THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA INTERNATIONAL LAW SECTION

The YEAR IN REVIEW

AN ANNUAL SURVEY OF INTERNATIONAL LEGAL DEVELOPMENTS AND PUBLICATION OF THE ABA INTERNATIONAL LAW SECTION

VOLUME 56 | 2022

International Legal Developments Year in Review: 2021

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

Published in Cooperation with SMU Dedman School of Law

THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA INTERNATIONAL LAW SECTION

National Security Law

ORGA CADET, GEOFFREY GOODALE, LAURENCE R. HULL,
RENEE LATOUR, BARBARA LINNEY, JONATHAN MEYER,
GUY C. QUINLAN, MINJI "MJ" SHIN,
CHRISTOPHER VALLANDINGHAM, AND BONNIE H. WEINSTEIN*

This article highlights significant legal developments relevant to national security law that took place in 2021.

I. Diligence and Disclosure Obligations for Victims of Ransomware Attacks

Ransomware attacks—cyberattacks demanding that the victim pay a ransom for decryption keys and to avoid the publication of exfiltrated information—have been described as a "scourge" on U.S. companies.[1] These attacks affect a wide range of industries, including but not limited to healthcare, manufacturing, finance, and insurance.[2] In 2020, the largest ransom demand was over $65 million,[3] and the largest ransom paid was in excess of $15 million dollars—each more than three times greater than their respective values in 2019.[4]

Companies considering paying such ransomware demands risk violating U.S. economic sanctions. In October 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) released an advisory directing companies that facilitate ransomware payments on behalf of

---

* Orga Cadet served as the committee editor of this article. Barbara Linney, Partner at Baker & Hostetler LLP, and Orga Cadet, Associate at Baker & Hostetler LLP, co-authored "Diligence and Disclosure Obligations for Victims of Ransomware Attacks." Geoffrey Goodale, Partner at Duane Morris, LLP, and Jonathan Meyer, Attorney at Law, co-authored "Efforts to Secure the Information and Communications Technology and Services Supply Chain." Renee Latour, Partner at Clifford Chance US LLP, Laurence R. Hull, Senior Associate at Clifford Chance US LLP, and MJ Shin, Law Clerk at Clifford Chance US LLP, co-authored "CFIUS's Evolving Concept of National Security in 2021." Guy C. Quinlan, President of the Lawyers Committee on Nuclear Policy, is the author of "Nuclear Arms Control." Christopher Vallandingham, Head of Collections and Professor of Legal Research at the University of Florida Levin College of Law and National Security Law Attorney for the U.S. Army, is the author of "Targeted Disinformation Campaigns." Bonnie H. Weinstein, Attorney at Law, is the author of "Update on the Budapest Convention on Cybercrime."

1. THEODORE J. KOBUS III & CRAIG A. HOFFMAN, BAKER & HOSTETLER, 2021 DATA SECURITY INCIDENT RESPONSE REPORT 4 (2021), https://f.datasrvr.com/fr1/021/74237/2021_DSIR_Report.pdf.

2. *Id.* at 3.

3. *Id.* at 4.

4. *Id.*

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

victims—e.g., banks, cyber insurance providers, and digital forensics companies—to "account for the risk that a ransomware payment may involve a SDN [specially designated national] or blocked person, or a comprehensively embargoed jurisdiction."[5] As noted in the advisory, many ransomware actors have been added to OFAC's List of Specially Designated Nationals and Blocked Persons.[6] The digital currency wallet utilized by the threat actors may also be designated.[7] In addition, ransomware actors may be located in sanctioned countries.[8]

On September 21, 2021, OFAC released updated advice for companies who suffer ransomware attacks (the Updated Advisory).[9] In the Updated Advisory, OFAC stated, "ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks."[10] As a result, OFAC stated that "[t]he U.S. Government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks."[11]

OFAC also stated in the Updated Advisory that "license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will continue to be reviewed by OFAC on a case-by-case basis with a presumption of denial."[12] OFAC strongly encouraged all victims, and those involved with addressing ransomware attacks, to report incidents to the Cybersecurity and Infrastructure Security Agency (CISA),

---

5. U.S. Department of the Treasury, Office of Foreign Assets Control, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments 4 (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

6. *See id.* at 2. *See also*, *e.g.*, Press Release, U.S. Department of the Treasury, *Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities* (Dec. 29, 2016), https://home.treasury.gov/news/press-releases/jl0693; Press Release, U.S. Department of the Treasury, *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware* (Dec. 5, 2019), https://home.treasury.gov/news/press-releases/sm845.

7. *See*, *e.g.*, Press Release, U.S. Department of the Treasury, *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses* (Nov. 28, 2018), https://home.treasury.gov/news/press-releases/sm556.

8. *See*, *e.g.*, Press Release, U.S. Department of Justice, *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (charging North Korean hacking team with perpetrating the 2017 WannaCry 2.0 global ransomware attack).

9. U.S. Department of Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* 1 (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

10. *Id.* at 3.

11. *Id.* at 1.

