the Commission was to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks [sic] of significant consequences."[150] The 2020 Cyberspace Solarium Commission's report recommended a layered approach to cyber defense capabilities as well as the creation of a new cybersecurity office within the U.S. government, the Office of the NCD.[151] The 2021 NDAA contains a provision requiring the immediate establishment of an NCD position within the Executive Office of the President.[152]

b. Cybersecurity Laws Governing Private Corporations

After a cyberattack, private corporations must consider the scope and severity of thebreach to determine which parties they are legally obligated to notify. Potential parties include the victim corporation's investors, customers, commercial partners, and, potentially, law enforcement. However, this disclosure determination depends on the discrete laws of the state governing the corporation as well as a handful of federal disclosure obligations. This results in even further complications, particularly for larger companies who may be subject to multiple jurisdictions, as each state and territory has its own data breach law resulting in fifty-four unique legal regimes.[153]

Additionally, there is very little incentive for businesses to cooperate with law enforcement and federal oversight agencies, which is reflected in the number of reported breaches. In 2011, the Security and Exchange Commission ("SEC") issued guidance regarding reporting requirements. However, since that time, only 106 companies reported incidents to the SEC despite there being at least

[150] McCain NDAA, *supra* note 104, at § 1652(a)(1).
[151] United States Cyberspace Solarium Commission, Final Report, March 2020, at 1-3 (available at www.solarium.gov/report) [hereinafter "CSC Final Report"].
[152] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. § 1752 (2020) [hereinafter 2021 NDAA].
[153] *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATORS (July 17, 2020), www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

4,732 successful cyberattacks on U.S. businesses.[154] This clearly indicates that breaches are drastically underreported to the federal government. To effectively investigate and attribute cybercrimes to their source, law enforcement must have access to this breach information as soon as it is detected.

Given the inconsistency in reporting requirements and the overall lack of reporting to law enforcement, federal officials are beginning to consider alternatives to state regulation. For example, Deputy Assistant Attorney General of the National Security Division, Adam S. Hickey,recommended to the Senate Subcommittee on Crime and Terrorism that Congress pass a federal data breach law, which will "include a requirement to promptly notify law enforcement in addition to, and in advance of, notification to impacted customers. Government notification would increase federal law enforcement's ability to pursue hackers and prevent databreaches."[155]

The importance of folding the private sector into the United States' overall cybersecurity plan is reflected in the potential damage an attack on private industry could cause. For example, if a malicious actor targets a privately owned utility, such as a water company, the loss of that service could impact millions of Americans. This threat is also demonstrated by the real-world implications of the cyberattack against Ukraine's power grid as previously mentioned. Thus, even though an industry is privately operated, an attack on such an industry could constitute "an attack against [a] nation's critical infrastructure and, therefore, against [the] nation."[156]

---

[154] Craig A. Newman, *When to Report a Cyberattack? For Companies, That's Still a Dilemma*, N.Y. TIMES (Mar. 5,2018), www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html.

[155] *Dangerous Partners: Big Tech & Beijing: Hearing Before the Subcomm. On Crime & Terrorism, of the S. Comm. on the Judiciary*, 116th Cong. 11 (2020) (statement of Adam S. Hickey, Deputy Assistant Att'y Gen., Nat'l Sec. Div.).

[156] *The Cybersecurity Partnership Between the Private Sector and Our Gov't: Protecting Our Nat'l and Econ. Sec.:Joint Hearing Before the S. Comm. On Com., Sci., & Transp. & the S. Comm. On Homeland Sec. & Governmental Aff.*, 113th Cong. 1 (2013) (statement of Sen. John D. Rockefeller IV, Chairman, S. Comm. of Com., Sci., & Transp.).

C. Understanding China's Perceptions of Cyberspace

In order to understand the U.S.-China relationship in cyberspace, it is critical to have at least a basic understanding of the fundamental differences in how the United States and China perceive the challenges and threats presented by the digital arena. China and the United States have very divergent cultures with regards to legal systems and societal values, which results in different views in foreign policy and international affairs.[157]

While an in-depth comparative law analysis between U.S. and Chinese systems is beyondthe scope of this Article, the purpose of this section is to provide a basic overview of the United States' understanding of Chinese priorities in cyberspace. These are the lenses through which China views cyberspace, a perspective that U.S. national security practitioners must understand to successfully secure cyberspace. Two of those main priorities are cyber sovereignty and mutualstrategic trust, which includes perceived U.S. hegemony over cyberspace. This section will also provide a brief overview of previous U.S.-China dialogues regarding conduct in cyberspace.

1. Cyber Sovereignty

The creation of the cyber domain introduced a new frontier, whose ownership is up for grabs. Some nations believe cyberspace should be a free and independent area controlled byprivate individuals and companies.[158] Other nations believe cyberspace should be controlled by nation-states and each nation should be able to determine what information is available and limit their citizens' access to this new space.[159]

---

[157] SCOTT W. HAROLD ET AL., GETTING TO YES WITH CHINA IN CYBERSPACE 3-4 (2016), www.rand.org/pubs/research_reports/RR1335.html.

[158] Sascha Meinrath & Nathalia Foditsch, *How Other Countries Deal with Net Neutrality*, SMITHSONIAN (Dec. 15, 2017).

[159] Paul Bischoff, *Internet Censorship 2020: A Global Map of Internet Restrictions*, COMPARITECH (Jan. 15, 2020),www.comparitech.com/blog/vpn-privacy/internet-censorship-map/.

The concept of a government-controlled and censored internet runs contrary to U.S. interests and intents regarding the Internet, as spelled out in the U.S. National Cyber Strategy. Pursuant to the Cyber Strategy, one of the United States' key tenants for the Internet is that it remains "open, interoperable, reliable, and secure."[160] The Cyber Strategy also states that the responsibility of cybersecurity and the security of U.S. critical infrastructure "is shared by the private sector and the Federal Government."[161]

However, China places its focus on information control and preserving the interests ofthe government, a concept referred to as cyber sovereignty. An expert of Sino-U.S. defense relations described the concept of cyber sovereignty "as the foundation for a new internationalcode of conduct for cyberspace . . . in which the principle of sovereignty enshrined in the UN Charter extends to cyberspace."[162] Thus, to understand China's perspective regarding cyber sovereignty, one must understand traditional national sovereignty pursuant to the UN Charter.

According to the UN Charter, member-states are entitled to "sovereign equality"[163] in exchange for fulfilling "in good faith the obligations assumed by them in accordance with the present Charter."[164] This is intended to ensure that all nations, regardless of traditional measures of power or size, are regarded as deserving equal treatment and respect of their sovereign rights. The UN Charter also upholds the principle of non-intervention amongst member states. Article 2(4) of the Charter calls on all member-states to respect the sovereignty, territorial integrity, and political independence of other member-states.[165] This principle of non-intervention echoes the notion of co-equal sovereigns.[166] Out of respect for sovereignty, no

[160] *National Cyber Strategy of the United States of America*, WHITE HOUSE 1 (Sept. 2018) [hereinafter National Cyber Strategy].
[161] *Id.* at 8.
[162] Michael Kolton, *Interpreting China's Pursuit of Cyber Sovereignty and Its Views of Cyber Deterrence*, 2 CYBER DEF. REV. 119, 120 (2017).
[163] U.N. Charter, art. 2(1).
[164] *Id.* at art. 2(2).
[165] *Id.* at art. 2(4).
[166] *Id.* at art. 2(1).

nation should attempt to interfere in the internal affairs of another.[167] These traditional notions of sovereignty are "under pressure by a combination of international tensions and disruptive digital transformation throughout economy and society."[168]

One of the most treasured and traditional areas of sovereignty is the exclusive ability to enforce criminal sanctions and conduct law enforcement activities within one's own territory.[169] However, the digital transformation is not limited to the economy but has resulted in a new categoryof crime: cybercrime. These crimes are comprised of new variants of old crimes (for example: fraud, money laundering, and information theft) as well as an array of new crimes (such as ransomware and denial of service attacks).[170] Cybercrime can originate from and target any nation in the world resulting in unprecedented complications to criminal investigation and law enforcement.

Nations have attempted to overcome these challenges while preserving their sovereignty through mutual legal assistance agreements. These agreements are typically executed through bilateral treaties, which create reciprocal obligations to provide assistance in gathering evidence and information regarding transnational crime like cybercrime.[171] These treaties are typically bilateral as this allows them to be "tailored to a particular relationship" and also permits "states to choose their treaty partners."[172] China and the United States entered into such a treaty in 2000.[173] This treaty ensures a basic level of cooperation and mutual assistance between the two nations in

[167] Nicaragua v. United States (ICJ Reports 1986, ¶ 202).
[168] Paul Timmers, *Challenged by "Digital Sovereignty,"* 23 J. INTERNET L. 11, 12 (2019).
[169] For general overview of prescriptive and enforcement jurisdiction, *see* Restatement (Fourth) of the ForeignRelations Law of the United States, § 401 (Am. L. Inst. 2017).
[170] BOISTER, *supra* note 119, at 187.
[171] *Id.* at 313.
[172] *Id.* at 314.
[173] Agreement on Mutual Legal Assistance in Criminal Matters, China-U.S., June 19, 2000, State Dep't No. 13102,www.state.gov/wp-content/uploads/2019/02/13102-China-Law-Enforcement-MLAT-6.19.2000.pdf.

furtherance of preventing crime, namely cybercrime.[174] This bilateral treaty constituted a crucial step forward in Sino-U.S. relations; however, further steps are often hindered by the lack of mutual strategic trust between the two nations. The next section explores this concept in greater depth as well as its influence in Chinese foreign affairs.

2. Mutual Strategic Trust

Mutual strategic trust is an important concept to Chinese practitioners and experts.[175] However, this concept is not one that frequently surfaces in Western practice and strategic conversations. A simple definition of the term is that "both sides are aware of each other's strategic purposes while holding positive expectations of each other's positions and actions onissues of vital interests."[176] This does not mean that mutual strategic trust requires complete disclosure of priorities and prerogatives; however, it does entail an expectation that conversations and interactions be sincere and consider the mutual benefit of both nations.[177] Mutual strategic trust constitutes the foundational framework that two nations recognize that they have more in common than not and that both nations are invested in a healthy, long-term relationship.[178]

The current level of mutual strategic trust between China and the United States is negligible, if any exists at all.[179] In fact, China has expressed concerns regarding the perceived monopoly that the United

[174] *Id.* ("Desiring to improve the effectiveness of cooperation between the two countries in respect of mutual legal assistance in criminal matters on the basis of mutual respect for sovereignty, equality and mutual benefit.").
[175] HAROLD ET AL., *supra* note 157, at 51.
[176] Yingyi Qian et al. *Building Mutual Trust Between China and the U.S.*, 2 THE WORLD IN 2020 ACCORDING TO CHINA: CHINESE FOREIGN POLICY ELITES DISCUSS EMERGING TRENDS IN INTERNATIONAL POLITICS 277, 281 (SHAO Binhong ed., 2017).
[177] Yawen Chen & Se Young Lee, *China Slams U.S. Blacklisting of Huawei as Trade Tensions Rise*, REUTERS (May16, 2019), www.reuters.com/article/us-usa-trade-china-huawei/china-opposes-u-s-move-to-blacklist-telecom-giant-huawei-idUSKCN1SM0NR.
[178] QIAN ET AL., *supra* note 176.
[179] Yan Xuetong, *Strategic Cooperation without Mutual Trust: A Path Forward for China and the United States*, 15 ASIA POLICY, 4 (2013).

States enjoys over the Internet.[180] China has even gone so far as to label this perceived U.S. monopoly and dominance in cyberspace as "cyber hegemony."[181] This description and perception indicate the lack of trust and common interests currently expressed between China and the United States, particularly in cyberspace. The lack of mutual strategic trust makes it difficult for China's representatives to engage in a meaningful relationship and discussions with U.S. representatives on the future of global policies and rules in cyberspace.

However, this does not mean that the United States and China cannot establish a relationship based on mutual strategic trust in the future. Nor does it mean that the United States and China cannot engage in productive conversations regarding the future of cyberspace and cybersecurity in the absence of this mutual strategic trust.[182] Building that mutual trust will take time, dedication, and resources on both sides. Despite the current tensions in the relationship, parties on both sides of the Pacific have attempted to reach out and engage in constructive dialogue regarding the future of cyberspace. In order to understand the future of the Sino-U.S. relationship, it is important to understand past dialogues. The next section details some of those recent efforts.

