including recent air strikes, continue to cause civilian casualties and suffering, and . . . reaffirmed the U.S. commitment to work alongside the African Union and regional partners to help Ethiopians peacefully resolve the conflict."[52] Later the same day, media reported that drone strikes in Tigray killed nineteen people, including women and children at a flour mill.[53] Nonetheless, by late January, after a visit by AU High Representative Obasanjo to Addis Ababa and the Tigrayan capital, UN Secretary-General Guterres expressed optimism that "there is now a demonstrable effort to make peace."[54] Guterres noted, however, that "[o]ngoing military operations in some parts of Ethiopia remain a challenge to the peace process" and that the humanitarian situation is concerning.[55]

On March 24, Ethiopia's government announced a "humanitarian truce" to permit food and other aid into Tigray, and the Tigrayan government responded "that if sufficient humanitarian aid arrived to meet the needs on the ground 'within a reasonable timeframe,' then it, too, would be 'committed to implementing a cessation of hostilities effective immediately.'"[56] The AU, UN, and United States welcomed the declarations, expressing hope that aid will quickly reach those in need and urging the parties to work toward a permanent end to the conflict.[57]

International Criminal Law

The Biden Administration Cracks Down on Ransomware

doi:10.1017/ajil.2022.12

Following several significant ransomware attacks against U.S. companies last summer, the Biden administration has acted internationally and domestically to punish the perpetrators and prevent future attacks. As part of a shift from addressing ransomware as a law

[52] White House Press Release, *supra* note 51.

[53] Walsh, *supra* note 51; *Ethiopia: 19 People Killed in Latest Drone Strikes in Tigray*, GUARDIAN (Jan. 11, 2022), *at* https://www.theguardian.com/world/2022/jan/11/ethiopia-19-people-killed-in-latest-drone-strikes-in-tigray.

[54] UN Press Release, Secretary-General Statement on Ethiopia (Jan. 19, 2022), *at* https://www.un.org/sg/en/node/261460; *UN Chief Cites "Demonstrable Effort" at Peace in Ethiopia*, ABC NEWS (Jan. 19, 2022), *at* https://abcnews.go.com/International/wireStory/chief-demonstrable-effort-peace-ethiopia-82352791.

[55] UN Press Release, *supra* note 54.

[56] Abdi Latif Dahir & Simon Marks, *Ethiopia Declares "Humanitarian Truce" in War-Ravaged Tigray Region*, N.Y. TIMES (Mar. 24, 2022), *at* https://www.nytimes.com/2022/03/24/world/africa/ethiopia-tigray-conflict-truce.html.

[57] African Union Press Release, AUC Chairperson Welcomes the Declaration of an Indefinite Humanitarian Truce by the Ethiopian Government in Tigray Region (Mar. 25, 2022), *at* https://au.int/en/pressreleases/20220325/auc-chairperson-welcomes-declaration-indefinite-humanitarian-truce-tigray; United Nations, Welcoming Ethiopian Government's Declaration of Indefinite Humanitarian Truce, Secretary-General Urges All Parties to Take Steps Towards Lasting Ceasefire (Mar. 25, 2022), *at* https://www.un.org/press/en/2022/sgsm21207.doc.htm; U.S. Dep't of State Press Release, Declaration of a Humanitarian Truce by the Government of Ethiopia (Mar. 24, 2022), *at* https://www.state.gov/declaration-of-a-humanitarian-truce-by-the-government-of-ethiopia/ [https://perma.cc/VU47-523C]; U.S. Dep't of State, Department Press Briefing-March 25, 2022 (Mar. 25, 2022), *at* https://www.state.gov/briefings/department-press-briefing-march-25-2022/ [https://perma.cc/3M8E-5VPB].

enforcement matter to treating it as a national security threat,[1] the administration has targeted ransomware infrastructure, clawing back ransom payments and disrupting ransomware groups, while also targeting individual ransomware operators with indictments and sanctions. The administration is also offering rewards for information leading to the identification and arrest of ransomware operators and continuing diplomatic efforts aimed at convincing other governments to act against ransomware groups.[2] Whether the administration's holistic approach to combatting ransomware will prove effective in decreasing ransomware attacks remains to be seen.