12. *Id.* at 5.

the Federal Bureau of Investigation (FBI), or the U.S. Secret Service (USSS).[13] If there is any reason to suspect a potential sanctions nexus regarding a ransomware payment, OFAC directs victims to also report ransomware attacks and payments to OFAC and the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (CCIP).[14] Doing so could constitute a significant mitigating factor in OFAC's determination of any penalty or other enforcement response.[15]

OFAC continues to sanction ransomware operators and entities that facilitate ransomware payments. For instance, on November 8, 2021, OFAC sanctioned two ransomware operators and a virtual currency exchange that allegedly facilitated ransomware payments.[16] This action indicated OFAC's continuing commitment to applying U.S. economic sanctions laws towards not only ransomware attackers, but also facilitators of ransomware payments to those attackers.[17] Ransomware victims and their supporters should, therefore, strongly consider both the enforcement risk of violating U.S. sanctions laws if paying the perpetrators of cyberattacks and the risk of designation.

In addition to disclosing ransomware attacks to CISA, the FBI, or the USSS, and potentially also to OFAC and the CCIP, victims of ransomware attacks should always consider disclosing the attack to other U.S. government agencies tasked with roles related to export controls or the protection of other sensitive data. For instance, such victims should consider whether to disclose the ransomware incident to the U.S. Departments of Defense, State, and Commerce. The U.S. Department of Defense generally requires U.S. government contractors to disclose within seventy-two hours cyber incidents involving the potential release of unclassified controlled technical information or other information.[18] The U.S. Department of State requires reporting of certain violations under the International Traffic in Arms Regulations (ITAR).[19] Victims should also consider whether reporting other unauthorized exports of technical data listed on the U.S. Munitions List[20] under the voluntary disclosure provisions of the ITAR would be advisable.[21] The U.S. Department of Commerce (DOC) similarly encourages reporting of violations of the Export Administration Regulations (which include similar definitions of "release"

13. *Id.*

14. *Id.*

15. *Id.*

16. Press Release, U.S. Department of the Treasury, *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange* (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471.

17. *See id.*

18. *See* 48 C.F.R. §252.204–7012(a).

19. *See* 22 C.F.R. § 126.1(a)–(e)(2).

20. *See id.* at §§ 120.50 (definition of "release"), -120.17 (definition of "export"), -127.1 (definition of "violations").

21. *See id.* at §127.12.

and "export"),[22] including any unauthorized release of data controlled under the Commerce Control List.[23] Whether to voluntarily disclose ransomware attacks to U.S. government agencies is a decision best made on a case-by-case basis, but given the level of communication and collaboration amongst the various U.S. government agencies with jurisdiction over such matters, entities who are victims of ransomware attacks should consider the value of transparency when weighing the costs and benefits of disclosure.

II. Efforts to Secure the Information and Communications Technology and Services Supply Chain (ICTS)

In 2021, the U.S. government took several actions to help secure the supply chain relating to information and communications technology and services (ICTS). As discussed below, these actions will have profound implications for U.S. and non-U.S. entities that operate throughout the ICTS supply chain.

On January 19, 2021, the DOC published an interim final rule designed to help secure the ICTS supply chain (Interim Rule).[24] Issued pursuant to Executive Order 13,873 of May 15, 2019, (EO 13,873),[25] and noting that the ICTS supply chain "must be secure to protect our national security, including the economic strength that is an essential element of our national security,"[26] the Interim Rule established regulations to provide the DOC with authority to review certain U.S. transactions involving the ICTS supply chain that have a nexus with foreign adversaries that were initiated, pending, or completed on or after January 19, 2021.[27]

Pursuant to the Interim Rule, which went into effect on March 22, 2021, the DOC may prohibit or restrict transactions conducted by any person, or involving any property, subject to U.S. jurisdiction, if they: (1) involve certain categories of ICTS;[28] (2) are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or

22. *See* 15 C.F.R. § 772.1.

23. *See* 15 C.F.R. § 774.

24. Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (proposed Jan. 19, 2021) (to be codified 15 C.F.R. pt. 7). *See also* Exec. Order 14,017, 86 Fed. Reg. 11,849 (Mar. 1, 2021). Separate from the Interim Rule, President Biden issued Exec. Order 14,017 of February 24, 2021 (EO 14,017), which required (among other things) that the Secretary of Commerce and the Secretary of Homeland Security prepare and submit a report on supply chains for critical sectors and subsectors of the information and communications technology (ICT) industrial base within one year of the date of EO 14,017. Since that report and many of the other deliverables required by EO 14,017 are not due until 2022, they are beyond the scope of this article).

25. Exec. Order 13,873, 86 Fed. Reg. 96 (May 15, 2019).

26. Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909, 4909.

27. *Id.* at 4912.

28. *Id.* at 4917.

direction of a "foreign adversary";[29] and (3) pose an "undue or unacceptable risk" to the national security of the U.S.[30] Importantly, the DOC can impose significant civil and criminal penalties for violations of DOC determinations or mitigation measures (*e.g.*, civil penalties not to exceed the greater of $250,000, subject to inflationary adjustment, or an amount that is twice the amount of the transaction that is the basis of the violation; criminal penalties of not more than $1,000,000, and/or imprisonment for no more than 20 years).[31]

Under the Interim Rule, "ICTS" is defined as any "hardware, software, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display."[32] "ICTS Transaction" is defined as any "acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download."[33]

The six categories of ICTS that are reviewable by the DOC under the Interim Rule are:

