CONTEMPORARY PRACTICE OF THE UNITED STATES RELATING TO INTERNATIONAL LAW

EDITED BY KRISTEN E. EICHENSEHR*

In this section:

* Elizabeth M. Fritz, Joshua A. Goland, Jack Hoover, Phil Tonseth, and Kimberly Veklerov contributed to the preparation of this section.

https://doi.org/10.1017/ajil.2021.54 Published online by Cambridge University Press

General International and U.S. Foreign Relations Law

United States Joins with Allies, Including NATO, to Attribute Malicious Cyber Activities to China

doi:10.1017/ajil.2021.54

In July, the United States, the North Atlantic Treaty Organization (NATO), the European Union (EU), and other allies attributed a variety of malicious cyber activities, including the Microsoft Exchange hack, to China. This joint attribution builds on commitments made in June summits with NATO, the G7, the EU, and the United Kingdom, and is consistent with the Biden administration's multilateral approach to confronting cybersecurity threats and China more generally. Still, critics question whether the administration's efforts will succeed in altering the behavior of states that pose cybersecurity threats to the United States.

Over the past few years, the United States has repeatedly accused China of responsibility for cyber intrusions, beginning with a focus on intellectual property theft. In 2015, the U.S. Department of Justice indicted five members of China's People's Liberation Army (PLA) for stealing trade secrets from six U.S. companies including Westinghouse, Alcoa, and U.S. Steel.[1] Later that year, President Barack Obama and Chinese President Xi Jinping announced a deal to refrain from "conduct[ing] or knowingly support[ing] cyber-enabled theft of intellectual property . . . for commercial advantage" and to "promote international rules of the road for appropriate conduct in cyberspace."[2] But the United States has repeatedly accused China of violating that deal,[3] as detailed in indictments of various Chinese government-linked hackers for compromises of the Equifax credit reporting agency,[4] health insurer Anthem,[5] and hundreds of individual, corporate, and government victims.[6]

[1] U.S. Dep't of Justice Press Release, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *at* https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [https://perma.cc/B72Q-999Q].

[2] Barack Obama, The President's News Conference with President Xi Jinping of China, 2015 Daily Comp. Pres. Doc. 00647, at 1 (Sept. 25, 2015).

[3] *U.S. Accuses China of Violating Bilateral Anti-hacking Deal*, Reuters (Nov. 8, 2018), *at* https://www.reuters.com/article/us-usa-china-cyber-idUSKCN1NE02E.

[4] U.S. Dep't of Justice Press Release, Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), *at* https://www.justice.gov/usao-ndga/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud [https://perma.cc/LN5J-BBH9].

[5] U.S. Dep't of Justice Press Release, Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People (May 9, 2019), *at* https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including [https://perma.cc/F4ZL-2WM4].

[6] U.S. Dep't of Justice Press Release, Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (July 21, 2020), *at* https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion [https://perma.cc/8UJG-E9MK].

On July 19, 2021, the United States and allies accused China of responsibility for hacking hundreds of thousands of computer systems running Microsoft Exchange software.[7] While U.S. officials continued to address the Russian government's hack of SolarWinds, which came to light in December 2020,[8] Microsoft revealed on March 2, 2021 that it had suffered a breach of its Exchange servers and attributed the intrusion to "Hafnium," a group Microsoft called "state-sponsored and operating out of China.[9] Using four previously undiscovered vulnerabilities (commonly known as "zero-days") in the Microsoft Exchange Server email software, the hackers gained access to computer systems and created "web shells," which allowed the hackers administrative access to victim computers even after Microsoft patched the vulnerabilities.[10] Hackers could then use the web shells to execute commands and download malware onto the computers.[11] Although Microsoft's cloud-based "Microsoft 365" email services were not compromised,[12] the hack affected users of on-premises Exchange servers, including small businesses, local governments,[13] and, notably, the European Banking Authority.[14] Estimates suggested that the hack affected 30,000 servers in the United States and hundreds of thousands globally.[15]

To respond to the hack, the U.S. National Security Council established a Unified Coordination Group that for the first time included representatives not just from government agencies, but also from the private sector.[16] The White House has since announced that this "new model for cyber incident response" will serve as a paradigm for future responses.[17]

The government's first public action in response to the compromise came in April, when the Justice Department announced that the Federal Bureau of Investigation successfully

[7] *See* John Hudson & Ellen Nakashima, *U.S., Allies Accuse China of Hacking Microsoft and Condoning Other Cyberattacks*, WASH. POST (July 19, 2021), *at* https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.

