#UnconventionalCyber

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

Countering Ransomware: Lessons from Aircraft Hijacking

AUGUST 2021

SIMON HANDLER, EMMA SCHROEDER, FRANCES SCHROEDER, TREY HERR

EXECUTIVE SUMMARY

Ransomware has plagued organizations for more than a decade, but the last three years have experienced a surge in both the number of incidents and the ransoms demanded. These events do not emerge in a vacuum, but are products of structural problems, some of which are similar to past surges in extortion crimes that the United States, along with its allies and partners, countered successfully. To more effectively counter ransomware, the US government should develop a strategy that draws on lessons learned from addressing a surge in aircraft hijackings through the late 1960s and early 1970s. Importantly, in most cases, ransomware and aircraft hijacking are both tactics of extortion. This extortion is utilized by organizations to both fund future operations and achieve a range of strategic objectives. Like the contagion effect of successful aircraft hijackings, ransomware successes beget imitation and evolution. Both activities pose challenges to defenders, which must defend all access points, while an attacker need only exploit one to be successful.

While ransomware and aircraft hijackings defy any one-to-one comparison, three lessons from combatting aircraft hijackings could inform an effective ransomware strategy. First, ransomware payment should not be banned as a first step. Second, the United States must employ both active and passive measures, prioritizing system security and resilience, while also imposing costs on individual ransomware operators and groups. Third, the United States should address the conditions under which ransomware groups are given freedom to operate, and apply pressure on safe-haven states that either actively or passively support their activities. Success in reducing the frequency and severity of ransomware will likely encourage movement to other means of cybercrime. Success in reducing the value of ransomware—shrinking potential for payoffs and hardening the technology base used by potential victims—offers much more wide-ranging protection and value to defenders. Therefore, this strategy fits within the understanding that strengthening cybersecurity is a process of marginal improvement, rather than anything resembling absolute victory.

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

INTRODUCTION

In July 2021, when the REvil ransomware group exploited a vulnerability in Kaseya's VSA software to stealthily distribute ransomware to a number of managed-service providers—and, in turn, thousands of their customers—it was a reminder of the dire state of software supply-chain security and a wake-up call about the potential disruption that attacks of this nature could wreak on a wide scale.[1] As companies and governments move to respond to similar threats, easy solutions and silver bullets are yet again touted, but tangible progress remains elusive. A Department of Homeland Security study this year assessed approximately $350 million in losses "attributable to ransomware" in 2021, and that amount is only expected to increase.[2] Ransomware is a type of malware, or malicious software, designed to encrypt data, and deployed to block a victim's access to their own data until they pay the attacker's demanded ransom in return for the data's decryption.[3] In addition to the Kaseya attack, this year has already seen several other significant ransomware incidents—most prominently, a relatively unsophisticated yet effective attack against Colonial Pipeline.[4] This is more evidence that ransomware groups are increasingly targeting critical infrastructure.[5]

But, the threat from ransomware goes far beyond these recent headline-catching incidents; indeed, as a cybercrime technique it reaches back more than thirty years.[6] Throughout its early years, ransomware was a sporadically employed tool, consisting largely of homebrew encryption and relatively unsophisticated methods of delivery, such as widespread phishing campaigns.[7] Over time, ransomware groups began leveraging off-the-shelf code that utilized algorithms that were much harder to decrypt, coupled with more sophisticated and targeted spear-phishing campaigns.[8] Ransomware would not fully take off, though, until the 2010s with the introduction of cryptocurrencies, such as Bitcoin, which made it easier for groups to act largely anonymously and collect ransoms without leaving much of a trace.[9] In 2016, ransomware attacks began increasingly targeting companies, instead of individuals, with escalating ransom demands. Ransomware demands have continued escalating ever since, with average ransomware payments in the first quarter of 2021 experiencing a 43-percent jump from the fourth quarter of 2020.[10]

Moreover, the number of unique users targeted by ransomware jumped 767 percent between 2019 and 2020.[11] Each successive news story covering "successes" and the

[1] Charlie Osborne, "Updated Kaseya Ransomware Attack FAQ: What We Know Now," ZDNet, July 23, 2021, https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/; Liam Tung, "Kaseya Ransomware Attack: 1,500 Companies Affected, Company Confirms," ZDNet, July 6, 2021, https://www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-company-confirms/; *Breaking Trust, Atlantic Council*, March 29, 2021, https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/.