Ransomware is a type of malicious software that is "designed to encrypt files on a device, rendering any files and the systems that rely on them unusable," and then ransomware operators "demand ransom in exchange for decryption."[3] Sometimes ransom demands are accompanied by threats "to publish exfiltrated data, or sell it on the dark web" if the ransom is not paid.[4] In recent years, ransomware attacks have disrupted state and local governments, caused outages at healthcare facilities, and targeted other critical infrastructure.[5] Ransomware incidents have increased significantly in frequency, cost, and severity.[6] For example, U.S. authorities "observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors" in 2021,[7] and according to the U.S. Treasury Department, "[r]eported ransomware payments in the United States . . . reached $590 million in the first half of 2021," up from $416 million reported in all of 2020,[8] which in turn quadrupled the amount paid in 2019.[9]

Beginning in May 2021, a series of significant ransomware attacks raised the profile of ransomware as a national security concern for the U.S. government and the public.[10] The first incident disabled the networks of Colonial Pipeline Co. and became the "largest publicly

[1] *See* Julian E. Barnes, *U.S. Military Has Acted Against Ransomware Groups, General Acknowledges*, N.Y. Times (Dec. 5, 2021), *at* https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.

[2] *See, e.g.*, Kristen E. Eichensehr, Contemporary Practice of the United States, 115 AJIL 715, 715–21 (2021).

[3] Cybersecurity & Infrastructure Security Agency, Stop Ransomware, *Ransomware 101*, *at* https://www.cisa.gov/stopransomware/ransomware-101 [https://perma.cc/3Y6L-4RG8].

[4] U.S. Secret Service Cybercrime Investigations, Preparing for a Cyber Incident: A Guide to Ransomware, *available at* https://www.secretservice.gov/sites/default/files/reports/2021-11/Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.1.pdf [https://perma.cc/2X9N-ZUXN].

[5] *See, e.g.*, Luke Broadwater, *Baltimore Transfers $6 Million to Pay for Ransomware Attack; City Considers Insurance Against Hacks*, Balt. Sun (Aug. 28, 2019), *at* https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html; Nicole Sganga, Catherine Herridge & Musadiq Bidar, *Foreign Hacking Group Targets Hospitals, Clinics with Ransomware Attacks, Says New Report*, CBS News (Oct. 7, 2021), *at* https://www.cbsnews.com/news/cyberattacks-ransomware-hacking-hospitals-target-foreign-groups.

[6] *See, e.g.*, Institute for Security & Technology Ransomware Task Force, *Combatting Ransomware* 7 (2021), *available at* https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf.

[7] Cybersecurity & Infrastructure Security Agency, *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware* (Feb. 9, 2022), *at* https://www.cisa.gov/uscert/ncas/alerts/aa22-040a [https://perma.cc/C335-MZFL].

[8] U.S. Dep't of the Treasury Press Release, Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange (Nov. 8, 2021), *at* https://home.treasury.gov/news/press-releases/jy0471.

[9] U.S. Dep't of the Treasury Press Release, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), *at* https://home.treasury.gov/news/press-releases/jy0364.

[10] Eichensehr, *supra* note 2, at 720–21.

https://doi.org/10.1017/ajil.2022.12 Published online by Cambridge University Press

disclosed cyber attack against critical infrastructure in the [United States]."[11] Although the attack did not directly affect the systems regulating the flow and delivery of oil, Colonial Pipeline shut down the pipeline to prevent the ransomware's spread after it infected other parts of the company's network.[12] The pipeline spans Texas to New Jersey, and its closure left consumers vulnerable to shortages, partly due to a wave of panic buying across the country.[13] The FBI quickly attributed the incident to a group called DarkSide.[14] Eventually, Colonial Pipeline paid a $5 million ransom in Bitcoin to decrypt its compromised data.[15] In a press conference, President Biden noted that "we do not believe the Russian government was involved in this attack. But we do have strong reason to believe that criminals who did the attack are living in Russia," and he explained that "[w]e have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks."[16]