> (1) Critical Infrastructure: ICTS that will be used by a party to a transaction in a sector designated as "critical infrastructure" by Presidential Policy Directive 21–Critical Infrastructure Security and Resilience, including any subsectors or subsequently designated sectors;[34]
>
> (2) Networking: ICTS that is integral to wireless local area networks, mobile networks, satellite payloads, satellite operations and control, cable access points, wireline access points, core networking systems, or long- and short-haul systems;[35]
>
> (3) Sensitive Personal Data: ICTS that is integral to data hosting or storage or computing services that uses, processes, or retains "sensitive personal data" of greater than one million U.S. persons at any point over the twelve months preceding an ICTS Transaction;[36]
>
> (4) Surveillance/Monitoring/Home Networking/Drones: Surveillance or monitoring devices, home networking devices, and drones or any other unmanned aerial system, where one million units of

29. *Id.* at 4917.
30. *Id.* at 4917.
31. *Id.* at 4928.
32. *Id.* at 4923.
33. *Id.* at 4923.
34. *Id.* at 4924.
35. *Id.* at 4924.
36. *Id.* at 4924.

> the ICTS item at issue have been sold in the twelve months prior to the ICTS Transaction;[37]
>
> (5) Communications Software: Software designed primarily for connecting with and communicating via the Internet that is in use by greater than one million U.S. persons at any point over the twelve months preceding an ICTS Transaction, including desktop, mobile, web-based, and gaming applications;[38] and
>
> (6) Emerging Technology: ICTS that is integral to artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.[39]

As can be discerned from the above description of the six categories, the scope of the Interim Rule is quite broad.

Significantly, only ICTS that is designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary" is subject to review by the DOC.[40] Under the Interim Rule, "foreign adversary" means "any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."[41] As stated in the Interim Rule, "foreign adversaries" specifically include China (including Hong Kong), Cuba, Iran, North Korea, Russia, and Venezuela's Maduro regime.[42]

In accordance with the Interim Rule, the Secretary of Commerce, in consultation with the heads of other relevant US government agencies, may review any covered ICTS transaction to determine if it involves both (1) ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary" and (2) any "undue or unacceptable risk" to U.S. national security as set out in EO 13,873, and ultimately to conclude whether the ICTS Transaction should be permitted, permitted with negotiated mitigation measures, or prohibited.[43]

On March 29, 2021, the DOC requested comments on a possible licensing regime that could be used relating to ICTS transactions.[44] Subsequently, on November 26, 2021, the DOC issued a notice of proposed rulemaking that included proposals to amend the ICTS Supply Chain Regulations to include "connected software applications" as covered items

37. *Id.* at 4295.
38. *Id.* at 4295.
39. *Id.* at 4295.
40. *Id.* at 4293.
41. *Id.* at 4293.
42. *Id.* at 4925.
43. *Id.* at 4926-28.
44. Securing the Information and Communications Technology and Services Supply Chain: Licensing Procedures, 86 Fed. Reg. 16312, 16312 (proposed Mar. 29, 2021) (to be codified at 15 C.F.R. pt 7).

and to propose potential indicators of risk for the DOC to consider when assessing whether an ICTS Transaction involving connected software applications poses an undue or unacceptable risk.[45] It is expected that the DOC will issue final rules relating to the above matters in 2022.

III. CFIUS's Evolving Concept of National Security in 2021

Over the past five decades, the evolution of the concept of "national security" has significantly transformed the U.S. government's foreign investment regime. While reviews of direct or indirect foreign investment into the U.S. remain the domain of the Committee on Foreign Investment in the U.S. (CFIUS or the Committee), the Committee's role in such reviews has continuously evolved, expanded, and shifted to reflect changes in U.S. national security priorities. In particular, CFIUS's actions in 2021 reflect national security concerns with novel critical technology areas and possible repositories of sensitive personal data.

The Committee's basic structure was established in 1975 by Executive Order 11,858 and evolved through a series of amendments and the enactment of the Foreign Investment and National Security Act of 2007 (FINSA), which significantly expanded CFIUS's authority and presence.[46] Post-FINSA, the focus of national security discourse in the U.S. gradually shifted to China, and the question of "technology transfer."[47] These trends culminated with the passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA),[48] which further expanded CFIUS's authority and significantly changed the regulatory process. In 2020, CFIUS introduced the concept of the "TID US Business" – US businesses that (1) produce, design, test, manufacture, fabricate, or develop one or more critical [t]echnologies; (2) own, operate, manufacture, supply, or service critical [i]nfrastructure; or (3) maintain or collect, directly or indirectly, Sensitive Personal [d]ata of US citizens.[49] This past year has seen renewed examples

45. *Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications*, 86 Fed. Reg. 67379, 67379 (Nov. 26, 2021) (to be codified at 15 C.F.R. pt. 7).

46. *See* Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 9, 1975); *see also* Foreign Investment and National Security Act of 2007. 50 U.S.C. App. 2170 (2007).

47. *See* MICHAEL BROWN & PANVEET SINGH, DEFENSE INNOVATION UNIT EXPERIMENTAL (DIUx), CHINA'S TECHNOLOGY TRANSFER STRATEGY: HOW CHINESE INVESTMENTS IN EMERGING TECHNOLOGY ENABLE A STRATEGIC COMPETITOR TO ACCESS THE CROWN JEWELS OF U.S. INNOVATION 3-4 (2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf; *see also* David R. Hanke, Visiting Fellow, National Security Institute at George Mason University's Antonin Scalia Law School, Testimony at the U.S.-China Economic and Security Review Commission's Hearing on U.S.-China Relations in 2021: Emerging Risks Panel III: Assessing Export Controls and Foreign Investment Review 6 (Sept. 8, 2021), https://www.uscc.gov/sites/default/files/2021-08/David_Hanke_Testimony.pdf.