[8] Kristen E. Eichensehr, Contemporary Practice of the United States, 115 AJIL 539 (2021).

[9] *HAFNIUM Targeting Exchange Servers With 0-Day Exploits*, MICROSOFT (Mar. 2, 2021), *at* https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers.

[10] Brian Krebs, *At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software*, KREBS ON SECURITY (Mar. 5, 2021), *at* https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software.

[11] *Id.*

[12] Frank Bajak, Eric Tucker & Matt O'Brien, *Microsoft Server Hack Has Victims Hustling to Stop Intruders*, AP NEWS (Mar. 8, 2021), *at* https://apnews.com/article/technology-politics-national-security-hacking-email-4813d462835dcf54cd1397adb94d468b.

[13] Krebs, *supra* note 10.

[14] Eur. Banking Auth. Press Release, Cyber-Attack on the European Banking Authority (Mar. 7, 2021), *at* https://www.eba.europa.eu/cyber-attack-european-banking-authority.

[15] Bajak, Tucker & O'Brien, *supra* note 12; Andy Greenberg, *Chinese Hacking Spree Hit an "Astronomical" Number of Victims*, WIRED (Mar. 5, 2021), *at* https://www.wired.com/story/china-microsoft-exchange-server-hack-victims.

[16] White House Press Release, Statements by Press Secretary Jen Psaki & Deputy National Security Advisor for Cyber Anne Neuberger on Microsoft Exchange Vulnerabilities UCG (Mar. 17, 2021), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/17/statements-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-anne-neuberger-on-microsoft-exchange-vulnerabilities-ucg [https://perma.cc/VS6U-7XSQ].

[17] White House Press Release, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China (July 19, 2021), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china [https://perma.cc/J89V-6UPJ].

https://doi.org/10.1017/ajil.2021.54 Published online by Cambridge University Press

carried out a court-authorized operation to remove the malicious web shells remaining on compromised systems.[18] The operation terminated hackers' access to the systems, but did not remove any malware that had already been downloaded.[19]

Then on July 19, the United States joined with the EU, NATO, and other allied countries to attribute the Microsoft Exchange hack to actors affiliated with China's Ministry of State Security (MSS) and to call out China for "foster[ing] an intelligence enterprise that includes contract hackers who also conduct unsanctioned cyber operations worldwide."[20] The White House "[a]ttribut[ed] with a high degree of confidence that malicious cyber actors affiliated with [the People's Republic of China's (PRC)] MSS conducted cyber espionage operations utilizing the zero-day vulnerabilities in Microsoft Exchange Server."[21] Furthermore, the United States noted:

> [H]ackers with a history of working for the PRC Ministry of State Security (MSS) have engaged in ransomware attacks, cyber enabled extortion, crypto-jacking, and rank theft from victims around the world, all for financial gain.
>
> In some cases, we are aware that PRC government-affiliated cyber operators have conducted ransomware operations against private companies that have included ransom demands of millions of dollars.[22]

The White House declared that "[t]he PRC's pattern of irresponsible behavior in cyberspace is inconsistent with its stated objective of being seen as a responsible leader in the world."[23]

In a separate statement, the State Department explained:

> Apart from the PRC's direct commitments not to engage in cyber-enabled theft of intellectual property for commercial gain, the international community has laid out clear expectations and guidelines for what constitutes responsible behavior in cyberspace. Responsible states do not indiscriminately compromise global network security nor knowingly harbor cyber criminals—let alone sponsor or collaborate with them. These contract hackers cost governments and businesses billions of dollars in stolen intellectual property, ransom payments, and cybersecurity mitigation efforts, all while the MSS had them on its payroll.[24]

Marking its first public attribution of malicious cyber activities to China,[25] NATO announced:

[18] U.S. Dep't of Justice Press Release, Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities (Apr. 13, 2021), *at* https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange [https://perma.cc/9XBK-M5G7].