Weeks later, JBS, "[t]he world's largest meat processor," suffered a ransomware attack that shut down "U.S. beef plants and disrupted operations at poultry and pork plants."[17] The FBI attributed the attack to REvil, a Russia-based "ransomware as a service" group that was formerly affiliated with DarkSide.[18] JBS paid the hackers $11 million dollars in Bitcoin and restored its operations quickly,[19] though the interruption caused meat prices to rise around the world.[20] The White House noted that it was "engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbor ransomware criminals."[21]

The third significant ransomware incident struck over the July 4 weekend, affecting Kaseya, a company that sells software to managed service providers who in turn use it to support other

[11] Sean Michael Kerner, *Colonial Pipeline Hack Explained: Everything You Need to Know*, TECHTARGET (July 7, 2021), *at* https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[12] *Id.*

[13] Clifford Krauss, Niraj Chokshi & David E. Sanger, *Gas Pipeline Hack Leads to Panic Buying in the Southeast*, N.Y. TIMES (May 11, 2021), *at* https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html.

[14] David E. Sanger & Nicole Perlroth, *F.B.I Identifies Group Behind Pipeline Hack*, N.Y. TIMES (May 10, 2021), *at* https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html.

[15] Michael D. Shear, Nicole Perlroth & Clifford Krauss, *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES (May 13, 2021; updated June 7, 2021), *at* https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html.

[16] White House Press Release, Remarks by President Biden on the Colonial Pipeline Incident (May 13, 2021), *at* https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident [https://perma.cc/9KDW-JDN3].

[17] Rebecca Robbins, *Meat Processor JBS Paid $11 Million in Ransom to Hackers*, N.Y. TIMES (June 9, 2021), *at* https://www.nytimes.com/2021/06/09/business/jbs-cyberattack-ransom.html.

[18] Nicole Perlroth, Noam Scheiber & Julie Creswell, *Russian Cybercriminal Group Was Behind Meat Plant Attack, F.B.I. Says*, N.Y. TIMES (June 2, 2021), *at* https://www.nytimes.com/2021/06/02/business/jbs-beef-cyberattack.html; Federal Bureau of Investigation Press Release, FBI Statement on JBS Attack (June 2, 2021), *at* https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-jbs-cyberattack [https://perma.cc/NN4V-FV55].

[19] Robbins, *supra* note 17.

[20] *See* Jacob Bunge & Jesse Newman, *Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants*, WALL ST. J. (June 11, 2021), *at* https://www.wsj.com/articles/ransomware-attack-roiled-meat-giant-jbs-then-spilled-over-to-farmers-and-restaurants-11623403800.

[21] White House Press Release, Press Gaggle by Principal Deputy Press Secretary Karine Jean-Pierre Aboard Air Force One En Route Tulsa, OK (June 1, 2021), *at* https://www.whitehouse.gov/briefing-room/press-briefings/2021/06/01/press-gaggle-by-principal-deputy-press-secretary-karine-jean-pierre-aboard-air-force-one-en-route-tulsa-ok [https://perma.cc/SDC7-SYFX].

https://doi.org/10.1017/ajil.2022.12 Published online by Cambridge University Press

businesses.[22] REvil demanded a $70 million ransom,[23] but Kaseya declined to pay and ultimately obtained a decryption key from a "trusted third party."[24] After the Kaseya incident, President Biden had a call with Russian President Vladimir Putin and "underscored the need for Russia to take action to disrupt ransomware groups operating in Russia" and emphasized that "the United States will take any necessary action to defend its people and its critical infrastructure."[25] Days later, REvil disappeared from the internet,[26] albeit temporarily.[27]

In response to these ransomware incidents, the Biden administration began a whole-of government effort to address ransomware as a national security priority. The United States has reportedly conducted several operations both to recover ransom payments and to disrupt ransomware operators. In June 2021, federal authorities recovered $2.3 million of the ransom that Colonial Pipeline had paid to DarkSide in Bitcoin.[28] In announcing the seizure, executed pursuant to a warrant issued by a federal judge, Deputy Attorney General Lisa O. Monaco explained, "[f]ollowing the money remains one of the most basic, yet powerful tools we have," and noted that the seizure "demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises."[29] The Justice Department explained,

> by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address, for which the FBI has the "private key," or the rough equivalent of a password needed to access assets accessible from the specific Bitcoin address.[30]

[22] 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.