48. *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, 50 U.S.C. § 4565.

49. 31 C.F.R. § 800.248(a)–(c).

of the Committee's focus on critical technology and sensitive personal data as national security risks.

For critical technology, the regulatory definition grants CFIUS a degree of flexibility to adapt and expand its inquiries with respect to technological developments, covering both existing export controls and yet-to-be-designated emerging and foundational technologies.[50] CFIUS's recent actions with respect to robotics technology show this expansion in the scope of interest. In June 2021, Hyundai Motor Group (Hyundai), a South Korean conglomerate, acquired an eighty percent stake in Boston Dynamics, an American robotics company, with the deal conditional on Hyundai receiving CFIUS clearance.[51] Boston Dynamics gained widespread public attention through viral videos of its robotic dog and backflipping robot among other products.[52] Robotics is an example of an 'emerging technology' of interest to CFIUS, even where the particular item or technology has not been formally designated as an "emerging technology." The inclusion of CFIUS clearance as a closing condition to the Hyundai/Boston Dynamics transaction indicated the parties' awareness of CFIUS interest in the robotics sector.

Following FIRRMA's codification of sensitive personal data as part of a broader notion of national security, CFIUS has continued its active review of transactions in which personal data is involved. Sensitive personal data is defined to include genetic data about any number of persons, and personally identifiable data about finances, health, geolocation, biometrics, security clearance, government ID, and certain non-public electronic communications.[53] Beyond high profile examples like the Kunlun-Grindr case,[54] this past year showed the Committee's interest in the national security risks of sensitive personal data through transactions involving start-up companies. Through publicly available investor materials, it was revealed that in January 2021, CFIUS made inquiries with Italian-American transportation company HelBiz regarding its relationship with Chinese bike sharing company GonBike.[55] HelBiz stated that its relationship with

50. 31 C.F.R. § 800.215(a)–(f) (including the U.S. Munition List (USML), certain items on the Commerce Control List, nuclear-related equipment, parts, components, facilities, and material, and select agents and toxins.

51. *See* Boston Dynamics, *Hyundai Motor Group Completes Acquisition of Boston Dynamics from Softbank*, BOSTON DYNAMICS (Jun. 21, 2021), https://www.bostondynamics.com/hyundai-motor-group-completes-acquisition.

52. As of November 2021, Boston Dynamics' YouTube page amassed over 680 million views. See *About Boston Dynamics*, YOUTUBE (Nov. 1, 2021), https://www.youtube.com/user/BostonDynamics/about.

53. 31 C.F.R. 800.241(a)–(b).

54. Yuan Yang & James Fontanella-Khan, *Grindr Sold by Chinese Owner After US National Security Concerns*, FINANCIAL TIMES (Mar. 7, 2020), https://www.ft.com/content/a32a740a-5fb3-11ea-8033-fa40a0d65a98.

55. *See*, *e.g.*, GreenVision Acquisition Corporation, Proxy Statement Pursuant to Section 14(a) of the Securities Exchange Act of 1934 (Schedule 14A) (July 26, 2021), https://investors.helbiz.com/static-files/75a3bed1-267d-485f-a349-e0bdd723800a.

GonBike was purely contractual and only extended to the purchase of ebikes – GonBike did not invest in HelBiz.[56] Given HelBiz's business model which focused on "last-mile" solutions and offered geofencing,[57] CFIUS may have determined that HelBiz's use of sensitive transportation-related data, such as geolocation, posed a national security risk. CFIUS did not progress beyond these inquiries, but the case shows an active CFIUS when it comes to potential national security risks around sensitive personal data.

This attention to sensitive personal data is also in line with the Biden Administration's national security agenda. In June 2021, the White House announced the Executive Order 14,034 Protecting Americans' Sensitive Data from Foreign Adversaries (the Order).[58] The Order outlined criteria for identifying applications that could pose a risk to national security and directed federal agencies to make recommendations on how to protect personal data.[59] While the Order revoked and replaced former executive orders that sought to ban transactions involving TikTok and WeChat, it emphasized the continued focus on personal data as a national security threat.[60]

The evolving and expanding concept of national security is clearly reflected in the role played by CFIUS, as the monitor of foreign investment into the U.S. The Committee's actions in 2021 in the areas of critical technology and sensitive personal data clearly demonstrate this expanded concept of national security and therefore the range of U.S. businesses that can be implicated. Given the Committee's history, CFIUS's role and power will likely only continue to grow as national security concerns continue to evolve.

IV. Nuclear Arms Control

On February 3, 2021, the U.S. and Russia agreed to a five-year extension of the New START agreement,[61] which limited the deployment of strategic nuclear weapons,[62] as it was about to expire, and the two countries later announced their initiation of a series of discussions on strategic stability.[63]

56. *See id.* at 106.