[19] *Id.*

[20] White House Press Release, *supra* note 17.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] U.S. Dep't of State Press Release, Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace (July 19, 2021), *at* https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace [https://perma.cc/FY2N-ZBEP].

[25] *See* White House Press Release, Background Press Call by Senior Administration Officials on Malicious Cyber Activity Attributable to the People's Republic of China (July 19, 2021), *at* https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/19/background-press-call-by-senior-administration-officials-on-malicious-cyber-activity-attributable-to-the-peoples-republic-of-china [https://perma.cc/CMR3-56SF].

https://doi.org/10.1017/ajil.2021.54 Published online by Cambridge University Press

> We stand in solidarity with all those who have been affected by recent malicious cyber activities including the Microsoft Exchange Server compromise. Such malicious cyber activities undermine security, confidence and stability in cyberspace. We acknowledge national statements by Allies, such as Canada, the United Kingdom, and the United States, attributing responsibility for the Microsoft Exchange Server compromise to the People's Republic of China. In line with our recent Brussels Summit Communiqué, we call on all States, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace.[26]

Other U.S. allies followed suit in attributing the Microsoft Exchange hack and other malicious activities to China. The UK National Cyber Security Centre assessed with "almost certain[ty]" that the Exchange hack "was initiated and exploited by a Chinese state-backed threat actor," and UK Foreign Secretary Dominic Raab asserted that it followed "a reckless but familiar pattern of behavior" and that "[t]he Chinese Government must end this systematic cyber sabotage and can expect to be held [to] account if it does not."[27] The EU stated that it "strongly denounce[s] these malicious cyber activities, which are undertaken in contradiction with the norms of responsible state behaviour as endorsed by all UN member states," and that it "urge[s] the Chinese authorities to adhere to these norms and not allow its territory to be used for malicious cyber activities, and [to] take all appropriate measures and reasonably available and feasible steps to detect, investigate and address the situation."[28] Canada,[29] Japan,[30] Australia,[31] and New Zealand,[32] among others, released similar statements.[33]

[26] N. Atl. Treaty Org. Press Release 120, Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise (July 19, 2021), *at* https://www.nato.int/cps/en/natohq/news_185863.htm.

[27] UK Government Press Release, UK and Allies Hold Chinese State Responsible for a Pervasive Pattern of Hacking (July 19, 2021), *at* https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking.

[28] European Council Press Release 11:35, China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action Against Malicious Cyber Activities Undertaken from Its Territory (July 19, 2021), *at* https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory.

[29] Glob. Affs. Can. Press Release, Statement on China's Cyber Campaigns (July 19, 2021), *at* https://www.canada.ca/en/global-affairs/news/2021/07/statement-on-chinas-cyber-campaigns.html.

[30] Ministry Foreign Affs. Japan Press Release, Cases of Cyberattacks Including Those by a Group Known as APT40 Which the Chinese Government Is Behind (July 19, 2021), *at* https://www.mofa.go.jp/press/danwa/press6e_000312.html.

[31] Minister for Home Affs. Karen Andrews Press Release, Joint Media Release with Senator the Hon Marise Payne and the Hon Peter Dutton MP – Australia Joins International Partners in Attribution of Malicious Cyber Activity to China (July 19, 2021), *at* https://minister.homeaffairs.gov.au/KarenAndrews/Pages/aus-joins-intl-partners-in-attribution-of-malicious-cyber-activity-to-china.aspx.

[32] Gov't Comm. Sec. Bureau Minister Andrew Little Press Release, New Zealand Condemns Malicious Cyber Activity by Chinese State-Sponsored Actors (July 19, 2021), *at* https://www.beehive.govt.nz/release/new-zealand-condemns-malicious-cyber-activity-chinese-state-sponsored-actors.