[23] Liam Tung, *Kaseya Ransomware Attack: US Launches Investigation as Gang Demands Giant $70 Million Payment*, ZDNet (July 5, 2021), *at* https://www.zdnet.com/article/kaseya-ransomware-attack-us-launches-investigation-as-gang-demands-giant-70-million-payment; *see also* Joseph Menn, *Kaseya Ransomware Attack Sets Off Race to Hack Service Providers—Researchers*, Reuters (Aug. 3, 2021), *at* https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03.

[24] Rachel Lerman, *Company Hit by Massive Ransomware Attack Obtains Key to Unlock Customer Files*, Wash. Post (July 26, 2021), *at* https://www.washingtonpost.com/technology/2021/07/22/kaseya-ransomware-revil-key.

[25] White House Press Release, Readout of President Joseph R. Biden, Jr. Call with President Vladimir Putin of Russia (July 9, 2021), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/readout-of-president-joseph-r-biden-jr-call-with-president-vladimir-putin-of-russia-2 [https://perma.cc/7GJ3-ZKZJ]; 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.

[26] 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.

[27] *See* Julian E. Barnes, *Russia Influences Hackers but Stops Short of Directing Them, Report Says*, N.Y. Times (Sept. 9, 2021), *at* https://www.nytimes.com/2021/09/09/us/politics/russia-ransomware-hackers.html.

[28] Ellen Nakashima, *Feds Recover More Than $2 Million in Ransomware Payments from Colonial Pipeline Hackers*, Wash. Post (June 7, 2021), *at* https://www.washingtonpost.com/business/2021/06/07/colonial-pipeline-ransomware-payment-recovered.

[29] U.S. Dep't of Justice Press Release, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), *at* https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside [https://perma.cc/6R8Z-5H2E].

[30] *Id.*

https://doi.org/10.1017/ajil.2022.12 Published online by Cambridge University Press

How officials obtained the key remains unclear.[31]

Reports indicate that the United States disrupted REvil's infrastructure in the fall of 2021, prompting the group to shut down.[32] According to the *Washington Post*, a foreign government hacked REvil's servers in the summer of 2021, and in October, after cooperation with the FBI, U.S. Cyber Command (CyberCom) "blocked [REvil's] website by hijacking its traffic," and thereby "deprived the criminals of the platform they used to extort their victims."[33] CyberCom's actions caused REvil to shut down again, at least temporarily, due to fear of discovery.[34] A REvil leader with the username o_neday wrote that "'[t]he server was compromised' . . . 'and they are looking for me,'" following up with "'Good luck everyone, I'm taking off.'"[35] In December, Gen. Paul M. Nakasone, who leads both CyberCom and the National Security Agency, noted that the government had shifted away from treating ransomware as "the responsibility of law enforcement" and publicly confirmed that "'with a number of elements of our government, we have taken actions and we have imposed costs,'" though he declined to specify which groups had been targeted.[36]

The Biden administration has also targeted the financial infrastructure underlying ransomware operations by imposing sanctions on cryptocurrency exchanges that launder ransom payments. On September 21, 2021, the Treasury Department used authority provided by the Obama administration's cybersecurity sanctions executive order to sanction Suex, "a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors," including "transactions involving illicit proceeds from at least eight ransomware variants."[37] According to the Treasury Department, "[a]nalysis of known SUEX transactions shows that over 40% of SUEX's known transaction history is associated with illicit actors."[38] In November, the Treasury Department sanctioned another virtual currency exchange, Chatex, for facilitating transactions on behalf of many ransomware actors.[39] The Treasury Department alleged that half of Chatex's "known transactions . . . are directly traced to illicit or high-risk activities such as darknet markets, high-risk exchanges, and ransomware," and Chatex has "direct ties with SUEX."[40] The Department also designated three companies for providing "material support and assistance to Chatex" by "set[ting] up infrastructure for Chatex, enabling [its] operations."[41]

[31] Nakashima, *supra* note 28.