57. *See* Press Release, Helbiz, GreenVision Acquisition Corp. Announces Merger Agreement with Helbiz, Inc. to Become the First Micro-Mobility Company Listed on NASDAQ (Feb. 8, 2021), https://helbiz.com/_nuxt/static/pdf/press-release-en.pdf.

58. Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 11, 2021).

59. *See id.* at 31,424.

60. *See id.*

61. *See* Treaty Between the United States of America & the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, Russ.-U.S., Apr. 8, 2010, T.I.A.S. No. 11,205 [hereinafter New START Treaty].

62. Press Statement, Antony J. Blinken, Secretary of State, U.S. Department of State, On the Extension of the New START Treaty with the Russian Federation (Feb. 3, 2021), https://www.state.gov/on-the-extension-of-the-new-start-treaty-with-the-russian-federation.

63. Press Release, The White House, United States-Russia Presidential Joint Statement on Strategic Stability (June 16, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/16/u-s-russia-presidential-joint-statement-on-strategic-stability.

On November 16, 2021, U.S. National Security Advisor Jake Sullivan announced that Presidents Biden and President Xi Jinping, during their virtual summit, had agreed to "look to begin to carry forward discussions" between the U.S and China on strategic stability.[64]

The nuclear weapon states continued to modernize their arsenals in 2021.[65] Russia continued to test new types of nuclear weapons,[66] and the Russian defense ministry announced plans for increased nuclear weapons budgets over the next three years.[67] The U.S. continued technical upgrades of its existing nuclear missiles to enhance their "hard-target kill capacity,"[68] and the national defense authorization for the coming year includes plans for a new generation of silo-based missiles as well as a new stealth air-launched cruise missile.[69] China prepared what appears to be new missile silos[70] and tested hypersonic delivery vehicles, one of which was designed for earth orbit.[71] The government of India announced that the Chinese orbital vehicle "will not go unanswered" and tested a new missile with a range sufficient to strike most places in China.[72] The United Kingdom announced

64. *U.S. Says It Is Not Engaged in Formal Arms Control Talks with China*, REUTERS (Nov. 17, 2021), https://www.usnews.com/news/world/articles/2021-11-17/us-says-it-is-not-engaged-in-formal-arms-control-talks-with-china.

65. *Global Nuclear Arsenals Grow as States Continue to Modernize—New SPIRI Yearbook Out Now*, STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE (June 14, 2021), https://www.sipri.org/media/press-release/2021/global-nuclear-arsenals-grow-states-continue-modernize-new-sipri-yearbook-out-now.

66. *See, e.g.*, *Russia Test-Fires New Hypersonic Missile from Submarine*, ASSOCIATED PRESS (Oct. 4,2021), https://apnews.com/article/business-europe-russia-vladimir-putin-navy-a941853d791d8b57cc1a2bc39e9d4df4.

67. *See* Alexander Bratersky, *Russian Nuclear Weapons Stand Out in Defense Budget Request*, DEFENSE NEWS (Nov. 1, 2021), https://www.defensenews.com/global/europe/2021/11/01/russian-nuclear-weapons-stand-out-in-defense-budget-request.

68. Jeffrey Smith, *Sensors Add to Accuracy & Power of U.S. Nuclear Weapons But May Create New Security Perils*, WASHINGTON POST (Oct. 29, 2021), https://www.washingtonpost.com/national-security/us-nuclear-weapons-electronic-sensors-accuracy/2021/10/28/79533ff0-34cc-11ec-9bc4-86107e7b0ab1_story.html.

69. CENTER FOR ARMS CONTROL & NONPROLIFERATION, SUMMARY: FISCAL YEAR 2022 NATIONAL DEFENSE AUTHORIZATION ACT (H.R. 4350) AS PASSED 1, 3 (2021), https://armscontrolcenter.org/summary-fiscal-year-2022-national-defense-authorization-act-h-r-4350-as-passed.

70. Matt Korda and Hans Kristensen, *A Closer Look at China's Missile Silo Construction*, FEDERATION OF AMERICAN SCIENTISTS (Nov. 2,2021), https://fas.org/blogs/security/2021/11/a-closer-look-at-chinas-missile-silo-construction.

71. U.S. DEPARTMENT OF DEFENSE, OFFICE OF THE SECRETARY OF DEFENSE, ANNUAL REPORT TO CONGRESS ON MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 60, (Nov. 3, 2021), https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

72. *India Tests Nuclear-Capable Missile Amid Tensions with China*, ASSOCIATED PRESS (Oct. 28, 2021), https://apnews.com/article/china-india-beijing-new-delhi-bay-of-bengal-b460bdea8236801954d114d95c004e3b.

plans to increase the ceiling on the number of warheads in its arsenal.[73] North Korea intensified its missile testing program and vowed to expand its "growing reliable deterrent."[74]

The Biden administration is conducting a reexamination of the Nuclear Posture Review, a general formulation of national nuclear strategy, with results currently expected in early 2022.[75] Arms control advocates are pressing for a declaration that the U.S. will never be the first to use nuclear weapons, but these efforts are reportedly opposed by the U.S. military and by allies currently under the U.S. "nuclear umbrella."[76]

The Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons,[77] postponed in 2020 because of the pandemic, is currently scheduled to convene in January 2022. Meanwhile, a Treaty on the Prohibition of Nuclear Weapons (TPNW), prepared by non-nuclear states frustrated over lack of progress on disarmament under the NPT, entered into force in 2021 with its fiftieth ratification,[78] but is opposed by all states currently possessing nuclear weapons.[79]

In 2021, efforts continued to revive the Joint Comprehensive Plan of Action (JCPOA) restricting nuclear activities of Iran,[80] from which the U.S. withdrew during the Trump administration. No agreement has yet been reached to revive the JCPOA.