3. Previous Dialogues Between the U.S and China

The Sino-U.S. relationship experienced many ups and downs in the last ten years. The decade began with a series of mixed formal-informal talks between Chinese and U.S. think-tanks, civilian research institutes, and government personnel.[183] These mixed talks were interspersed with formal government talks and were eventually supplemented by the U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues which began in 2015 after President Xi

[180] Michael D. Swaine, *Chinese Views on Cybersecurity in Foreign Relations*, 42 CHINA LEADERSHIP MONITOR 1, 5 (2013), carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf.
[181] HAROLD ET AL., *supra* note 157, at 10.
[182] *See generally* Xuetong, *supra* note 179 (providing a more detailed discussion regarding cooperation without mutual strategic trust).
[183] HAROLD ET AL., *supra* note 157, at 49.

Jinping's state visit to the United States in September of 2015.[184] The High-Level Joint Dialogue continued until 2017 when it was replaced by the U.S.-China Law Enforcement and Cybersecurity Dialogue after President Xi's meeting with then-President Trump in April of 2017.[185] However, since the increased trade tensions between the United States and China, discussions regarding the future of cyberspace at the highest levels have "been in limbo."[186] In 2019, representatives from the United States and China engaged in a Track Two dialogue to discuss the risks ofcyber conflict.[187]

Between 2009 and 2017, the Center for Strategic and International Studies in the United States and the China Institute of Contemporary International Relations held formal and informal meetings on cybersecurity. These meetings were originally proposed as the Track 2.0 dialogue but became known as the Track 1.5 dialogue due to the heavy involvement of non-government officials in the working groups.[188] The purpose of these meetings was to "reduce misperceptions and to increase transparency of both countries' authorities and understand how each country approaches cybersecurity, and to identify areas of potential cooperation, including confidence building measures and agreement on norms and rules for cybersecurity."[189] During these meetings, China repeatedly

[184] Press Release, The White House, Office of the Press Sec'y, FACT SHEET: President Xi Jinping's State Visit tothe United States (Sept. 25, 2015) [hereinafter White House Fact Sheet].

[185] Media Note, The White House, Office of the Spokesperson, *U.S.-China Law Enforcement and Cybersecurity Dialogue* (Oct. 3, 2017), 2017-2021.state.gov/u-s-china-law-enforcement-and-cybersecurity-dialogue/index.html [hereinafter Media Note].

[186] Nike Ching, *US, China Look to October Talks to Patch Up Rocky Relations*, VOA NEWS (Sept. 8, 2018, 1:35 AM),www.voanews.com/a/us-china-look-to-october-talks-to-patch-up-rocky-relations/4562339.html.

[187] *2019 U.S.-China Track II Dialogue on the Digital Economy*, NAT'L COMM. ON U.S.-CHINA RELS., www.ncuscr.org/program/us-china-track-ii-dialogue-digital-economy/2019 (last visited Feb. 27, 2022).

[188] HAROLD ET AL., *supra* note 157, at 49.

[189] *Track 1.5 U.S.-China Cyber Security Dialogue*, CSIS, www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/other-projects-cybersecurity-3 (last visited Feb. 27, 2022).

emphasized the importance sovereignty in the information sphere and articulated its worries about U.S. dominance in cyberspace.[190]

In 2015, the discussions between the United States and China were elevated to the highest levels via a state meeting between then-President Obama and President Xi. During this meeting, the two leaders reached agreement that neither country would "conduct or knowingly support cyber- enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[191] This agreement was touted as a success and a significant first step toward improving relations between China and the United States.[192] The state meeting also resulted in an agreement to hold the U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues.[193]

The U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues had its firstmeeting in December of 2015.[194] During the first meeting, the U.S. Attorney General and China's State Councilor reached an agreement regarding guidelines for requesting assistance on cybercrime and responding to these requests.[195] Both sides also agreed to develop further cooperation to combat cyber-enabled crimes and established a group of cyber incident and network protection experts in furtherance of this goal.[196] In June 2016, the second meeting specifically addressed misuse of technology and communications to facilitate terrorism and created an action plan to address the threat posed from business e-mail compromise scams.[197]

---

[190] HAROLD ET AL., *supra* note 157, at 49.
[191] White House Fact Sheet, *supra* note 184.
[192] Marianne Kolbasuk McGee, *U.S., China Reach Cyber Agreement*, BANK INFO. SEC. (Sept. 25, 2015),www.bankinfosecurity.com/us-china-a-8553.
[193] White House Fact Sheet, *supra* note 184.
[194] Press Release, U.S. Dep't. of Just., First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues: Summary of Outcomes, (Dec. 2, 2015), www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0.
[195] *Id.*
[196] *Id.*
[197] Press Release, U.S. Dep. of Homeland Sec., Second U.S.-China Cybercrime and Related Issues High Level JointDialogue (June 15, 2016),

The third, and final, meeting of the High-Level Joint Dialogue was held in December 2016 where the group launched the U.S.-China Cybercrime Hotline to facilitate expedited cooperation between the two nations.[198] The group also continued its discussions regarding cybercrime deterrence and network protection.[199]

In 2017, the U.S.-China Law Enforcement and Cybersecurity Dialogue replaced the Obama administration's dialogue.[200] The first, and only, meeting affirmed the commitments of the previous High Level Joint Dialogue, declared both nations' intentions to make progress on those previous commitments, and both nations agreed to meet in 2018 to measure and discuss their progress.[201] However, escalating tensions between the United States and China have prevented productive cybersecurity conversations between the two governments since 2018. Despite these tensions and difficulties, in 2019, a Track Two Dialogue began to analyze the situation between the two nations and discuss the risks of cyber conflict.[202]

III. ADDRESSING INTERNATIONAL AND DOMESTIC CHALLENGES: PROPOSED SOLUTIONS

The diverse array of issues in cyberspace requires a multi-pronged solution. Subsection A addresses international solutions, specifically the Budapest Convention and international standard-

www.dhs.gov/news/2016/06/15/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue.

[198] Press Release, U.S. Dep. Of Just., Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues (Dec. 8, 2016), www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues.

[199] *Id.*

[200] Media Note, *supra* note 185.

[201] Press Release, U.S. Dep. of Justice, First U.S.-China Law Enforcement and Cybersecurity Dialogue, (Oct. 6, 2017), www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.

[202] These Track Two dialogues, initiated by the Belfer Center not the U.S. or China, are comprised of former government and military officers as well as professionals in the field to discuss the Sino-U.S. cyber relationships.There is no official government participation in these discussions as of the writing of this paper. Julia Voo, *U.S.-China Cybersecurity Group Explores Mutual Interests, Goals*, HARVARD KENNEDY SCH. BELFER CTR. (last visited Feb. 27, 2022), www.belfercenter.org/publication/us-china-cybersecurity-group-explores-mutual-interests-goals.

setting organizations. First, this Article proposes new membership protocols which convey a message of inclusivity and acceptance. Additionally, AP II contains two specific provisions which would further alienate non-member nations (namely China and Russia) and solidify the Convention's place as a "Western" treaty. In accordance with previous criticisms, these provisions should be removed or, at least, amended. Second, as already recognized, the United States, both private companies and government, must continue to participate in international standard-setting organizations to preserve international unity and increase U.S. input regarding the global 5G process.

Subsection B addresses domestic solutions to the United States' cyber readiness. First, CISA is perfectly placed to act as the desperately needed governmental focal point for all cyber-related issues. Congress should reject proposals creating an NCD at this time. Second, due to the United States' privatization of infrastructure and critical systems, private corporations are integral to national security. As suggested by Federal Bureau of Investigation ("FBI") Director Christopher Wray, a mandatory reporting requirement for data breaches in private corporations would ensure that the federal government is apprised of all malicious cyber activity and further protect private corporations by increasing cooperation and information sharing.[203] Finally, this Article supports opening and diversifying the supply chain through existing solutions, such as the Blue Dot Network, which do not target specific entities, but rather set impartial and consistent technical requirements for supply chain sources.

A. Reforms to International Law and U.S. Participation

As previously discussed, the Budapest Convention was signed in 2001 and came into force in 2004. The technological advances of the last twenty years have been enormous. Today's global community faces issues that the drafters of the Convention did not account for, including data confidentiality and responsibilities of Internet service

[203] Maggie Miller, *Intelligence Leaders Push for Mandatory Breach Notification Law*, THE HILL (April 15, 2021), thehill.com/policy/cybersecurity/548289-officials-push-for-breach-notification-deterrence-measures-following.

providers.[204] While it is true that the Convention was initially groundbreaking, there are significant issues with the Convention as applied today.

One of the main attacks against the Convention is that it was drafted by Western nationsand thus does not reflect the interests of non-Western nations. China and Russia regularly repeat this criticism and argue that the Convention should be replaced by a truly global agreement.[205] However, the time and resources it would take to agree on a new global cybercrime treaty, if an agreement could be reached at all, would be better spent elsewhere. Thus, the United States should lead the effort to modify the existing Convention. The keys to these reforms lie in a new proposal amending membership procedures and heeding current calls to revise the proposed additional protocol.

The United States should answer previous calls to increase its participation in global standard-setting organizations (such as 3GPP) to address mounting cyber issues. The world isalready in disarray regarding cyberspace and cybercrime, the United States should take all necessary steps to prevent further fragmentation. To ensure the continuation of "an open, interoperable, reliable, and secure Internet," the United States needs to create larger global buy-in and support for this concept.[206]

In order to ensure a single, global internet in the future, the United States must recognize the serious possibility that China could establish its own independent internet servers. This secondary option could attract other nations, such as China's traditional and regional allies, thus creating a divide in the international community and the very fabric of the global economy. To prevent this, the United States should lead the way and open discussions regarding the future of the Internet and cybersecurity.

[204] BOISTER, *supra* note 119, at 195.
[205] BARRERA, *supra* note 130.
[206] National Cyber Strategy, *supra* note 160.

1. Reforms to the Budapest Convention

a. Western Dominance and Calls for a New Convention

The primary argument against the Convention is that it was drafted primarily by Westernnations and that the exclusion of other nations (such as China and Russia) has resulted in the Convention's inability to fulfill its original purpose: global action against cybercrime.[207] In fact, a comprehensive study conducted by the UN Office of Drugs and Crime ("UNODC") concluded that "fragmentation at the international level" could "lead to the emergence of countrycooperation 'clusters'" which are not "well suited to the global nature of cybercrime."[208] China has already expressed concerns over U.S. "cyber dominance" and have even labeled this dominance as "cyber hegemony."[209] In its report, UNODC recommended that the international community work on developing a comprehensive multilateral instrument on cybercrime to remedy the deficiencies in the global cyber response.[210]

The Chinese government has made it clear that its primary concern is cyber sovereignty and information control.[211] Additionally, the Chinese are concerned about the perceived monopoly that the United States enjoys over the Internet and seems to have concluded that the United States has de facto control over the Internet.[212] In 2015, China and the United States engaged in a series of negotiations (known as Track 1.5 U.S.-China Cyber Security Dialogue) where the two nations discussed the future of cyberspace. Throughout the negotiations, the "Chinese emphasis on sovereignty in the information

[207] BOISTER, *supra* note 119, at 199.
[208] UNITED NATIONS OFFICE ON DRUGS AND CRIME, COMPREHENSIVE STUDY ON CYBERCRIME xi (2013) [hereinafter UNODC Report].
[209] HAROLD ET AL., *supra* note 157, at 9.
[210] UNODC Report, *supra* note 208, at xii.
[211] HAROLD ET AL., *supra* note 157, at 4.
[212] SWAINE, *supra* note 180.

sphere persisted" as did "China's perception that that United States dominated and would continue to dominate cyberspace."[213]

In accordance with concerns regarding Western dominance in the Budapest Convention and a mutual desire to strengthen sovereignty in cyberspace, China and Russia have proposed a new convention on cybersecurity.[214] While the language of the proposal seems innocuous on itsface, it poses a threat to the overall freedom and openness of the Internet through human rights violations and government control. Human rights organizations submitted a public letter to the UN General Assembly protesting the potential human rights violations of the proposed convention.[215] Specifically, the proposal prohibits "criminal purposes" in cyberspace, but does not define what those purposes are. Human rights organizations worry that this proposal could be used to criminalize "ordinary online behaviour [sic] that is protected under international human rights law," such as the ability to advocate for racial equality or criticize one's government.[216]

Additionally, the proposed treaty contains two specific provisions that run contrary to the interests and freedoms of U.S. citizens. The first issue would curtail freedom of speech on the Internet while the second would bring Internet governance and regulation under the exclusive control of sovereign nations. These general issues have already been targeted by critics of the proposed treaty.[217]

---

[213] HAROLD ET AL., *supra* note 157, at 49.