[32] Ellen Nakashima & Dalton Bennett, *A Ransomware Gang Shut Down After Cybercom Hijacked Its Site and It Discovered It Had Been Hacked*, WASH. POST (Nov. 3, 2021), *at* https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] Barnes, *supra* note 1. Notably, media reports suggest that CyberCom also undertook operations against ransomware operators prior to the 2020 election. *See* Ellen Nakashima, *Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election*, WASH. POST (Oct. 9, 2020), *at* https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.

[37] U.S. Dep't of the Treasury Press Release, *supra* note 9; *see also* Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016) (amending Exec. Order No. 13,694 of Apr. 1, 2015).

[38] U.S. Dep't of the Treasury Press Release, *supra* note 9.

[39] U.S. Dep't of the Treasury Press Release, *supra* note 8.

[40] *Id.*

[41] *Id.*

https://doi.org/10.1017/ajil.2022.12 Published online by Cambridge University Press

In addition to its efforts to target ransomware infrastructure, the Biden administration has targeted individual hackers through criminal indictments and sanctions. On November 8, 2021, the Justice Department announced charges against two ransomware operators linked to REvil.[42] In announcing the indictments, Attorney General Merrick Garland said that "[c]ybercrime is a serious threat to our country: to our personal safety, to the health of our economy, and to our national security," and continued, explaining that "[t]he United States, together with our allies, will do everything in our power to identify the perpetrators of ransomware attacks, to bring them to justice, and to recover the funds they have stolen from their victims."[43] The first indictment charged a Ukrainian national, Yaroslav Vasinskyi, for his role in the July ransomware attack on Kaseya.[44] Vasinskyi was arrested in Poland and extradited to the United States for prosecution.[45] The second indictment charges Russian citizen Yevgeniy Polyanin with crimes related to "conducting Sodinokibi/REvil ransomware attacks against multiple victims, including businesses and government entities in Texas on or about Aug. 16, 2019."[46] Simultaneously, the Department announced "the seizure of $6.1 million in funds traceable to alleged ransom payments" to Polyanin.[47] The Warrant to Seize Property Subject to Forfeiture denoted seizure of a cashier's check totaling $6,123,652.21, but also requested "[a]ll funds up to $13 million in the FTX Trading Limited account" in Polyanin's name.[48] Both defendants face charges of "conspiracy to commit fraud and related activity in connection with computers, substantive counts of damage to protected computers, and conspiracy to commit money laundering," and if convicted on all counts could be sentenced to more than one hundred years in prison.[49] The same day that the indictments were released, the Treasury Department sanctioned both Vasinskyi and Polyanin.[50]

Rounding out a carrot-and-stick approach, the State Department now offers rewards for information leading to ransomware operators. In July 2021, the Department's Rewards for Justice program began offering rewards "of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious cyber activities against U.S. critical infrastructure."[51] In November 2021, the State Department cited the Colonial Pipeline incident in announcing

[42] U.S. Dep't of Justice Press Release, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), *at* https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya [https://perma.cc/75AF-KW4F].

[43] *Id.*

[44] *Id.*; *see also* Indictment, United States v. Vasinskyi, No. 3:21-cr-00366-S (N.D. Tex. Aug. 11, 2021), *available at* https://www.justice.gov/opa/press-release/file/1447126/download [https://perma.cc/D6RX-2F97].

[45] U.S. Dep't of Justice Press Release, Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas (Mar. 9, 2022), *at* https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas [https://perma.cc/T22E-45TV].

[46] U.S. Dep't of Justice Press Release, *supra* note 42.; *see also* Indictment, United States v. Polyanin, No. 3:21-cr-00393-B (N.D. Tex. Aug. 24, 2021), *available at* https://www.justice.gov/opa/press-release/file/1447121/download [https://perma.cc/Z93K-C36X].

[47] U.S. Dep't of Justice Press Release, *supra* note 42.