The National Defense Authorization Act (NDAA) enacted in 2021 mandates that the National Academies of Science, Engineering, and Medicine must complete a study, within eighteen months, on the effects of various nuclear war scenarios on the climate and environment.[81] The

73. Kingston Reif &Shannon Burgos, *UK to Increase Cap on Nuclear Warhead Stockpile*, ARMS CONTROL TODAY (April 2021), https://www.armscontrol.org/act/2021-04/news/uk-increase-cap-nuclear-warhead-stockpile.

74. Julia Masterson, *North Korea Claims to Test Hypersonic Missile*, ARMS CONTROL TODAY (Nov. 2021), https://www.armscontrol.org/act/2021-11/news/north-korea-claims-test-hypersonic-missile.

75. Kingston Reif, *Biden Administration Begins Nuclear Posture Review*, ARMS CONTROL TODAY (Sept. 2021), https://www.armscontrol.org/act/2021-09/news/biden-administration-begins-nuclear-posture-review (quoting U.S. Defense Department Spokesman Lt. Col. Uriah Orland).

76. AMY F. WOOLF, CONG. RSCH. SERV., U.S. NUCLEAR WEAPONS POLICY: CONSIDERING "NO FIRST USE" 2 (2021), https://sgp.fas.org/crs/nuke/IN10553.pdf.

77. *See* Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161 [hereinafter NPT].

78. *Guterres Hails Entry into Force of Treaty Banning Nuclear Weapons*, UNITED NATIONS (Jan. 22, 2021), https://news.un.org/en/story/2021/01/1082702.

79. *The Status of the TPNW*, NUCLEAR WEAPONS BAN MONITOR (last visited Dec. 11, 2021), https://banmonitor.org/tpnw-status.

80. *See, e.g.*, *Senior State Department Official*, *Special Briefing on Ongoing U.S. Engagement Regarding the JCPOA*, U.S. DEPARTMENT OF STATE (June 24. 2021), https://www.state.gov/senior-state-department-official-on-ongoing-u-s-engagement-regarding-the-jcpoa.

81. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No: 116-283, § 3171, 134 Stat. 3388 (codified as amended in scattered sections of 10 U.S.C.).

NDAA directs the U.S. Secretary of Defense and Director of National Intelligence to furnish the study groups with relevant information.[82]

A United Nations research report on cybersecurity and nuclear weapons risk concluded that "[t]here remains much ambiguity, some intentional, surrounding the types of cyber operations that could elicit nuclear response; this lack of clarity around these 'red lines' feeds into the type of misperception, miscalculation, or misunderstanding that can drive escalation."[83]

V. Targeted Disinformation Campaigns

In 2021, the U.S. government continued to pursue legal avenues to combat disinformation campaigns conducted by foreign actors. Legal methods employed by the U.S. government include the imposition of sanctions on individuals and entities responsible for disinformation campaigns, the seizure of websites, and the indictment of individuals. Though measures to counter disinformation campaigns have received bipartisan support, legislation expanding the ability of the U.S. government to punish individuals and nations that engage in disinformation campaigns has languished in both chambers of Congress since the beginning of the 117th Congress in January 2021.

Disinformation campaigns are coordinated efforts to intentionally mislead the target audience.[84] Congress has distinguished legitimate attempts to influence the U.S. audience "through public diplomacy and strategic communication campaigns"[85] from illegitimate ones, whose aim is "to weaken American alliances and partnerships by creating new divisions between them, or by exacerbating existing ones"[86] and "to foment domestic social and political divisions, and to exacerbate existing ones, within democratic countries, by undermining popular confidence in democracy and its essential institutions."[87]

In a March 10, 2021 unclassified summary of an Intelligence Community Assessment required by Executive Order 13,848,[88] the Intelligence Community concluded that Russia and Iran attempted to influence the 2020

82. *Id.* at § 3171(c).

83. WILFRED WAN ET AL., UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, at vi (Nov. 9, 2021), https://unidir.org/publication/cyber-nuclear-nexus-interactions-and-risks.

84. *See* SAM ALEXANDER ET AL., DEPARTMENT OF HOMELAND SECURITY, COMBATTING TARGETED DISINFORMATION CAMPAIGNS: A WHOLE-OF-SOCIETY ISSUE 4 (2019), https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

85. Countering the Chinese Government and Communist Party's Political Influence Operations Act, S. 2606, 117th Cong. § 3(a)(7) (2021).

86. *Id.* at § 3(a)(8)(E).

87. *Id.* at § 3(a)(8)(F).