[214] Russia-China Proposal, *supra* note 131.

[215] *Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat toHuman Rights Online*, ASS'N FOR PROGRESSIVE COMMC'NS (Nov. 6, 2019), www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human [hereinafter Open Letter].

[216] *Id.*

[217] *State Department Official on Multilateral Cyber Efforts*, Special Briefing from the Office of the Spokesperson inthe Press Correspondents Room (Dec. 19, 2019), (transcript available at 2017-2021.state.gov/state- department-official-on-multilateral-cyber-efforts/index.html) [hereinafter State Department Official Speech].

First, the proposal specifically calls for "curbing dissemination of information that . . . inflames hatred on ethnic, racial, or religious grounds."[218] This language runs afoul of the First Amendment of the U.S. Constitution, which prohibits Congress from passing any law "abridging the freedom of speech."[219] While U.S. courts have upheld the constitutionality of criminalizing speech inciting violence, it is highly unlikely that the proposed text would pass constitutional muster.[220] For example, after mass shootings at New Zealand mosques in Christchurch shooting where fifty-one individuals were killed, the United States declined to support the Christchurch call to prohibit online extremism, which arguably inspired the shootings due to these same free speech concerns.[221]

Second, the proposal calls for "international governance of the Internet" by sovereign states, which effectively eliminates private companies from the conversation.[222] If this convention went into effect, the United States would likely not sign and ratify the treaty. However, if it did, it would require an unprecedented level of government oversight of private companies, like Facebook and Google, for the federal government to maintain the required level of control and "governance of the Internet." It is a cornerstone of U.S. policy that the federal government work hand-in-hand with private corporations to ensure the freedom and openness of the Internet.[223]

Finally, as pointed out by the Department of State, the non-controversial provisions of the Russia-China proposal are duplicative of the Budapest Convention.[224] The calls for cooperationand mutual assistance in deterring and prosecuting cybercrime are essentially the

[218] Russia-China Proposal, *supra* note 131, at § 2(4).
[219] U.S. CONST., amend I.
[220] A conversation regarding the criminalization of speech in the United States is beyond the scope of this paper. Forthe prevailing legal standard regarding criminal incitement, *see* Brandenburg v. Ohio, 395 U.S. 444 (1969).
[221] Tony Romm & Drew Harwell, *White House Declines to Back Christchurch Call to Stamp out Online Extremism Amid Free Speech Concerns*, WASH. POST. (May 15, 2019), www.washingtonpost.com/technology/2019/05/15/white-house-will-not-sign-christchurch-pact-stamp-out-online-extremism-amid-free-speech-concerns/.
[222] Russia-China Proposal, *supra* note 131, at § 2(8).
[223] National Cyber Strategy, *supra* note 160, at 6.
[224] State Department Official Speech, *supra* note 217.

same. These redundancies and specific issues make the proposal an untenable waste of resources; particularly to nations who support a truly free Internet where individuals can share thoughts without government interference.

Not only are there issues with the specific proposal by Russia and China, but there are issues with a new cyber convention in general. The first issue is that the negotiation of a new cyber convention will cost a huge amount of time and resources.[225] These resources should instead be allocated to efforts and projects assisting nations develop their cyber defense and practical ability to deter cybercrime.[226] Additionally, the Budapest Convention is, arguably, accomplishing its purpose—"there are 64 member-states that are members of it, and over 130 countries use it as the basis for how they govern cyber crime [sic]."[227] Despite accusations of being a failure, the Convention has served as a baseline for cyber strategies all over the world. Admittedly, the Convention requires some updating and should become more global in nature, but those concerns can be addressed, in part, through the two proposed changes to the Convention in the next two sections.

To come to a meeting of the minds regarding global cybersecurity, the United States mustrenew conversations with China, both formal and informal.[228] In 2015, then-President Obama struck an agreement with President Xi regarding the prevention of "cyber-enabled theft of intellectual property."[229] Economic espionage is one of the United States' greatest concerns.[230] As a result of the 2015

[225] "Building on and improving existing instruments is more desirable and practical than diverting already scarce resources into the pursuit of a new international framework, which is likely to stretch over many years and unlikelyto result in consensus." Open Letter, *supra* note 215.
[226] State Department Official Speech, *supra* note 217.
[227] *Id.*
[228] Formal and informal law enforcement cooperation in 2014 resulted in the arrest and conviction of several cybercriminals. *See* Ron Cheng, *Prospects for U.S.-China Cybercrime Cooperation: The Road Thus Far*, LAWFARE (Mar. 9, 2017), www.lawfareblog.com/prospects-us-china-cybercrime-cooperation-road-thus-far.
[229] John W. Rollings et al., *U.S.-China Cyber Agreement*, CRS INSIGHT (Oct. 16, 2015),fas.org/sgp/crs/row/IN10376.pdf.
[230] Frank J. Cilluffo et al., *A Blueprint for Cyber Deterrence: Building Stability Through Strength*, 4 MIL. & STRATEGIC AFFS. 3, 10-11 (2012).

agreement, Chinese cyber activity is occurring "at lower volumes than existed before the [agreement]."[231] While China still engages in cyber operations targeting the United States, these operations do not seem to violate the agreement. This agreement wasphrased very specifically to ensure the United States could also continue cyber operations without violating the agreement.[232] Even though Chinese cyber operations continue to pose a national security threat to the United States, the fact that the limits of this agreement have had a real-world impact on China's operations constitutes a ray of hope for mutual trust and understanding moving forward; first with bilateral agreements (like the 2015 agreement) then multilateral agreements (like the Budapest Convention).

In order to start down the road to true global cooperation, the United States must work with China and like-nations to determine how to best address their concerns while still ensuring the needs of the United States and its allies are also met. This can only be accomplished through diplomatic means as well as formal and informal cooperation. While accounting for differences in culture and legal systems[233] will, admittedly, limit the reach of the Convention, it is the only way to ensure the Convention actually constitutes a global response to cybercrime and to prevent the formation of "country cooperation clusters."[234]

b. New Proposal to Amend Membership Protocol

Under the Convention, to admit a new, non-CoE member, there must be a "unanimous consent of the Contracting States."[235]

---

[231] Herb Lin, *What the National Counterintelligence and Security Center Really Said About Chinese EconomicEspionage*, LAWFARE (July 31, 2018), www.lawfareblog.com/what-national-counterintelligence-and- security-center-really-said-about-chinese-economic-espionage.

[232] *Id.*

[233] There are three distinct global legal systems: civil law, common law, and Islamic law. A significant percentage ofUN member nations (28%) employ a mixed system. For example, "Chinese criminal law has been influenced by a range of legal systems with the judiciary retaining important power to give binding judicial interpretations of law." *See* UNODC Report, *supra* note 208, at 57, n.21.

[234] *Id.* at xi.

[235] Budapest Convention, *supra* note 112, at art. 37(1).

Pursuant to the CoE's Treaty Office of the Directorate of Legal Advice and Public International Law, the decision regarding an invitation must "be unanimously agreed by those Council of Europe members which have ratified the Convention."[236] The Convention further requires that the Committee of Ministers of the Council of Europe must issue an invitation to the proposed member.[237] A non-CoE nation has five years to accept the invitation before it lapses.[238] These requirements impose an onerous burden on any non-CoE nation seeking to join the Convention and sets the balance of power in favor of those nations already party to the Convention.

By contrast, to join the UN, an applicant presents their request to the UN Secretary-General along with a letter stating that the nation accepts the obligations of the UN Charter.[239] The Security Council as well as the General Assembly consider the membership and vote on the applicant's admission.[240] To pass in the Security Council, an applicant needs nine of the fifteen member states to approve (with no veto from any of the five permanent members).[241] In the General Assembly, an applicant needs two-thirds of the body to vote in favor of admission.[242] While the UN admission process is rigorous, it is self-initiated by the perspective member anddoes not require a unanimous vote to permit admission.

In order to encourage new member states to join the Convention, the admission process should be updated to reflect the UN model and eliminate the membership preference for CoE nations. The UN model is already accepted by the international community and has been for decades. The Convention faces enough challenges to

---

[236] DIRECTORATE OF LEGAL ADVICE AND PUBLIC INTERNATIONAL LAW, *Accession by States which are not member States of the Council of Europe and which have not participated in the elaboration of the Convention* ¶ 3 ETS No. 185 (2018), rm.coe.int/16808ff396 [hereinafter Accession of non-CoE Members].

[237] Budapest Convention, *supra* note 112, art. 37(1).

[238] Accession of non-CoE Members, *supra* note 236, at ¶ 4.

[239] *About UN Membership*, UNITED NATIONS, www.un.org/en/about-us/about-un-membership#:~:text=Membership%20in%20the%20Organization%2C%20in,to%20carry%20out%20these%20obligations%E2%80%9D (last visited Feb. 8, 2022).

[240] *Id.*

[241] *Id.*

[242] *Id.*

its relevance without the administrative rigmarole of a needlessly burdensome admission process. For the Convention to truly constitute a global stance against cybercrime, the United States (and other Convention members) need to indicate their willingness to open the dialogue with all nations through a more relaxed membership process. Amendment of the membership protocol is a simple gesture which indicates the more open nature of the Convention.

The membership provisions of Article 37(1)-(2) should be combined and amended toread as follows:

> After the entry into force of this Convention, any State which desiresto become a Member to the Convention shall submit an applicationto the Secretary General for the Council of Europe. Such applicationshall contain a declaration, made in a formal instrument, that the State in question accepts the obligations contained in the Convention. The Contracting Members shall consider whether the applicant is willing to carry out the obligations contained in the Convention. After consulting with and obtaining the consent of two-thirds of the Contracting States to the Convention, the Secretary General shall inform the applicant State of the decision of the Contracting States, made in a formal instrument. The applicant State shall become a member upon receipt of the formal instrument of acceptance.

This proposed amendment closely mirrors the existing language of the Convention with additions from the text of the UN Charter. The amalgamation of the membership protocols should allow for a fairly seamless application due to the consistency of the general process with changes only to the majority required for admission (two-thirds as opposed to unanimous). If, for example, China decided to join the Convention under this proposed membership protocol, the government would no longer have to wait for an invitation. Instead, China's government could submit a letter to the CoE Secretary General indicating their intention and willingness to adhere to the Convention's obligations. The Secretary General would then consult with all Contracting States (not just CoE members) and, if two-thirds concur, inform China that their membership request is approved. Pursuant to existing Convention

language, China would then become a full member of the Convention on the day it receives notification of its acceptance.

It is likely that the CoE States will oppose amendment to the membership protocol. Afterall, the Convention is the brain-child of the CoE and the membership protocol was drafted to give the CoE added control over membership, and consequently the direction, of the Convention. In its current form and membership composition, the Convention can meet theneeds of similarly-minded nations and thus specifically address the goals and priorities of those nations, making it a more effective tool against cybercrime. Opening membership to nations with different goals and priorities will limit the Convention's reach and prevent its deterrent effect.

However, the fact that the Convention is controlled primarily by Western nations inhibits its ability to act as a *global* check on cybercrime.[243] In reality, the Convention's membership is two-thirds CoE States with the remainder of member-states comprised of like-minded allies. If the CoE truly intends this document to guide the global fight against cybercrime, all members of the global community, particularly nations with different priorities, must become party to the Convention. If the Convention is limited to like-minded nations, then other nations not party to the Convention will engage in their own agreements thus resulting in fragmentation and countrycooperation clusters which will hinder the global fight against cybercrime.[244]

Thus, the Convention's original membership protocol should be amended to reflect the above proposed membership procedure. Instead of unanimous approval coupled with an invitation requirement, membership of the Convention should allow the applicant to initiate the membership process and require a two-thirds majority approval, similar to the UN membership process. This

[243] The text of the Convention is not even publicly available in Mandarin, making this translation available is another small but mighty step that the Convention can take in furtherance of being considered a truly global stanceagainst cybercrime. *See Convention of Cybercrime*, COUNCIL OF EUROPE, www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Feb. 21, 2021).

[244] UNODC Report, *supra* note 208, at xi.

amendment would constitute a subtle, but important, shift in the power dynamic ofthe Convention away from a Western-focus to a truly global perspective.

c. Problems with Proposed Additional Protocol II

The negotiations regarding AP II are active and ongoing. As previously discussed, the Chinese government, among others, already perceive the Convention as being oriented toward Western priorities and ideologies. In order to rectify this perception, the United States should adopt existing calls for the AP II negotiations to be delayed. Instead of pursuing a substantive additional protocol, the United States should sponsor the above amendment to membership protocol and allow other nations (including China) to apply for membership and join before passing any additional substantive protocol to the Convention. This delay will allow new member-nations (such as China and Russia) to provide meaningful input to AP II which will allow the protocol to reflect global concerns and priorities.