[33] Many European states released statements in support of the EU's announcement. *See* Cyber @ State Dept (@State_Cyber), TWITTER, *at* https://twitter.com/state_cyber?lang=en [https://perma.cc/EK2X-8M6B] (compiling these statements, dated July 19, 2021, from Estonia, Slovenia, Finland, Denmark, Poland, the Czech Republic, Latvia, Albania, Iceland, Belgium, the Netherlands, Austria, Romania, Lithuania, North Macedonia, and Sweden).

https://doi.org/10.1017/ajil.2021.54 Published online by Cambridge University Press

China denied the allegations and accused the United States of cyberattacks.[34] In comments to the press, Chinese Foreign Ministry Spokesperson Zhao Lijian stated that "[t]he US ganged up with its allies to make groundless accusations out of thin air against China on the cyber security issue. This act confuses right with wrong and smears and suppresses China out of political purpose. China will never accept this."[35] Asked specifically about NATO's statement, Zhao alleged that "[b]y introducing military alliance into cyberspace, NATO is not making itself more secure" and instead "might spur cyber arms race, increase risks of cyber friction and conflict between countries, and undermine international peace and security."[36]

The coordinated attribution to China built on U.S. diplomatic efforts, including meetings and summits in June with NATO, the G7, the EU, and the United Kingdom. In announcing the attribution, the White House explained, "[f]rom the G7 and EU commitments around ransomware to NATO adopting a new cyber defense policy for the first time in seven years, the President is putting forward a common cyber approach with our allies and laying down clear expectations and markers on how responsible nations behave in cyberspace."[37] NATO endorsed a Comprehensive Cyber Defence Policy in its June Brussels Summit Communiqué, noting that "[c]yber threats to the security of the Alliance are complex, destructive, coercive, and becoming ever more frequent," and citing recent "ransomware incidents and other malicious cyber activity targeting our critical infrastructure and democratic institutions."[38] The Communiqué called out Russia's "hybrid actions," including "attempted interference in Allied elections and democratic processes; . . . widespread disinformation campaigns; malicious cyber activities; and turning a blind eye to cyber criminals operating from its territory," and called on China to "act responsibly in the international system, including in the space, cyber, and maritime domains."[39] The Communiqué reaffirmed that NATO "is determined to employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law."[40]

The G7's Carbis Bay Summit Communiqué in June likewise addressed malicious cyber actions. The G7 leaders pledged to "work together to urgently address the escalating shared threat from criminal ransomware networks" and "call[ed] on all states to urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions."[41] The Communiqué specifically urged Russia to

[34] Joe McDonald, *China Rejects Hacking Charges, Accuses US of Cyberspying*, AP NEWS (July 20, 2021), *at* https://apnews.com/article/technology-business-china-hacking-6cd7d59f1b6aa4a0539d987e5340b705.

[35] Embassy of China in the U.S. Press Release, Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on July 20, 2021, *at* http://www.china-embassy.org/eng/fyrth/t1893769.htm; *see also* Embassy of China in the UK Press Release, Embassy Spokesperson's Comment on the Remarks by the UK Side About Cyber Attack (July 20, 2021), *at* http://www.chinese-embassy.org.uk/eng/PressandMedia/Spokepersons/t1893648.htm.

[36] Embassy of China in the U.S. Press Release, *supra* note 35.

[37] White House Press Release, *supra* note 17.

[38] N. Atl. Treaty Org. Press Release 086, Brussels Summit Communiqué (June 14, 2021) *at* https://www.nato.int/cps/en/natohq/news_185000.htm.