88. Exec. Order No. 13,848(1)(a), 83 Fed. Reg. 46,843, 46,843 (Sept. 14, 2018).

U.S. presidential elections.[89] Russian attempts included the promotion of false claims of wrongdoing by President Biden's family members related to Ukraine.[90] The U.S. Treasury Department's OFAC imposed sanctions on sixteen entities and sixteen individuals who assisted the Russian effort[91] and six Iranian individuals and one Iranian entity who assisted the Iranian effort.[92] The sanctions were based on statutory authorities granted to the president.[93]

In June 2021, the Department of Justice seized thirty-three websites run by the Iranian government, claiming that "components of the government of Iran . . . disguised as news organizations or media outlets, targeted the United States with disinformation campaigns and malign influence operations."[94] The legal basis for the seizure were violations of the Iranian Transactions and Sanctions Regulations, which ban the unauthorized export of services to Iran.[95] However, this tactic has been criticized by groups and individuals within the U.S. as a U.S. government attempt to suppress views critical of U.S. government policies arguing that determining what is a legitimate news organization and what is or is not disinformation should be left to individual readers.[96]

Two Iranian nationals were indicted for, among other things, hacking into an election website to obtain confidential voter information.[97] They used this information to disseminate disinformation about the vulnerabilities of voting websites, including a fake video which allegedly showed an individual

89. NATIONAL INTELLIGENCE COUNCIL, FOREIGN THREATS TO THE 2020 US FEDERAL ELECTIONS, at i (2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

90. *Id.* at 4.

91. Release, U.S. Department of the Treasury, Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections (April 15, 2021), https://home.treasury.gov/news/press-releases/jy0126.

92. Press Release, U.S. Department of Treasury, Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election (Nov. 18, 2021), https://home.treasury.gov/news/press-releases/jy0494.

93. *See* International Emergency Powers Act of 1977, 50 U.S.C. § 1701–02; National Emergencies Act of 1976, 50 U.S.C. § 1601–51; Immigration and Nationality Act of 1952, 8 U.S.C. § 1182(f).

94. Press Release, U.S. Department of Justice, United States Seizes Websites Used by the Iranian Islamic Radio and Television Union and Kata'ib Hizballah (June 22, 2021), https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib.

95. 31 C.F.R. § 560.204(a)–(b).

96. *See* Ted Galen Carpenter, *Federal Authorities Are Using 'Disinformation' as a Pretext to Silence Foreign Policy Dissent*, *Commentary*, CATO INSTITUTE (June 29, 2021), https://www.cato.org/commentary/federal-authorities-are-using-disinformation-pretext-silence-foreign-policy-dissent.

97. Devlin Barrett, *U.S. Indicts Two Iranian Hackers Over 2020 Election Misinformation Campaign*, WASHINGTON POST (Nov. 18, 2021), https://www.washingtonpost.com/national-security/iran-hackers-election-2020-indicted/2021/11/18/605ae112-4898-11ec-b05d-3cb9d96eb495_story.html.

casting fraudulent ballots.[98] The U.S. Department of Justice acknowledged that the suspects were presumed to be in Iran but believed that, due to the indictment, the suspects "will forever look over their shoulders as we strive to bring them to justice."[99]

The difficulty of combating these disinformation campaigns is compounded when foreign actors use witting or unwitting U.S. citizens to disseminate the disinformation.[100] The First Amendment limits the ability of the U.S. government to act against U.S. citizens for spreading disinformation since disinformation, in most cases, is not illegal.[101] Therefore, the U.S. government has relied on social media companies to curb the flow of disinformation on their platforms.[102] As revelations about the baneful impact of social media platforms continue to unfold,[103] pressure on social media companies continues to mount.

VI. Update on the Budapest Convention on Cybercrime

November 23, 2021, marks the twentieth anniversary of the first international treaty focused on cybercrime, officially known as the Council of Europe's Convention on Cybercrime, or more informally referred to as the Budapest Convention on Cybercrime (the Budapest Convention).[104] The treaty remains the most relevant and effective international treaty on internet, cyber (computer) crime, and electronic evidence. Among the

98. *Id.*

99. Press Release, Two Iranian National Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 Presidential Election, U.S. Department of Justice (Nov. 18, 2021), https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed.

100. *See, e.g.*, Alicia Wanless & Laura Walters, *How Journalists Become an Unwitting Cog in the Influence Machine*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Oct. 13, 2020), https://carnegieendowment.org/2020/10/13/how-journalists-become-unwitting-cog-in-influence-machine-pub-82923.

101. *See generally* Emily Bazelon, *Free Speech Will Save Our Democracy: The First Amendment in the Age of Disinformation*, N.Y. TIMES MAGAZINE (Oct. 13, 2020), https://www.nytimes.com/2020/10/13/magazine/free-speech.html.

102. *See, e.g.*, Zolan Kanno-Youngs and Cecilia Kang, *Inside the White House-Facebook Rift Over Vaccine Misinformation*, N.Y. TIMES, (Aug. 10, 2021), https://www.nytimes.com/2021/08/10/technology/facebook-vaccine-misinformation.html.

103. *See, e.g.*, *Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds: Hearing Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary*, 117th Cong. (April 27, 2021); *see also Protecting Kids Online: Testimony from a Facebook Whistleblower: Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Data Security of the S. Comm. on Commerce, Science & Transportation*, 117th Cong. (October 5, 2021).