The delay in adopting AP II is especially necessary given the status of the current proposed text. As written, the new protocol creates new issues with the Convention and will only increase China's existing concerns regarding membership. Articles Four and Five of AP II are ofmost concern. Both provisions relate to the expansion of mutual legal assistance requirements among member-states. Article Four, as written, requires the disclosure of a broad scope of information transfer between member states.[245] Article Five requires member-states to give immediate effect to orders from other nation-states.[246] The issues with the text of these provisions boils down to two primary concerns: (1) the broad category of required information disclosure; and (2) lack of contact with the host nation regarding requests.

Supporters for these provisions, such as the Protocol Drafting Group, argue that they are necessary to combat the rapidly evolving

[245] AP II, *supra* note 127.
[246] *Id.*

area of cybercrime.[247] The process of information sharing under traditional information sharing schemes (such as mutual legal assistance treaties) are too cumbersome and simply cannot keep up with the speed of cybercrime. For example, data modification constitutes a significant hurdle when it comes to using evidence in criminal court proceedings.[248] Cybercriminals often employ techniques to cover their digital tracks which make it more difficult to find incriminating data.[249] The longer it takes for law enforcement to access an infected computer system, the more difficult it is to properly reconstruct the digital crime scene. Thus, by the time a mutual legal assistance request is tendered to a foreign nation's government and answered, the information sought may be impossible for investigators to piece together in a useable format.

As previously discussed, cyber sovereignty is one of China's top concerns. Article Fourof AP II increases mutual legal assistance in regard to cybersecurity. In the context of cybercrime, seamless cooperation and information sharing is vital to gathering evidence and holding perpetrators accountable.[250] However, the level of cooperation and information sharing required by the Convention should establish the proverbial floor of cooperation in cyberspace, which includes the global concerns of China and its allies. The other nations privy to the Convention can utilize bilateral mutual legal assistance treaties specifically tailored to cybercrime which can rise above the floor set by the Convention.

The broad category of information disclosure under the proposed AP II should be concerning even to the United States. While it is important to deter cybercrime and hold hackers responsible, it is

[247] The Protocol Drafting Group is a working group comprised of approximately thirty Convention party memberstasked with drafting the proposed additional protocol. *See Protocol Negotiations*, COUNCIL OF EUROPE, www.coe.int/en/web/cybercrime/t-cy-drafting-group.

[248] *Practical Aspects of Cybercrime Investigations and Digital Forensics*, UNDOC, www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html (last visited Jan.29, 2021).

[249] *Id.*

[250] Allison Peters & Amy Jordan, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity onCybercrime*, 10 J. NAT'L SEC. L. & POL'Y 487, 502 (2020).

equally important that law enforcement not lose sight of potential civil liberties violations. As written, under AP II members of the Convention can request the subscriber's identity, payment information, type of communication service used, physical address, and static and dynamic IP addresses.[251] While the content of a communication is not included in this data dump, the level of information required by this provision should be more narrowly tailored to limit the unnecessary dissemination of personal data. The provision does contain an optional process for notification to the receiving nation which should alleviate some of China's sovereignty concerns.[252] However, China should be able to opine on this provision as a memberof the Convention before it is ratified and implemented.

While the Contracting States cannot wait indefinitely for China to accede to update the Convention's provisions, they should avoid taking steps which continue to alienate China and other like-minded nations in the interim. While there is no guarantee that China will ever become a member of the Convention, the establishment of an international cybersecurity regime can be analogized to the establishment of the nuclear arms control regime. Similar to nuclear weapons, mutual vulnerability to cybercrime and cyberattacks will likely lead nations to develop "rules, norms, and standards of behavior that brought order to what was highly contested and valuable terrain."[253] This process will take time and effort, but a unified cybersecurity regime would "mitigate uncertainty, strengthen legal liability, and reduce transaction costs related to the use of cyberspace."[254]

The second provision (lack of contact with the host nation) is, again, an ideal to eventually strive for, but something that is not practically feasible right now. This provision is similar to the recently

[251] Jennifer Daskal & Debrae Kennedy-Mayo, *Budapest Convention: What Is It and How Is It Being Updated?* CROSS-BORDER DATA FORUM (July 2, 2020), www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/#_edn23.
[252] AP II, *supra* note 127, at art. 4.2
[253] Polly M. Holdorf, *Prospects for an International Cybersecurity Regime*, U.S.A.F. INST. FOR NAT'L SEC. STUD. 11 (2015) (internal citation omitted).
[254] *Id.*

passed CLOUD Act, which permits law enforcement agencies to directly contact service providers for stored communications without going through the host nation.[255] Those agreements are negotiated on an individual basis with nations that meet U.S. standards for due process and law enforcement tactics. To date, there is only one agreement in effect.[256]

While obviating the need to contact the host nation directly saves precious time when it comes to law enforcement efforts, this step is indisputably an encroachment on a nation's traditional sovereign ability to regulate law enforcement in their own territory. As indicated by the tedious and lengthy negotiations involved in the CLOUD Act,[257] this step requires an enormous amount of trust and mutual understanding between nations. While reaching this level should be a global objective, there is currently too much diversity in position and opinion for it to be a viable option for all Convention members at this point.

This type of information-sharing provision can be individually negotiated through bilateral mutual legal assistance agreements, but it is not feasible to apply to the entire Convention. Mutual legal assistance agreements constitute a legally binding process between governments intended to facilitate information sharing in regard to criminal activities.[258] Thefact that this provision is on the

[255] U.S. Dep't of Just., *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (2019), www.justice.gov/opa/press-release/file/1153446/download.

[256] Press Release, U.S. Dep't of Just., U.S. and U.K. Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019), www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

[257] Theodore Christakis & Fabien Terpan, *EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges, and EU Law Procedures and Options*, 11 INT'L DATA PRIVACY L. 81, 81-82 (There have been four rounds of negotiations between the nations and "[t]here are strong divergences between the EU and the US about what the scope and the architecture of this agreement should be.").

[258] While the mutual legal assistance treaty ("MLAT") constitutes a legally binding process, the existence of an MLATdoes not guarantee that the requestor nation will receive the requested information. Typically, MLATs provide limited grounds for declining to act on a request. DAVID J. LUBAN ET. AL., INTERNATIONAL AND TRANSNATIONAL CRIMINAL LAW 398 (3rd ed., 2019).

table demonstrates the like-mindedness of the current Convention members, which betrays its exclusion of certain members of the global population.

Thus, AP II should include a process for expedited information requests from a foreign country. However, this process must be based on trust and mutual understanding. In order to reach that level with nations like China, the United States should strengthen its formal and informal law enforcement cooperation efforts with China and building that trust. These mutual legal assistance provisions, which should be rapid but allow for appropriate review, will addressChina's concern over information control while allowing the prosecution of bad actors in cyberspace. Reinforcing certain notions of cyber sovereignty demonstrates that the United States takes China's concerns seriously and will assist in fostering a future of cooperation and stability in cyberspace while also protecting U.S. citizens and U.S. interests in cyberspace.

2. U.S. Participation in International Standard Setting Organizations

a. Participation of Private American Industry

Standard-setting organizations form the foundation of the international community's response to emergent global issues, including cybersecurity and developing technologies. In thecontext of 5G, global consensus standards and specifications are informed by almost 600 member-organizations working together to ensure interoperability between networks and devices.[259] Despite the Department of Commerce promulgating a new rule allowing U.S. companies to participate in certain standard-setting bodies where Huawei is also a member, the negotiations and discussions concerning the standards for 5G continued during the United States' year-long absence from the process which, arguably, left the United States with some catching up to do.[260]

[259] AT&T Policy Primer, *supra* note 67.
[260] Schwartz, *supra* note 81.

While U.S. businesses were waiting on clarification from the Department of Commerce, the process of developing and standardizing 5G technology continued moving forward. Particularly, between May 2019 and early 2020 (before the onset of COVID-19), 3GPP did a great deal of development for Releases 16 and 17. Release 16 was frozen before the Department of Commerce amended the EAR thus prohibiting U.S. companies from participating in any last-minute revisions to the Release.[261] Additionally, the initial Release 17 package was approved at the end of 2019, which prevented U.S. companies from contributing to that process.[262]

However, the damage may not be as grave as initially feared. While Huawei was able to take advantage of U.S. companies' absence from the process, U.S. companies, particularly technology giant Qualcomm, had already laid a substantial foundation for the future of 5G before the Department of Commerce initiated the ban. In fact, Qualcomm "played a critical role" in Release 16 regarding 5G technical specifications for 5G New Radio technology.[263] Discussions regarding Release 17 (the next big step in 3GPP's 5G specification decisions) began before the Department of Commerce initiated its ban, which allowed Qualcomm and other U.S. companies to participate in framing the specifications for Release 17. Furthermore, continued discussions regarding Release 17 were delayed until December 2020.[264] At that time, 3GPP approved a timeline to freeze Release 17 in June 2021.[265] Thus, Qualcomm and other U.S. companies were able to rejoin the conversation before 3GPP moves to the final decision phase of Release 17.

It is essential that U.S. companies, such as Qualcomm, Intel, and AT&T, rejoin these standard-setting bodies and participate in the

[261] *Release 16*, 3GPP, www.3gpp.org/release-16 (last visited Jan. 28, 2021).
[262] *Id.*
[263] Yang, *supra* note 14, at 16.
[264] Discussions were delayed due to the "continued need for virtual e-meetings, instead of physical meetings." *Release 17*, *supra* note 24.
[265] Assuming that physical meetings resume in June 2021. "After freezing, a Release can have no further additionalfunctions added. However . . . a considerable number of refinements and corrections can be expected for at least twoyears following this date." *Releases*, *supra* note 15.

development of international norms and procedures for 5G.[266] If China is allowed to continue dominating submissions and maintaining its monopoly on leadership positions in these organizations, China will be in a position to replicate the U.S. leadership and command of the 4G systems.[267] China's National Informatization Strategy calls on China's technology companies to facilitate the development of digital infrastructure that "strengthens China's points of control in the digital economy."[268] China owns a significant percentage of the essential 5G-related patents.[269] If China's technology sector is able to exercise control over the international 5G standards, China's influence over the system, in both physical technology and standards, will be cemented. With U.S. companies back in the fray, reclaiming leadership positions and increasing standards submissions, China's hold over the technology will be weakened.

Qualcomm's role as a chipset vendor relegates the company to a more limited role than infrastructure vendors, such as Huawei.

[266] Qualcomm, Intel, AT&T, and U.S. Cellular are the American companies which contribute the most to 3GPP at this point in time. Their contributions are still moderate compared to other companies, such as Huawei and Ericsson.*See* Mike Sullivan-Trainor, *3GPP Contributions Analysis*, OMDIA TECH (12 Oct. 2020), omdia.tech.informa.com/-/media/tech/omdia/brochures/service-providers/omdia_3gpp_2020_contribution_white-paper.pdf; *but see* Antonio Villas-Boas, *The US is Making its Own 5G Technology with American and European Companies, and Without Huawei*, BUS. INSIDER (Feb. 4, 2020), www.businessinsider.com/5g-huawei-white-house-kudlow-dell-microsoft-att-nokia-ericsson-2020-2. (Explaining that the U.S. government has indicated that other companies, such as Microsoft and Dell, will be principal players inconstructing America's 5G infrastructure, specifically the software aspect of the technology rather than the hardware. These companies have not made any discernable contributions to 3GPP standards).

[267] Nicol Turner Lee, *Navigating the U.S.-China 5G Competition*, BROOKINGS INST. (Apr. 2020), www.brookings.edu/research/navigating-the-us-china-5g-competition/.

[268] Sangeet Paul Choudary, *China's Country-as-Platform Strategy for Global Influence*, BROOKINGS INST. (Nov. 19, 2020), www.brookings.edu/techstream/chinas-country-as-platform-strategy-for-global-influence/.

[269] Robyn Mak, *Breakingviews – China's Huawei Holds a 5G Trump Card*, REUTERS (July 27, 2020), www.reuters.com/article/us-huawei-tech-5g-security-breakingviews/breakingviews-chinas-huawei-holds-a-5g-trump-card-idUSKCN24S09Y.