[48] Warrant to Seize Property Subject to Forfeiture, No. 3-21MJ-888BT (N.D. Tex. Sept. 10, 2021), *available at* https://www.justice.gov/opa/press-release/file/1447131/download [https://perma.cc/5M77-RF5P].

[49] U.S. Dep't of Justice Press Release, *supra* note 42.

[50] U.S. Dep't of the Treasury Press Release, *supra* note 8.

[51] U.S. Dep't of State Press Release, Rewards for Justice—Reward Offer for Information on Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure (July 15, 2021), *at* https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure [https://perma.cc/C4X3-AKQF].

https://doi.org/10.1017/ajil.2022.12 Published online by Cambridge University Press

additional rewards pursuant to its Transnational Organized Crime Rewards Program of up to $10 million for information on leaders of DarkSide and up to $5 million "for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in" a DarkSide ransomware attack.[52] Days later, citing the JBS and Kaseya incidents, the State Department offered a parallel reward for information about leaders or participants in REvil ransomware operations.[53] Evincing concern for the safety of potential tipsters, the Department has established a "Dark Web (Tor-based) tips-reporting line to protect the safety and security of potential sources" and advertises that "[p]ossible relocation and rewards payments by cryptocurrency may be available to eligible sources."[54]

After debate throughout the fall about whether the U.S. counter-ransomware actions were proving effective,[55] on January 14, Russia "arrested 14 alleged members of the REvil ransomware gang, including a hacker that U.S. officials say executed May's Colonial Pipeline attack, and announced that it had eliminated the group at Washington's request."[56] Russia's Federal Security Service also seized $1 million in various currencies, including Bitcoin and computer equipment.[57] Although the United States attributed the Colonial Pipeline incident to DarkSide, U.S. officials believe that the hacker responsible for the attack shifted to REvil when Darkside disappeared.[58] The arrests came amidst growing tensions with Russia over Ukraine, and experts noted "that the arrests, while significant, seem aimed at sending a signal that such cooperation would cease if the United States and Western allies impose sanctions in the event of a Russian invasion of Ukraine."[59]

[52] U.S. Dep't of State Press Release, Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice (Nov. 4, 2021), *at* https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice [https://perma.cc/K53H-MM54].

[53] U.S. Dep't of State Press Release, Reward Offers for Information to Bring Sodinokibi (REvil) Ransomware Variant Co-Conspirators to Justice (Nov. 8, 2021), *at* https://www.state.gov/reward-offers-for-information-to-bring-sodinokibi-revil-ransomware-variant-co-conspirators-to-justice/#:~:text=The%20Department%20of%20State%20is,variant%20transnational%20organized%20crime%20group [https://perma.cc/V3PA-K4AA].

[54] Rewards for Justice, Department of State, Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure, *at* https://rewardsforjustice.net/terrorist-rewards/foreign-malicious-cyber-activity-against-u-s-critical-infrastructure [https://perma.cc/VY74-78FN].

[55] *See, e.g.*, Aaron Schaffer, *Russian Hackers Haven't Backed Off, Administration Official Acknowledges*, WASH. POST (Oct. 6, 2021), *at* https://www.washingtonpost.com/politics/2021/10/06/russian-hackers-havent-backed-off-administration-official-acknowledges (noting that CISA Director Jen Easterly said that she had "not seen any significant, material changes" despite the Biden administration's efforts, while others within the administration expressed greater optimism); Kevin Collier, *Biden's Cybersecurity Policies Praised Despite Persistence of Ransomware*, NBC NEWS (Jan. 20, 2022), *at* https://www.nbcnews.com/tech/security/biden-gets-praise-cybersecurity-ransomware-persistence-rcna12707.

[56] Robyn Dixon & Ellen Nakashima, *Russia Arrests 14 Alleged Members of the REvil Ransomware Gang, Including Hacker U.S. Says Conducted Colonial Pipeline Attack*, WASH. POST (Jan. 14, 2022), *at* https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil.

[57] *Id.*

[58] *Id.*

[59] *Id.*

https://doi.org/10.1017/ajil.2022.12 Published online by Cambridge University Press