104. The Budapest Convention on Cybercrime, Nov. 23, 2001, T.I.A.S 13174, E.T.S. 185 [hereinafter the Budapest Convention]; Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Jan. 28, 2003, E.T.S. 189 [hereinafter the Additional Protocol] (supplementing the Budapest Convention in 2003, covering the criminalization of acts of a racist and xenophobic nature committed through computer systems).

topics covered by the treaty are the harmonization of national laws, improved investigative techniques and increased cooperation among signatory nations, violations of network security, computer-related forgery and fraud, offenses in connection with child pornography, and offenses related to the infringement of copyrights.[105] Its main objective, as set forth in its preamble, is to pursue a common criminal policy by the signatory member states aimed at the protection of society against cybercrime, especially by the adoption of relevant legislation by the member states and the fostering of international cooperation.[106]

The Budapest Convention, which opened to signatories in November 2001, went into effect on July 1, 2004.[107] As of April 2022, sixty-six states have ratified the treaty, while a number of additional states had signed but have yet to ratify it.[108] The U.S. Senate ratified the treaty in 2006.[109] Russia, while a member of the Council of Europe, has declined to become a signatory, citing national sovereignty issues.[110] Nonetheless, for the last ten years, Russia has made its own proposals for revisions and expansion of the treaty.[111] Two other significant countries, India[112] and Brazil,[113] also have declined to adopt the treaty.

As the Budapest Convention was formulated in the early 2000s, it covers only cybercrimes recognized at the time. It does not account for the

105. *See generally*, The Budapest Convention.
106. *Id.* at Preamble.
107. *Chart of Signatures & Ratifications of Treaty 185*, THE COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (last updated April 13, 2022) (The original four states which signed the treaty—Japan, the U.S., Canada, and South Africa—were non-member observer status states to the Council of Europe).
108. *Id.*
109. *Id.*
110. *See* Davide Giovannelli, *Proposal of United Nations Convention on Countering the Use of Information & Communications Technologies for Criminal Purposes: Comment on the First Draft Text of the Convention*, NATO COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE, https://ccdcoe.org/library/publications/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention (last visited April 13, 2022) ("Russian emphasis on sovereignty in cyberspace, indeed, it is well-noted and it is also the main reason for Russia to not join the 2001 Budapest Convention on fighting cybercrimes, which authorizes cross-border cyber operations.").
111. *See*, *e.g.*, Arjun Ramprasad, *Russia Gives the UN Draft Convention to Fight Cybercrime*, PREVIEWTECH SECURITY NEWS (Aug. 5, 2021), https://previewtech.net/russia-gives-the-un-draft-convention-to-fight-cybercrime.
112. *See* Alexander Seger, *India & the Budapest Convention: Why Not?*, CYBERCRIME CONVENTION COMMITTEE COUNCIL OF EUROPE (Aug. 10, 2016), https://rm.coe.int/16806a6698#:~:text=india%20would%20certainly%20not%20expect,which%20it%20is%20a%20Party.&text=that%20it%20is%20a%20criminal,up%20to%20the%20Budapest%20Convention.
113. Gustavo Rodrigues, *The Budapest Convention on Cybercrime and the controversies over Brazilian membership*, INSTITUTE FOR RESEARCH ON INTERNET AND SOCIETY (Nov. 12, 2021), https://irisbh.com.br/en/the-budapest-convention-on-cybercrime-and-the-controversies-over-brazilian-membership.

exponential expansion of cyber and malicious activity, cloud computing, and digitalization.[114] To address these and other concerns, on May 28, 2021, the Council of Europe adopted the Second Additional Protocol to the Convention on enhanced co-operation and disclosure of electronic evidence (the Second Additional Protocol).[115] As set forth by the Council at the time of the adoption, "Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement are limited by territorial boundaries. As a result, only a very small share of cybercrime that is reported to criminal justice authorities is leading to court decisions."[116]

The Second Additional Protocol provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards.[117] The text is scheduled to be opened for signing by Member State participants in May 2022.[118]

Since its formulation, there have been calls by signatory and non-signatory member states for a more comprehensive version of the Budapest Convention. In July 2021, the Russian government submitted a draft convention to the U.N., recommending it to be used as the basis of a future treaty.[119] The U.S. has indicated consideration of the proposal with modification to account for U.S. norms and policy, which is set to be taken-up by the U.N. in 2022.[120]

---

114. *E.g.*, *id.*

115. Second Additional Protocol to the Convention on Enhanced Co-Operation and Disclosure of Electronic Evidence, May 12, 2022, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/new-treaties [hereinafter Second Additional Protocol].

116. Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe, COUNCIL OF EUROPE (Nov. 17, 2021), https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe [hereinafter Council Statement].

117. *See generally*, Second Additional Protocol, *supra* note 115.

118. *See* Council Statement, *supra* note 116.

119. *United Nations Convention on Countering the use of Information and Communications Technologies for Criminal Purposes*, KOMMERSANT (June 29, 2021) (unofficial translation draft), https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf.

120. Human and First Amendment rights and other concerns with respect to the proposal have been raised by various governments, non-governmental organizations and other constituencies. *See*, *e.g.*, Deborah Brown, *Cybercrime is Dangerous But a New UN Treaty Could Be Worse for Rights*, HUMAN RIGHTS WATCH (Aug. 13, 2021), https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights; *but see* Joyce Hakmeh & Allison Peters, *A New UN Cyber-Treaty? The Way Forward for Supporters of an Open, Free and Secure Internet*, COUNCIL ON FOREIGN RELATIONS (Jan. 13, 2020), https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.