However, Qualcomm's participation remains vital.[270] Qualcomm and other U.S. companies retain the ability to comment and influence the process as long as they are part of the 3GPP conversation. Qualcomm specifically has "a rich history of building consensus" for new directions technology since 3GPP's inception in 1998.[271] If the aforementioned U.S. companies abandon these conversations, the U.S. private sector would completely lose its voice in the global 5G standardization process.

Additionally, while 5G infrastructure is of immediate concern (as addressed in Subsection B, Domestic Issues and Enforcement),[272] "5G is the conversion to a mostly all-software network, future upgrades will be software updates."[273] After the establishment of the initial 5G infrastructure (an admittedly crucial first step), future upgrades to the system will rely on software development, a traditionally U.S. -dominated industry.[274] In order to ensure U.S. voices are heard in the requirements for 5G specifications as well as future technologies, U.S. companies must continue and increase participation in standard-setting organizations, such as 3GPP.

b. U.S. Government Participation

While private U.S. corporations re-enter with 3GPP, the U.S. federal government has recently butted heads with an international standard-setting organization that it previously supported, the ITU. In August 2020, the Federal Communications Committee ("FCC")

[270] Yang, *supra* note 14.
[271] Lorenzo Casaccia, *Demystifying 3GPP – An Insider's Perspective to How 4G and 5G Standards Get Created*,ONQ BLOG (Aug. 2, 2017), www.qualcomm.com/news/onq/2017/08/02/demystifying-3gpp-insiders-perspective-how-4g-and-5g-standards-get-created.
[272] *See* discussion *infra* Section III.B.
[273] Wheeler & Simpson, *supra* note 11.
[274] Andes & Muro, *supra* note 50.

completed its first 5G Spectrum Auction.[275] The ITU, however, deferred its decisionregarding spectrum usage until 2023.[276]

Some scholars believe that this deviation from the ITU will be counter-productive in the long run. Specifically, they believe that incorporation of individual nations' national security concerns into the ITU's process will trigger conflict and gridlock within the ITU while challenging the efficacy and legitimacy of the ITU as an organization.[277] Additionally, the United States' unilateral spectrum allocation will likely cause interoperability issues with the new technology as devices from different nations could operate on different ranges of the spectrum.[278] The ITU's position as a unifying global force could be doomed to failure because of the United States' unilateral spectrum allocation.

While this divergence from international cooperation was not ideal, it was, in many ways,necessary to protect U.S. interests. As previously discussed, there are numerous viable national security threats posed by the 5G rollout. In order to ensure the protection of U.S. interests in cyberspace, the Federal Communications Commission ("FCC") obviated any further delay from the ITU in U.S. spectrum allocation. The FCC took this step because other countries had already moved forward with their own 5G spectrum allocation and the United States was quickly falling behind.[279] Instead of waiting three more years to determine the ITU's approved 5G spectrum

[275] Jon Reid, *FCC Ends 5G Spectrum Auction After Raising $4.5 Billion*, BLOOMBERG L. (Aug. 25, 2020), news.bloomberglaw.com/tech-and-telecom-law/fcc-ends-5g-spectrum-auction-after-raising-4-5-billion.

[276] World Radio Conference, Res. 235, *Review of the Spectrum Use of the Frequency Band 470-960 MHz in Region1*, (2015), www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000C0029PDFE.pdf.

[277] Rob Frieden, *The Evolving 5G Case Study in United States Unilateral Spectrum Planning and Policy,* 44 POL'Y TELECOMM. 1, 6-7 (Oct. 2020).

[278] *Id.* at 6.

[279] Other nations have already solidified their 5G plans and are prepared to allocate more than five times mid-bandspectrum than the United States. Half of the world's 5G connections are currently in China. *See* Roslyn Layton, *COVID Will Not Delay the FCC's 5G Spectrum Auction*, FORBES (Aug. 7, 2020), www.forbes.com/sites/roslynlayton/2020/08/07/covid-will-not-delay-the-fccs-5g-spectrum-auction/?sh=354d46138bd6.

allocation and thus continuing to lose the edge in the 5G rollout, the FCC held a spectrum auction and began the process of ensuring available bandwidth for the U.S. rollout of 5G.[280] This auction will ensure that the United States is prepared to support U.S. citizens' need for 5G once the technology is prepared for full implementation.

In addition to the spectrum allocation auction, the FCC has called for the United States to consider whether it should continue participating in the ITU at all due to the subversive influence of nations seemingly set against U.S. interests. To that end, FCC Commissioner Michael O'Rielly suggested that the United States should "explore the formation of a G7-like organization or loose coalition of leading wireless nations, as an alternative to the ITU."[281] Commissioner O'Rielly further stated that "[n]ear-global harmonization could be achieved through agreement of the largest, leading wireless nations of the world."[282] Such an organization would be smaller and able to make important decisions in a timelier fashion than the glacial ITU and its 193 member states. Moving to a more streamlined approval process would allow the United States to maintain and secure dominance in the global technology market for years to come. Thus, the United States would be able to influence global 5G spectrum allocation through a new organization instead of slogging through the politics and bureaucracy of the ITU.

However, the creation of a G7-type organization is not feasible. The ITU is currently comprised of 193 member nations in addition to approximately 700 private-sector entities.[283] Commissioner O'Rielly's comments describe an attempt to harm U.S. interests at the World Radio Conference. As demonstrated throughout the ITU's history, it takes time to come to an agreement with so many member-states. While the ITU's decisions are not

[280] *Id.*

[281] *Accountability and Oversight of the Fed. Commc'ns Comm'n: Hearing Before the Subcomm. on Commc'ns &Tech. of the H. Comm. on Energy & Com.*, 116th Cong. 2 (2019) (statement of Michael O'Rielly, FCC Comm'r).

[282] Bevin Fletcher, *FCC's O'Rielly Suggests "G-7-like" Alternative to ITU*, FIERCE WIRELESS (Jan. 17, 2020), www.fiercewireless.com/regulatory/fcc-s-o-rielly-suggests-g7-like-alternative-to-itu.

[283] *About International Telecommunication Union (ITU)*, *supra* note 70.

legally binding, many nations consider the ITU's decisions as treaty-like, creating a significant perceived obligation stemming from ITU's decisions.[284] If several of the largest and IT heavy nations were to leave the ITU and create their own organization, it would cause a permanent rift in the international community. Additionally, the ITU is part of the UN. Leaving a UN organization to create an independent (and presumably mostly Western) association would essentially constitute a vote of no confidence in the UN and what it stands for: global cooperation.

If the United States pulled out of the ITU and formed its own organization, the global ramifications would likely be disastrous. Currently, China is a member-nation of the ITU. If the United States spearheaded a new organization along with its Western allies, China would likely see this as a power move intended to reinforce U.S. dominance in cyberspace.[285] The fact that the United States has already taken unilateral steps toward a 5G spectrum plan will only reinforce and give weight to that perception. A U.S. withdrawal from the ITU along with its allies would likely result in the discreditation of the ITU as a truly global organization. It would also likely result in the creation of a similar organization with China and its allies (including Russia) to create their own 5G standards and regulations resulting in a global divide for current 5G and future developments in this area.

The United States needs to protect its interests, but also ensure the successful globalization of 5G technology. To ensure the continued global standardization of 5G spectrum policy, the United States must continue participating in the ITU. Despite alleged efforts by Russia, China, and even France to delay agenda items from moving forward,[286] the United States should use diplomatic channels to garner support for mutually advantageous decisions regarding 5G. These diplomatic efforts and conversations in advance of the next World Radio Conference could assist in cutting off some of these objections

[284] Robert Frieden, *Win, Lose, and Draw: Outcomes from the 2019 World Radio Conference* (July 27, 2020),ssrn.com/abstract=3661880.
[285] Even though China has already laid the framework for its own spectrum allocation. *See* Layton, *supra* note 279.
[286] Statement of Michael O'Rielly, *supra* note 281.

and arguments and make the next Conference more protective for U.S. interests. U.S. diplomatic and humanitarian efforts are vital to creating global harmony and buy-in for a 5G standardized plan for that supports U.S. interests and allows the United States to preserve its role in cyberspace and the technology industries.

If there is global division regarding the specifications and standards relating to 5G, it could result in the disruption of global services.[287] If the United States is truly interested in ensuring the future of the Internet and global technology remains status quo, then the United States needs to invest in that future. The United States can still recover from this divergence from international standard-setting organizations, both in the public and private spheres. It is essential that private companies, like Qualcomm, continue to work and cooperate with 3GPP and others. Likewise, the U.S. government should use diplomatic means and incentives to create global buy-in for its spectrum utilization plan to protect U.S. interests while ensuring the future of 5G is open, interoperable, reliable, and secure.[288]

B. Domestic Issues and Risk Management

In 2018, Congress created CISA, which acts as a cybersecurity coordinator at an organizational level.[289] In order to unify the diverse responsibilities and functions performed by each department and agency, the U.S. government should take steps to use CISA as an even stronger unifying force and elevate the director of CISA to lead all cyber responses and efforts. As recommended by the Cybersecurity Solarium Commission ("CSC"), CISA can act as a focal point to ensure that all government agencies are up to date with cyber hygiene procedures as well as coordinate risk management efforts across the cyber spectrum.[290] However, Congress should not have adopted the recommendation of the CSC regarding the creation of an NCD, rather, it should have given CISA additional time to assess the situation before moving forward with the NCD position.

---

[287] *Id.*
[288] National Cyber Strategy, *supra* note 160.
[289] CISA Act, *supra* note 143.
[290] CSC Final Report, *supra* note 151, at 3.

The U.S. government, through CISA, must improve working relationships with private industries regarding cybersecurity. To that end, Congress should institute mandatory reporting of all data breaches among private business entities as suggested by FBI Director, Christopher Wray.[291] Currently, corporations are eager to conceal breaches, when legally possible, to protect consumer confidence as well as their investors. However, data breaches will occur. This is a fact, and, in modern times, it is part of doing business. Mandatory reporting will increase the amount of information available to the federal government at an earlier time and it will help prevent additional companies falling prey to the same attack. Currently there are calls for a tax break for small businesses to incentivize cybersecurity, but a broader stance regarding proposed tax breaks for all corporations who comply with cyber hygiene standards will ease the cost of cybersecurity and mitigate damage from future cyberattacks.[292]

Finally, the United States must establish risk management policies and secure the 5G supply chain. In furtherance of this goal, the United States has already partnered with Japan and Australia to create international standards for infrastructure projects.[293] The United States has also imposed effective prohibitions regarding use of Huawei technology in the United States but should answer existing calls to reassess the export licensing requirements on technology, commodities, and software being exported to Huawei and its subsidiaries. Reassessing these prohibitions and export control requirements is essential to reducing tensions between China and the

[291] Miller, *supra* note 203.

[292] Currently, there is a business tax credit available for companies who invest in cyber-related research and development. That credit should be expanded to businesses who meet a set standard regarding cybersecurity and cyber hygiene. *See* Yair Holtzman & Melissa Cohen, *Insight: Save Money While Fighting Cyberattacks*, BLOOMBERG TAX (Dec. 11, 2018), www.anchin.com/uploads/1413/doc/BNA-Cybersecurity_122018.pdf.

[293] *The U.S., Australia and Japan Announce Trilateral Partnership on Infrastructure Investment in the Indo-Pacific*, U.S. Embassy & Consulates in Australia, July 30, 2018, au.usembassy.gov/the-u-s-australia-and-japan-announce-trilateral-partnership-on-infrastructure-investment-in-the-indopacific/.

United States and will not have an appreciable impact on U.S. national security interests as the sanctions have already had the intended effect.

1. Reforms to Domestic Organizational Structure

As previously discussed, there are at least eight departments and several subsidiary agencies responsible for cybersecurity in the United States. The creation of CISA was a step in the right direction, the creation of a single point of contact for risk management and critical infrastructure defense. However, CISA should have an even larger role in shoring up andunifying U.S. cyber efforts. Furthermore, the Director of CISA should become the new de facto cybersecurity coordinator or NCD. As with the previous cybersecurity coordinator, the CISA director would be responsible for heading up all major cyber response efforts and coordinating budget requests amongst all cyber components to prevent redundancies and ensure maximum efficiency and resource utilization.

Instead of relying on CISA, there are many proponents for the creation of a new cyber entity, namely an Office of the NCD.[294] Proponents of the NCD position, most notably the CSC, argue that it will act as a unifying factor and create much needed coordination across the federal government in the cyber domain.[295] Since the removal of the cyber coordinator position, the senior director of the National Security Council Cyber directorate has filled the duties previouslyperformed by the cyber coordinator.[296] However, a recent Government Accountability Office report highlighted the continuing lack of leadership as follows: "Without effective and transparent

[294] There have even been calls to create a Department of Cybersecurity or to refocusing the Department of Homeland Security (DHS) solely on CISA's mission by sending "the other entities…back to their former homes and CISA is DHS." Charlie Mitchell, *National Cyber Director Debate Raises Broader Issue: Is a Major Overhaul Needed at DHS?* INSIDE CYBERSECURITY (July 24, 2020), insidecybersecurity.com/share/11468.