[39] *Id.*

[40] *Id.*

[41] White House Press Release, Carbis Bay G7 Summit Communiqué (June 13, 2021), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/ [https://perma.cc/MD3C-CFFN].

https://doi.org/10.1017/ajil.2021.54 Published online by Cambridge University Press

"identify, disrupt, and hold to account those within its borders who conduct ransomware attacks, abuse virtual currency to launder ransoms, and other cybercrimes."[42] More broadly, the G7 leaders also pledged "to work together to further a common understanding of how existing international law applies to cyberspace," including working through "the UN and other international fora."[43]

In June meetings, the UK and EU each agreed to join the United States in combatting mutual cyber threats. As part of the "New Atlantic Charter," the United States and the UK pledged "to promote the framework of responsible state behaviour in cyberspace" and to maintain collective security "against the full spectrum of modern threats, including cyber threats."[44] Later in June, the United States and EU announced a new ransomware working group.[45]

These cyber-specific agreements constitute one part of the Biden administration's broader program of shoring up alliances to counter China on both security and economic issues. During the June summits, NATO declared that "China's stated ambitions and assertive behaviour present systemic challenges to the rules-based international order and to areas relevant to Alliance security."[46] The G7 also laid down a broad policy of countering China, asserting, "[w]ith regard to China, and competition in the global economy, we will continue to consult on collective approaches to challenging non-market policies and practices which undermine the fair and transparent operation of the global economy."[47] The Biden administration also worked with the EU to suspend the seventeen-year Airbus-Boeing trade dispute, which began in 2004 when the United States complained to the World Trade Organization that the EU was illegally subsidizing Airbus to Boeing's disadvantage.[48] The dispute led both sides to impose an escalating series of retaliatory tariffs,[49] but the United States and EU agreed in June to lift those tariffs for the next five years, joining forces "to challenge and counter China's nonmarket practices in this sector."[50] President Biden elaborated that the U.S.-EU collaboration in the aircraft industry is "a model we can build on for other challenges posed by China's economic model."[51]

It remains to be seen whether coordinated actions among U.S. allies can effectively address cyber threats. In just the last few months, several significant ransomware attacks have

[42] *Id.*

[43] *Id.*

[44] White House Press Release, New Atlantic Charter, § 5 (June 10, 2021), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/10/the-new-atlantic-charter [https://perma.cc/3TKG-QUDD].

[45] European Council Press Release 15:00, Joint EU-US Statement Following the EU-US Justice and Home Affairs Ministerial Meeting (June 22, 2021), *at* https://www.consilium.europa.eu/en/press/press-releases/2021/06/22/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting; *see also* Laurens Cerulus & Clothilde Goujard, *EU, US Launch Initiative Against Ransomware*, POLITICO (June 22, 2021), *at* https://www.politico.eu/article/eu-us-launch-ransomware-cooperation-group.

[46] N. Atl. Treaty Org. Press Release, *supra* note 38.

[47] White House Press Release, *supra* note 41.

[48] Doug Michaels, Andrew Restuccia & Doug Cameron, *US and EU Agree to Suspend Airbus-Boeing Trade Fight*, WALL ST. J. (June 15, 2021), *at* https://www.wsj.com/articles/u-s-and-eu-near-deal-on-boeing-airbus-trade-fight-11623747870.

[49] *Id.*

[50] Joseph R. Biden, Jr., Statement on the Tariff Suspension Agreement with the European Union on the Boeing-Airbus Trade Dispute, 2021 DAILY COMP. PRES. DOC. 00510, at 1 (June 15, 2021).

[51] *Id.*; *see also* Michael Birnbaum, Anne Gearan & David J. Lynch, *Biden, E.U. End 17-Year Airbus-Boeing Trade Dispute, Seek to Calm Relations After Trump*, WASH. POST (June 15, 2021), *at* https://www.washingtonpost.com/politics/biden-eu-tariffs/2021/06/15/88fcfe92-cd4c-11eb-a7f1-52b8870bef7c_story.html.

https://doi.org/10.1017/ajil.2021.54 Published online by Cambridge University Press

occurred. In May, ransomware directed against Colonial Pipeline prompted the East Coast's biggest gasoline supplier to shut down its pipeline, causing gasoline shortages.[52] Then in June, JBS, the world's largest meat company, paid an eleven million dollar ransom to avoid further disruptions to supply lines.[53] A third ransomware attack against a software provider, Kaseya, infected an estimated 1,500 small businesses, which faced ransom demands that reportedly ranged from $45,000 to $5 million.[54]