[295] Sen. Angus King & Rep. Mike Gallagher, *United States of America Cyberspace Solarium Commission*, U.S. CYBERSPACE SOLARIUM COMM'N (March 2020), www.solarium.gov/report [hereinafter CSC Report].

[296] *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GOV'T ACCOUNTABILITY OFF., GAO-20-629 (Sept. 2020), www.gao.gov/assets/gao-20-629.pdf.

leadership that includes a clearly defined leader, a defined management process, and a formal monitoring mechanism, the executive branch cannot ensure that entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and ultimately overcome this urgent challenge."[297]

However, the creation of yet another cyber-focused federal entity is premature. CISA was only recently created and has not yet had sufficient time to establish itself or test its capabilities, resources, and potential for expansion. Pursuant to the CSC report, CISA should be provided with extra resources to fulfill its many mission objectives. These objectives include incident management and recovery; national risk management; cyber defense and security collaboration; and continuous threat hunting.[298] According to the report, CISA is currently underfunded for its mission,[299] which demonstrates the logical fallacy and prematurity in establishing another entity. Before Congress creates a new position and agency, the current agencies must be properly resourced to avoid the creation of multiple and potentially redundant entities all of which are underfunded and unable to perform their designated functions.

Recently, the CSC published its report and recommended that, in addition to strengthening CISA, Congress establish the NCD position to manage "the integration of cybersecurity policy and operations across the executive branch."[300] The 2021 NDAA contains a provision requiring the immediate establishment of an NCD position within the Executive Office of the President.[301] Initially, there were two versions of the NDAA, one proposed by the Senate, which required investigation into the creation of the NCD position, and another proposed by the House, the final provision, requiring the immediate creation of the position.[302] The U.S. Chamber of

[297] *Id.*
[298] CSC Report, *supra* note 295, at 40-41.
[299] *Id.* at 39.
[300] *Id.* at 37.
[301] 2021 NDAA, *supra* note 152, at § 1752.
[302] Maggie Miller, *Senate Approves Defense Bill Establishing Cyber Czar Positions, Subpoena Power for Cyber Agency*, THE HILL (Dec. 11, 2020),

Commerce, amongst other entities, supported the immediate implementation of the NCD position.[303]

The NCD provision in the 2021 NDAA should not be implemented because the Office of the NCD would actually take away from CISA's influence as the newly ensconced NCD would "clear some bureaucratic space by asserting authority."[304] As previous critics have pointed out, while it is of paramount importance that there be coordination of cyber efforts at the highest level, the utilization of an existing position, such as the CISA director, to provide that necessary coordination is more efficient and reasonable than "introducing excessive bureaucracy from a standalone agency."[305] In sum, the federal government and lawmakers need to give CISA more time to get its feet off the ground. While it is understandable that the CSC made such a recommendation, the inclination will only overwhelm an already overwhelmed area. There are too many proverbial cooks in the U.S. cyber-kitchen.

Instead of creating an NCD, the President should implement the novel solution of makingthe CISA director the new cybersecurity coordinator. To that effect, the President should issue an Executive Order requiring that all executive cyber agencies, bureaus, and entities report to the Director of CISA to unify the U.S. cyber response. The Director of CISA should have a direct line to the President. This direct access would ensure that the President is given the full picture regarding U.S. posture and capability in cyberspace and enable the President to make informed decisions regarding cyber policy and

www.thehill.com/policy/cybersecurity/529888-senate-approves-defense-bill-establishing-cyber-czar-position-subpoena.

[303] Letter from Neil L. Bradley, EXEC. VICE PRESIDENT. & CHIEF POL'Y OFF., to Members of the FY21 NDAA Conference Committee (Oct. 2, 2020), www.uschamber.com/assets/documents/201002_fy21ndaa_conferees.pdf.

[304] Philip R. Reitinger, *Establishing a National Cyber Director Would Be a Mistake*, LAWFARE (July 17, 2020),www.lawfareblog.com/establishing-national-cyber-director-would-be-mistake.

[305] Suzanna Spaulding & Mieke Eoyang, *Bad Idea: Creating a U.S. Department of Cybersecurity*, CTR. FOR STRATEGIC & INT'L STUD. (Dec. 2018), www.csis.org/analysis/bad-idea-creating-us- department-cybersecurity.

response. The introductory text of the Executive Order should contain words to this effect:

> Subject to the authority, direction, and control of the President, the Director of the Cybersecurity & Infrastructure Security Agency (Director) shall serve as the head of the cybersecurity community, act as the principal advisor to the President, and shall oversee and direct the implementation of the National Cyber Strategy and execution of the Nation Cybersecurity budget. The Director will lead a unified, coordinated, and effective cybersecurity effort. The Director shall take into account the views of the heads of departments containing an element of the nation's cybersecurity response.[306]

Cybersecurity is critical to national security and should be treated as such within the federal government organizational structure.[307] Giving the Director of CISA direct access to the President allows better communication regarding cyber issues, which will result in more prompt decision-making. It also demonstrates to the nation and the world that the United States takes cybersecurity seriously and that decisions regarding our cyber policy are made by no less than the President of the United States.

Additionally, the United States must begin identifying and addressing redundancies in its cyber organizational structure to streamline cyber response capabilities. The Director of CISA, as the focal point of all cyber considerations, will be able to make determinations in that area and ensure that resource allocation is efficient and used to its maximum potential. This point is perfectly encapsulated in the Department of State's effort to create a new, internal cybersecurity bureau.[308] The Department of State's had the

[306] Draft language reflects the Executive Order pertaining to the Director of National Intelligence. *See* Exec. Order No. 13,470, 73 Fed. Reg. 150 (July 30, 2008) (amending Exec. Order No. 12,333).

[307] "Protecting America's national security and promoting the prosperity of the American people are my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors." National Cyber Strategy, *supra* note 160.

[308] Sean Lyngaas, *State Department Proposes New $20.8 Million Cybersecurity Bureau*, CYBERSCOOP (June 5,2019), www.cyberscoop.com/state-department-proposes-new-20-8-million-cybersecurity-bureau/.

admirable goal of reducing redundancies within U.S. government and increasing cooperation amongst the agencies with cyber capabilities. However, the Department of State left out one very important preparatory step while creating its new bureau: coordination with other agencies.[309] Without proper coordination and oversight in advance of the creation of these new agencies, redundancies are inevitable.

As coordinator, CISA will be able to assess current government agencies and programs. Additionally, with control over budget requests and cyber response, CISA will be able to limit the practice of establishing and then retooling redundant agencies and programs. This will streamline the organizational structure and prevent waste of resources. Simplifying the organizational structure should also create increased communication with Congress, which will enable legislators to react to cybersecurity issues more quickly.[310]

Given the critical responsibilities and duties of the cyber coordinator, representatives argue that the position should be Senate-confirmed, not solely an executive appointment.[311] This is one of the perceived strengths of the NCD position. The legislative branch would have a voice in the confirmation process which would ensure that the position reflected "strategic guidance from the President and Congress . . . to achieve coherence in the planning, resourcing, and employing of government cyber resources."[312] This coherence would

[309] *Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establishthe Cyberspace Security and Emerging Technologies Bureau*, GOV'T ACCOUNTABILITY OFF., GAO-20-607R (Sept. 22, 2020), www.gao.gov/assets/gao-20-607r.pdf.

[310] There are currently approximately 80 congressional committees and subcommittees claiming "some jurisdictionover cybersecurity" which means "it can take cyber legislation a disproportionately long time to get put to a vote." Jack Corrigan, *Lawmaker: Congress Needs Fewer Committees with Cyber Oversight*, NEXTGOV (Jan. 29, 2019), www.nextgov.com/cybersecurity/2019/01/lawmaker-congress-needs-fewer-committees-cyber- oversight/154506/.

[311] Representative Jim Langevin said that the Senate-confirmed position "gives the person who holds this spot, thisposition, more gravitas than just a staff person." Miller, *supra* note 203.

[312] CSC Report, *supra* note 295, at 37.

allow the NCD position to better fulfill the coordinator position and increase its effectiveness.

However, this argument puts the proverbial cart before the horse. Before the legislature adds another level of bureaucracy to United States' ability to respond in cyberspace, the existing players must be given time and resources to perform their roles and conduct studies on each piece of the cyber puzzle. Once CISA fleshes out redundancies in the existing organizationalstructure, Congress will be able to move forward with an evidence-based plan regarding a Senate-confirmed position. In the interim, the Director of CISA can meet with congressional committees, as necessary, to achieve the desired level of coherence. Essentially, CISA should be allowed to perform the study originally proposed by the Senate in the 2021 NDAA.

Giving CISA this task, as well the resources to accomplish it, eliminates the need to set up another committee or taskforce and allows CISA to fully exercise its already assigned function ofpartnering "with stakeholders across the executive branch."[313]

2. Increased Private Sector Cooperation in Domestic Cybersecurity

Increased cooperation between public corporations and the federal government would improve security and accountability for cyber misfeasors.[314] As such, Congress should implement a mandatory reporting requirement for data breaches. This mandatory reporting requirement would increase law enforcement's ability to successfully investigate cybercrime. A federal data breach law would also bring consistency and uniformity to data breach jurisprudence.[315] As previously discussed, the Department of Justice has already called for the enactment of such a provision.[316] In fact, New Jersey already has a state provision requiring corporations to "report the breach of security and any information pertaining to the breach to the Division of State Police . . . for investigation or handling" when personal

[313] *Id.* at 39.
[314] National Cyber Strategy, *supra* note 160.
[315] *Security Breach Notification Laws*, *supra* note 153.
[316] Statement of Adam S. Hickey, *supra* note 155.

information was or was reasonably believed to have been accessed by an unauthorized person.[317]

This federal data breach law should also shield corporations from other reporting requirements until law enforcement has decided the depth of the investigation necessitated by the report. A shielding provision would relieve the company from penalties and fines imposed under other reporting provisions while allowing law enforcement time to assess the situation. After law enforcement has concluded its assessment, corporations can report the breach to their consumers and investors as per usual.

When a company experiences a data breach, internally the best perceived remedy is to "shore up any internal deficiencies . . . and to fulfill its legal obligations in terms of notifying affected parties and regulators."[318] Most companies have determined that there is no benefit to reporting the incident to law enforcement if that reporting is not required. The crime is done. The best thing to do is let customers and investors know, move on, and try to ensure it does not happen again. Law enforcement involvement will only hinder the company's productivity by eating up additional resources and time required to cooperate with the investigation. Computer hackers are difficult to find and the likelihood of finding the perpetrator, let alone recovering the stolen data, is low.

The reality is that companies will be breached, and data will be stolen. While it is tempting to cover corporate losses and move on, mandatory reporting to law enforcement will result in increased tracking of these cybercriminals and ensure that multiple entities do not fall prey to the same attack. The short-term benefits of reporting may seem costly to businesses, but the long-term security benefits outweigh those costs. For example, based on reporting to law enforcement, the United States was able to partner with an international law enforcement operation and take down a

[317] N.J. Stat. § 56:8-163.

[318] Dan Swinhoe, *Why Businesses Don't Report Cybercrimes to Law Enforcement*, CSO ONLINE (May 30, 2019),www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

transnational cybercriminal network.[319] If mandatory reporting were put into action, law enforcement would be able to engage in more of these operations and shut down cyberattacks at the source. This would result in fewer sophisticated and coordinated attacks which will, in the long run, better protect businesses and their data.

This proposed mandatory reporting requirement is similar to existing required reportingimposed on national banks for suspicious activities involving money laundering or fraud.[320] A national bank must file a Suspicious Activity Report ("SAR") when it "detect[s] a known or suspected violation of federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act."[321] The Bank Secrecy Act ("BSA") requires financial institutions "to assist U.S. government agencies in detecting and preventing money laundering" activities.[322] There is a minimum monetary threshold imposed on filing a SAR.[323] The only exceptions to reporting are if the financial institution is the victim of a robbery or burglary and reports to appropriate law enforcement authorities or if the institution reports lost, missing, counterfeit or stolen securities in accordance with another regulation.[324] The U.S. government is made aware of the incident, either through law enforcement or a SAR filed with the Department of the Treasury, Financial Crimes Enforcement Network. This reporting requirement offers the U.S. government "an opportunity to spot and analyze emerging trends and patterns across

[319] Press Release, Europol, Goznym Malware: Cybercriminal Network Dismantled in International Operation (May 16, 2019), www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in- international-operation.

[320] Financial institutions are required to file a Suspicious Activity Report (SAR) to help monitor unusual or potentially illegal finance-related activity. *What Is a Suspicious Activity Report*, THOMASON REUTERS, www.legal.thomsonreuters.com/en/insights/articles/what-is-a-suspicious-activity-report [hereinafter Suspicious Activity Report].

[321] 12 C.F.R. § 21.11(a) (2012).

[322] Officer of the Comptroller of the Currency, *Suspicious Activity Reports (SAR)*, OFF. OF THE COMPTROLLER OF THE CURRENCY, www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html.

[323] 12 C.F.R. § 21.11(f)(1)-(2) (2012).

[324] *Id.*

a broad spectrum of personal and organized crimes. With this knowledge, they can anticipate and counteract fraudulent and criminal behavior before it gains a foothold."[325] The BSA has required SARs since 1970[326] and it is high time that the government enforced a similar reporting requirement for data breaches to provide the same benefits to law enforcement in combatting cybercrime.

The language for the federal data breach statute should include a broad definition of what constitutes a breach. For example, the definition of a breach could include "unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business."[327] This definition includes not only acquisition of private information, but mere access to that information, thus broadening the type of activity included in the reporting requirement.

Additionally, the federal data breach notification law should state that any business or public entity upon discovery or notification of a breach shall, in advance of any other disclosure,report the breach of security and any information pertaining to the breach to the FBI Cyber Crime Unit for investigation and handling. Notification to other parties shall be delayed if the law enforcement agency determines that the notification will impede a criminal or civil investigation. Required notification shall be made after the law enforcement agency determines that disclosure will not compromise the investigation and notifies the affected business or publicentity of its determination.[328]

However, a mandatory reporting requirement would interfere with a company's ability to conduct an internal investigation and its obligation to inform investors regarding major breaches and incidents, not just state regulatory authorities. Businesses have

[325] Suspicious Activity Report, *supra* note 320.
[326] *Id.*
[327] Sample text based on the language contained in New York's recent SHIELD Act. *See* Notification; Person Without Valid Authorization has Acquired Private Information, N.Y. Gen. Bus. Law § 899-aa (2019), at § 1(C).
[328] Sample text based off the language utilized by N.J. Rev. Stat. § 56:8-163 (2013).

generally refrained from reporting breaches to law enforcement to preserve their investments and interests. Due to the lack of transparency inherent in a criminal investigation, businesses are unable to answer tough questions from their investors.[329] Once law enforcement steps in, businesses are kept in the dark and no longer receive any information regarding the breach. This hinders the company's ability to provide information to their customers regarding the depth of the breach and to effectively pursue its remediation efforts.[330]

In order to help mitigate some of the internal risks of reporting, Congress should promulgate more robust rules giving victim corporations rights that specifically address their concerns. In 2018, FBI Director Christopher Wray stated that the FBI treats victim companies as crime victims.[331] The Crime Victims' Rights Act and Victims' Rights and Restitution Act provide victims with statutory rights regarding criminal investigations. These requirements include that the victim be reasonably allowed to confer with government counsel as well as be informed when certain milestones in the case occur.[332] Additionally, victims are entitled to updates regarding the status of the investigation, "to the extent it is appropriate" and "to the extent that it will not interfere with the investigation."[333] Notably, the Crime Victims' Rights Act requires that victims be treated with fairness and respect for their right to privacy which prevents unnecessary disclosure of victims' information.[334]

As stated by FBI Director Wray, these rules should be robustly applied to victim corporations in the context of data breaches. In legislating the mandatory reporting requirement, Congress should consider the implementation of additional victims' rights tailored to the victim entities. For example, legislation could include text to the

[329] Newman, *supra* note 154.
[330] Swinhoe, *supra* note 318.
[331] Nate Raymond, *FBI Chief: Corporate Hack Victims Can Trust We Won't Share Info*, REUTERS (Mar. 7, 2018), www.reuters.com/article/us-usa-fbi-wray/fbi-chief-corporate-hack-victims-can-trust-we-wont-share-info-idUSKCN1GJ2QS.
[332] *See* Crime Victims' Rights Act, 18 U.S.C. § 3771.
[333] Victims' Rights and Restitution Act, 34 U.S.C. § 20141(c)(3)(A).
[334] Crime Victims' Rights Act § 3771(a)(8).

effect that CISA personnel shall assist the victim entity in evaluating the victim entity's current cybersecurity protocol and assist in the implementation of updated guidelines utilizing the framework and recommendations issued by the National Institute of Standards and Technology ("NIST").[335] This assistance would ensure that the breach is contained while providing the corporation with additional security against future breaches.

These proposals require an extraordinary amount of federal resources. The FBI Cyber Crime Unit already struggles to stay afloat amidst its enormous caseload. If Congress passes legislation requiring mandatory reporting, the FBI's caseload would increase significantly as U.S. businesses face countless attempted incursions through spear phishing, malware, and other malicious attacks.[336] Any benefit of mandatory reporting would be lost through the FBI's inability to quickly conduct triage and determine which reports, if any, give rise to grounds justifying opening an investigation. This delay will prevent companies from publicly reporting the breach to their consumers which will only increase breach-related damages.[337] Thus, a mandatory reporting requirement will only overwhelm an already overtaxed FBI while causing delays and additional harm to victim corporations.

However, mandatory reporting does not necessitate an in-depth investigation for every incident. Each incident will be used as a data point to create a threat trend. Observing these patterns will allow law enforcement to amass data on popular targets. The FBI can then use thisinformation to inform CISA of recurring threats and national security risks who can adjust and prepare accordingly. Additionally,

---

[335] *See Cybersecurity Framework*, NAT'L INST. OF STANDARDS & TECH., www.nist.gov/cyberframework/framework (last visited Nov. 13, 2020).

[336] Mark Rasch, *DoJ Calls for Mandatory Data Breach Reporting to Law Enforcement*, SECURITY BOULEVARD (Apr. 9, 2020), securityboulevard.com/2020/04/doj-calls-for-mandatory-data-breach-reporting-to-law-enforcement/.

[337] Studies indicate that timely reporting increases consumer trust and that the most severe fallout with consumersatisfaction occurs when companies are not transparent. *See* LILLIAN ABLON ET AL., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 36-38 (RAND CORP. 2016).

CISA's assistance to breached companies will allow them toprevent future breaches and lower post-breach remediation costs.

Pursuant to the above proposed mandatory reporting language, whenever a company discovers that its data was accessed by an unauthorized party, that company must report the incident to law enforcement. Even if no data was lost or stolen, mere unauthorized access is sufficient to trigger the reporting requirement. Upon receiving the report, law enforcement will conduct a preliminary investigation to determine the severity of the breach. At this point, law enforcement will not report the breach publicly and any missed reporting requirements to regulators and consumers will be protected by the shield provision. Upon conclusion of the preliminary investigation, law enforcement will take further action if necessary or close the investigation. Either way, the victim company will receive assistance from CISA to ensure that breaches do not occur in the future.

Furthermore, Congress should consider providing tax breaks for companies who take proper precautions with their cyber hygiene and follow NIST guidance and recommendations. CISA, or another inspection agency, can ensure compliance and verify eligibility for tax breaksthrough regular inspections and assessments of U.S. businesses. These tax breaks would provide incentives for corporations to shore up their cyber protocols and mitigate the costs of implementing a robust defensive system.

One of the easiest steps to avoid a data breach is basic cyber hygiene, such as regularly patching software and establishing high standards for passwords and user information.[338] With corporations increasing their ability to fight off cyberattacks and penetration efforts, the FBI should see a corresponding drop in reports of data breaches. While it is unlikely that any private corporation could reach the level

[338] Marc van Zadelhoff, *The Biggest Cybersecurity Threats are Inside Your Company*, HARV. BUS. REV. (Sept. 19, 2016), hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.

of fending off an attack from a malicious nation-state attack,[339] these precautions will allow companies and the FBI alike to focus on more serious and pervasive threats from nation-states and organized cybercrime groups.

Traditional free market economics argue that the invisible hand of the market will encourage companies to invest in cybersecurity to prevent the costs of a data breach.[340] Under this theory, a tax break would constitute additional, enormous, and unnecessary costs to the federal government. The private sector corporations and businesses will adjust their investment and cybersecurity strategies to avoid the costs associated with a breach and ensure their data is safe.

However, tax breaks are often used to incentivize private entities to engage in what thefederal government deems to be desirable behavior—for example, there are tax incentives for capture and sequestration of CO_2 emissions from power plants.[341] Because of the way that the United States has developed its infrastructure and the level of inclusion of private corporations, private entities' cybersecurity systems are now integral to protecting infrastructure.[342] Critical infrastructure, such as power and water, is controlled by private companies and those systems have, to a certain extent, become digitized and thus are vulnerable to cyberattacks. Private entity cybersecurity has become an issue of national security. Furthermore, "it has become evident that cybersecurity cannot be adequately ensured by the market's 'invisible hand,'" which necessitates "state

[339] Five members of the People's Liberation Army, the Chinese military, were indicted for various computer-relatedoffenses, including economic espionage and conspiracy to hack into computers of six different American corporations. At least one of the victim corporations lost valuable trade secrets. *See* Indictment, United States v. Wang Dong, No. 14-118 (W.D. Pa. 2014).

[340] *See Cost of a Data Breach Report 2020*, IBM, www.ibm.com/security/data-breach (in 2020, the average cost of a data breach was $3.86 million).

[341] Angela C. Jones & Molly F. Sherlock, CONG. RSCH. SERV., IL 11455, THE TAX CREDIT FOR CARBON SEQUESTRATION (SECTION 45Q) (2020).

[342] The private sector owns roughly 85% of the United States' critical infrastructure and key resources. *See CriticalInfrastructure*, STRATEGIC FORESIGHT INITIATIVE 2 (June 2011), www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

intervention to advance public interest and mitigate cybersecurity risks."[343] As such, the United States has a national security interest in investing in the cybersecurity of private entities.

In the alternative, Congress could impose taxes on companies that do not comply withbasic cyber hygiene and the NIST framework. This will create additional inspection and regulatory work for CISA but will help offset the cost of additional expenses incurred by the FBI and other law enforcement agencies. This tax penalty approach was proposed by then- candidate Biden to penalize U.S. companies who move their operations overseas with a reciprocal tax credit to reward those companies who created jobs in the United States.[344] Thus, instead of using the proverbial carrot (tax credits) to encourage companies to strength their cybersecurity, companies will face penalties for failure to comply with basic standards and cyber hygiene. This alternate framework reflects the importance of cybersecurity and makes compliance a requirement rather than an optional benefit.

Since China began regulating data breach notifications, Chinese companies have always been required to report breaches to the authorities.[345] In the European Union ("EU"), data breach notification laws impose an obligatory seventy-two-hour breach notice for unauthorized access to systems and data as well as use and distribution of data to "the responsible national supervisory authorities."[346] The EU's seventy-two-hour notification window is

[343] Gabi Siboni & Ido Sivan-Sevilla, *The Role of the State in the Private-Sector Cybersecurity Challenge*, GEO. J. INT'L AFFS. (May 27, 2018), www.georgetownjournalofinternationalaffairs.org/online-edition/2018/5/27/the-role-of-the-state-in-the-private-sector-cybersecurity-challenge.

[344] Jennifer Epstein, *Biden Plan Sets Tax Penalties for Companies' Offshore Profits*, BLOOMBERG (Sept. 9, 2020), www.bloomberg.com/news/articles/2020-09-09/biden-plan-sets-tax-penalties-for-companies-offshore-profits.

[345] Until the 2016 Cybersecurity Law, Chinese corporations that fell victim to data breaches "were only required to notify the authorities" not the individuals impacted by the breach. Graham Greenleaf & Scott Livingston, *China's New Cybersecurity Law – Also a Data Privacy Law?* 144 UNSWLRS 1, 5 (2016).

[346] Mari Kert-St Aubyn, *EU Data Protection Reform Introduces Mandatory Data Security and Data Breach Notification Requirements*, COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, ccdcoe.org/incyder-articles/eu-data-protection-reform-

much stricter than in the United States, where companies typically have at least thirty days to assess the severity of the breach before reporting.[347] The Chinese data breach notification requirement is more like the United States' and generally requires its companies to provide notification to authorities "within a reasonable time."[348]

The bottom line is that U.S. allies and adversaries are handling data breaches in a more efficient and productive manner to ensure that they can combat cybersecurity threats on a national scale. It is time that the United States caught up. Mandatory reporting will enable the federal government to hold malicious actors, both state and non-state, responsible for their activities while creating a more secure environment for U.S. businesses.