In light of these ransomware incidents, all of which were carried out by Russia-based hacking groups, Biden has repeatedly raised concerns about ransomware with Russian President Vladimir Putin. At a June summit in Geneva, Biden proposed designating sixteen critical infrastructure sectors, including the energy sector and water systems, as "off limits to attack."[55] During a July phone call with Putin, Biden expressed that the United States expects Russia to stop ransomware attacks emanating from Russia, promising to treat continued attacks as national security threats rather than criminal acts.[56] Shortly after the phone call, one of the Russia-based ransomware groups went offline, for reasons that remain unclear, but reappeared in September.[57]

Critics argue that the White House must do more to prevent and combat cyberattacks. Sen. Angus King (I-ME), who co-chairs the Cyberspace Solarium Commission, said in June that the U.S. tactics of sanctions and indictments "haven't been nearly punitive enough."[58] He asserted, "[w]e've been a cheap date in cyber where we've been attacked repeatedly in a variety of ways [with] no real serious response."[59] Others specifically urged the United States to sanction China for the Microsoft Exchange hack.[60] In a background call with reporters, a senior Biden administration official warned that "[t]he U.S. and our allies and partners are not ruling out further actions to hold the PRC accountable."[61]

[52] David E. Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, N.Y. TIMES (May 14, 2021), *at* https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. Colonial Pipeline paid several million dollars in Bitcoins as a ransom, much of which the Justice Department subsequently recovered. Katie Benner & Nicole Perlroth, *U.S. Seizes Share of Ransom from Hackers in Colonial Pipeline Attack*, N.Y. TIMES (June 7, 2021), *at* https://www.nytimes.com/2021/06/07/us/politics/pipeline-attack.html.

[53] Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, WALL ST. J. (June 9, 2021), *at* https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

[54] Charlie Osborne, *Updated Kaseya Ransomware Attack FAQ: What We Know Now*, ZDNET (July 23, 2021), *at* https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now.

[55] Joseph R. Biden, Jr., The President's News Conference in Geneva, Switzerland, 2021 DAILY COMP. PRES. DOC. 00513, at 2 (June 16, 2021).

[56] David E. Sanger & Nicole Perlroth, *Biden Warns Putin to Act Against Ransomware Groups, or U.S. Will Strike Back*, N.Y. TIMES (July 9, 2021), *at* https://www.nytimes.com/2021/07/09/us/politics/biden-putin-ransomware-russia.html.

[57] David E. Sanger, *Russia's Most Aggressive Ransomware Group Disappeared. It's Unclear Who Made That Happen.*, N.Y. TIMES (July 13, 2021), *at* https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html; William Turton & Kartikay Mehrotra, *Notorious Russian Ransomware Group 'REvil' Has Reappeared*, BLOOMBERG (Sept. 7, 2021), at https://www.bloomberg.com/news/articles/2021-09-07/notorious-russian-ransomware-group-revil-has-reappeared.

[58] Joseph Marks & Aaron Schaffer, *The Cybersecurity 202: Angus King Says It's Time to Get Tougher on Russian Hackers*, WASH. POST (June 30, 2021), *at* https://www.washingtonpost.com/politics/2021/06/30/cybersecurity-202-angus-king-says-its-time-get-tougher-russian-hackers (alteration in original).

[59] *Id.*

[60] Dmitri Alperovitch & Ian Ward, *The White House Responded to the Chinese Hacks of the Microsoft Exchange Servers This Week. Is It Enough?*, LAWFARE (July 21, 2021), *at* https://www.lawfareblog.com/white-house-responded-chinese-hacks-microsoft-exchange-servers-week-it-enough.

[61] White House Press Release, *supra* note 25.

https://doi.org/10.1017/ajil.2021.54 Published online by Cambridge University Press