3. Manage Risk and Secure the Supply Chain

Currently, one of the biggest concerns in 5G is developing the necessary infrastructure. This 5G foundation will persist and shape the global community for decades to come. International organizations, such as 3GPP, have been discussing the technological specifications of 5G infrastructure and hardware for years.[349] If the federal government increases its level of cooperation with 3GPP, as well as other leading standard-setting organizations, there should quickly be agreement regarding minimum standardization to assure proper security and to mitigate risk in the United States' 5G

introduces-mandatory-data-security-and-data-breach-notification-requirements/ (last visited Nov. 13, 2020).

[347] For example, the Health Insurance Portability and Accountability Act (HIPAA) requires notification to the affected individuals no later than 60 days after the breach. If the breach affected more than 500 individuals, the breached entity must also inform the Secretary of Health and Human Services within 60 days. *See Breach Notification Rule*, U.S. DEP. OF HEALTH AND HUMAN SER., www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Nov. 14, 2020).

[348] This "reasonable time" notice requirement is imposed by the 2018 Specification. Some scholars believe that the Chinese government is simply assessing the data regarding a "reasonable time" and will impose a set timeframe at alater date. Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?* 8 PENN. ST. J.L. & INT'L AFF. 49, 89 (2020).

[349] 3GPP began working on 5G standards in 2016. Lorenzo Casaccia, *Understanding 3GPP-Starting with the Basics*, QNQ BLOG (Aug. 2, 2017), www.qualcomm.com/news/onq/2017/08/02/understanding-3gpp-starting-basics.

implementation. This is another area where the United States' continued participation in and engagement with standard-setting organizations at all levels, both private and public, remains integral to the secure roll out of 5G technology in the United States.

Due to these concerns regarding 5G infrastructure, the U.S. government has taken significant steps against Chinese corporations, such as Huawei.[350] However, these targeted actions against specific companies have increased tensions between the United States and China.[351] While talks between the two nations have not yet broken down completely, the Chinese foreign ministry spokesman, Lu Kang, stated that "negotiations and consultations, to have meaning, must be sincere. First, there must be mutual respect, equality and mutual benefit. Second, one's word must be kept, and not be capricious."[352] This statement echoes the Chinese concerns with mutual strategic trust and their holistic, relational view of foreign relations.[353]

To smooth relations and ensure stability moving forward, the United States should develop objective standards for infrastructure to secure risk management standards, as well as the supply chain. To this end, in November 2019, the United States announced its partnership with Japan and Australia to initiate the Blue Dot Network ("BDN").[354] The BDN will "promot[e] quality, market-driven, and private-sector led investment" in developing infrastructure around the world and

[350] U.S. Government agencies and contractors are prohibited from using Huawei technology pursuant to the 2019 NDAA. Huawei and seventy of its affiliates were also added to the Department of Commerce's Entity List causing supplychain, chip, and software challenges for the Chinese corporations. *See* Joe Panettieri, *Huawei: Banned and Permittedin Which Countries? List and FAQ*, CHANNEL E2E (Nov. 13, 2020), www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/.

[351] Chen & Lee, *supra* note 177.

[352] *Id.*

[353] HAROLD ET AL., *supra* note 157, at 33-34.

[354] Matthew P. Goodman et al., *Connecting the Blue Dots*, CTR. FOR STRATEGIC & INT'L STUD. (Feb. 26, 2020),www.csis.org/analysis/connecting-blue-dots.

ensure that these infrastructure projects "meet the highest standards."[355]

Japan's BDN strategy adopts a "cross-vendor approach" to 5G infrastructure which allows for a combination of vetted suppliers rather than locking-in to a single supplier which, in turn, alleviates supply-chain risks.[356] Unlike the United States, Japan does not specifically ban technology from any corporations or nation-states.[357] Rather, Japan relies on its standard-setting requirements and supply-chain diversity to protect itself from potential 5G vulnerabilities.

Like Japan, the United States should develop objective standards for hardware and infrastructure.[358] The United States can develop these standards through its partnership with 3GPP as well as nations like Japan who have already successfully implemented this framework. While the Entity List constitutes an effective protection of U.S. national security interests, it is possible to accomplish the same goal of excluding Huawei's products without directly targeting the corporation, a step that could go a long way in smoothing the path toward a more productive dialogue with China.

However, there are those who argue that the specific ban on Huawei is necessary due to Huawei's close ties to the People's Liberation Army, China's Ministry of State Security, as wellas Chinese state-backed hackers.[359] Additionally, the Huawei-specific ban continues sending themessage that the United States will not work

---

[355] *Blue Dot Network: Frequently Asked Questions*, U.S. DEP'T OF STATE, www.state.gov/blue-dot-network-frequently-asked-questions/.

[356] Mihoko Matsubara, *Japan's 5G Approach Sets a Model for Global Cooperation*, LAWFARE (Sept. 14, 2020),www.lawfareblog.com/japans-5g-approach-sets-model-global-cooperation.

[357] *Id.*

[358] NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, NSTAC REPORT TO THE PRESIDENT ON ADVANCING RESILIENCY AND FOSTERING INNOVATION IN THE INFORMATION AND COMMUNICATIONS TECHNOLOGY ECOSYSTEM 24 (2019), www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_2.pdf.

[359] Doug Brake, *A U.S. National Strategy for 5G and Future Wireless Innovation*, INFO. TECH. & INNOVATION FOUND. (Apr. 27, 2020), itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation.

with nations who use this technology.[360] Several nations have already prohibited Huawei technology from their systems, which has, in turn, protected U.S. national security interests. Without specifically banning China's technology corporations from entering the supply chain, BDN fails to provide this level of protection for national security. Since Huawei's placement on the Entity List, it is more difficult for the Chinese company to secure the necessary technology to further its 5G rollout.[361] This has led, in part, to the United Kingdom's decision to not allow the installation of any additional Huawei equipment due to supply chain concerns.[362] The strict export controls imposed on Huawei served their purpose by ensuring that U.S. allies refrain from utilizing Huawei technology in their 5G rollouts, thus protecting U.S. allies as well as U.S. national security interests.

While the restrictions on Huawei within the United States did protect U.S. national security, the continuation of export controls only hurt U.S. businesses with negligible positive impact on national security.[363] Current export controls prevent U.S. companies from doing business with Huawei. These "[e]xport controls do not address any immediate security threat, are not effective at slowing down Huawei, are very harmful to U.S. component supplies, and are likely to accelerate Huawei's technological autonomy."[364] Based on current evidence, it is clear that Huawei is already experiencing security defects in its technology and will be unable to clear any objective minimum standard of security established by the United States and the international community.[365] By cutting off Huawei's access to U.S.

---

[360] Bowler, *supra* note 43.

[361] Paul Sandle & Guy Faulconbridge, *Britain Set to Ban Huawei from 5G, Though Timescale Unclear*, REUTERS (July 13, 2020), www.reuters.com/article/us-britain-huawei-idUSKCN24E0K3.

[362] *Id.*

[363] Brake, *supra* note 359.

[364] *Id.*

[365] Regardless of fears that Huawei may build backdoors into their technology, reviews of Huawei equipment and security show that there are front doors through which a sophisticated hacker may enter. Thomas Seal, *U.K. Found "Critical" Weakness in Huawei Equipment*, BLOOMBERG (Oct. 1, 2020), bloomberg.com/news/articles/2020-10-01/u-k-found-critical-weakness-in-huawei-equipment-last-year.

technology, it will be forced to develop its own technology, which will only increase issues of interoperability while hurting U.S. economic interests abroad.

The United States should establish internationally accepted norms and standards regarding 5G hardware and infrastructure specifications to ensure a safe and secure rollout in the United States and around the world. To that end, the United States has already taken significant steps forward in sponsoring the BDN. The import limits currently in place prohibit Huawei equipment in U.S. telecommunication networks. Due to the aforementioned security concerns though, operators were unlikely to use Huawei equipment in the first place.[366] These inherent security concerns are easily addressed by the objective standards of the BDN and can protect U.S. national security just as effectively through more simple and narrow import restrictions.[367]

In regard to export controls, the Department of Commerce and the U.S. government argue that these export controls are in place due to Huawei's involvement in activities that are contrary to U.S. national security, namely exporting technology to Iran without a license in violation of U.S. sanctions and export controls.[368] In fact, a bill was recently introduced in the House of Representatives which would keep Huawei on the Entity List by Congressional mandate.[369] This bill was reportedly a response to the new Secretary of Commerce's refusal to expressly commit to keeping Huawei on the Entity List during her confirmation hearing.[370]

---

[366] *Id.*

[367] Brake, *supra* note 359.

[368] Entity List, *supra* note 65.

[369] The Secretary of Commerce would be prohibited from removing Huawei from the Entity List until the Secretary determines, with the unanimous concurrence of the End-User Review Committee, that Huawei is not engaged and isunlikely to engage in activities contrary to U.S. national security interests and that Huawei is not owned, controlled or influenced by the Communist Party of China. Keep Huawei on the Entity List Act, H.R. 1595, 117th Cong. § 2 (2021).

[370] Press Release, *Steube Introduces Legislation to Counter CCP-Controlled Huawei, Force Biden Admin to Keep on Entity List,* GREG STUEBE (Mar. 3, 2021),

However, the United States should relax export control requirements as they negatively impact U.S. businesses without providing much tangible benefit to the U.S. people.[371] Overly broad export controls will only force Huawei to look to other sources or internally develop components that it used to get from U.S. companies, which will result in greater technological independence to the detriment of the U.S. economy. Essentially, Huawei will continue its activities and U.S. companies will simply be cut out of the operation. Reducing export controls requirements will help U.S. businesses as well as begin the process of mending tense relations with China. Improving relations with China will further the ultimate goal of coming to anagreement regarding stability and security in global technology and cyberspace.

IV. CONCLUSION

This Article attempts to lay the framework for realistic and practical solutions to the threats posed by 5G networks and future technologies. The main issue behind the 5G threat is the future of cyberspace and each nation's role in that future. China is attempting to push through and establish itself as a global leader in technology while the United States is attempting to hold on to its historic role in that arena. The security and economic benefits of leading the 5G charge are significant and will lead to opportunities to lead the way in future generations of technology.

For the United States to maintain its position, the nation must present a unified front regarding cyber response and handling new technologies, like 5G. To that end, this Article suggests that CISA should be given the primary role in leading the nation's cybersecurity program. This solution can and should be accomplished immediately, and CISA should be given at least a year to assess and make

steube.house.gov/media/press-releases/steube-introduces-legislation-counter-ccp-controlled-huawei-force-biden-admin.

[371] "These export controls…have faced considerable criticism, particularly due to the damage to the U.S. semiconductor industry-which is harming U.S. leadership in 5G and related fields without must benefit to speak of.Chinese companies account for about 23 percent of global demand for semiconductors, so cutting off access to that market is a very costly decision." Brake, *supra* note 359.

recommendations to Congress. Additionally, private industry should be held to a higher cyber-related standards due to the United States' reliance on the private industry for its critical infrastructure. The process of drafting and passing legislation regarding data breach reporting requirement as well as the accompanying tax incentives will likely take between one and two years. Most importantly, to counter imminent national security threats, the United States must secure and diversify its digital supply chain in a way that establishes objective security standards without escalating tensions between nations by singling out specific entities.

The global response to issues in cyberspace is one of the most divisive aspects in the relationship between the United States and China. In order to create a unified and global response to navigating the future of cyberspace, the Budapest Convention must become a truly global treaty. The United States should spearhead efforts to include nations like China and Russia in the Convention to protect the future of cyberspace and the principle of a free and open Internet. Curating the necessary buy-in amongst member states to amend the membership protocol could take several years but defeating the AP II must occur immediately to ensure the Convention is not effectively barred from becoming a truly global treaty. Continued and increased U.S. participation in international standard-setting organizations, like 3GPP and the ITU, will keep the global dialogue open and ensure U.S. input and influence into these rapidly developing technologies and accompanying standards.

Cybersecurity is national security. In order to combat the threats posed by 5G and future technologies, the United States must champion changes to domestic and international law and policy to ensure a secure future for U.S. citizens. These proposed solutions will not solve the cybersecurity issues faced by this nation, but they will provide a firm framework to move forward in anobjective and unified fashion that will increase our national security and improve international relations.