[2] "Press Briefing by Press Secretary Jen Psaki, Secretary of Energy Jennifer Granholm, and Secretary of Homeland Security Alejandro Mayorkas, May 11, 2021," White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/11/press-briefing-by-press-secretary-jen-psaki-secretary-of-energy-jennifer-granholm-and-secretary-of-homeland-security-alejandro-mayorkas-may-11-2021/; Charlie Osborne, "The Cost of Ransomware Attacks Worldwide Will Go Beyond $265 Billion in the Next Decade," ZDNet, June 7, 2021, https://www.zdnet.com/article/the-cost-of-ransomware-around-the-globe-to-go-beyond-265-billion-in-the-next-decade/.

[3] "Stop Ransomware," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/stopransomware.

[4] Andy Greenberg, "The Colonial Pipeline Hack Is a New Extreme for Ransomware," *Wired*, May 8, 2021, https://www.wired.com/story/colonial-pipeline-ransomware-attack/.

[5] Danny Palmer, "Ransomware Gangs Now Have Industrial Targets in Their Sights. That Raises the Stakes for Everyone," ZDNet, February 2, 2021, https://www.zdnet.com/article/ransomware-gangs-now-have-industrial-targets-in-their-sights-that-raises-the-stakes-for-everyone/.

[6] Leonid Grustniy, "Ransomware: From Blockers to Cryptors and Beyond," Kaspersky Daily, April 7, 2021, https://www.kaspersky.com/blog/history-of-ransomware/39203/.

[7] Steven Melendez, "Ransomware Attacks Are Still on the Rise, Experts Warn," *Fast Company*, June 1, 2016, https://www.fastcompany.com/3060487/ransomware-attacks-are-still-on-the-rise-experts-warn.

[8] Juliana De Groot, "A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time," *Guardian*, December 1, 2020, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

[9] Greg Myre, "How Bitcoin Has Fueled Ransomware Attacks," National Public Radio, June 10, 2021, https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks.

[10] Bill Siegel, "Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound," Coveware, April 26, 2021, https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound.

[11] "Ransomware by the Numbers: Reassessing the Threat's Global Impact," SecureList by Kaspersky, April 23, 2021, https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/.

exorbitant ransoms paid, in turn, encourages even more attacks.[12] Ransomware attacks do not require sophisticated access to computer networks, and a single flaw or mistake can be enough for criminal groups to establish a foothold in their targets' networks. Ransomware is a "low-risk, high-yield endeavor."[13] As demonstrated in the Colonial Pipeline ransomware incident, attackers do not need the complex and stealthy malware of the Sunburst cyberespionage campaign, which weaseled its way into the build process of SolarWinds' Orion software before the company unwittingly pushed it to thousands of customers through a routine software update.[14] This ease for attackers can prove exceptionally challenging for those small-to-medium-sized companies that fall below what Wendy Nather calls the "security poverty line"—those that do not have the resources to implement adequate security measures or in-house talent to jury-rig more effective defenses.[15]

The ease of operation is facilitated by the "ransomware-as-a-service" marketplace, an emerging criminal sector complete with marketing and customer service, which allows aspiring ransomware groups to operate without even developing their own malware or expertise.[16] While the technical barrier to entry for ransomware groups is extremely low, the potential profits for these groups are significant and only increasing, as known ransomware profits increased by 336 percent in 2020, raising the total to $370 million. According to UK Home Secretary Priti Patel, ransomware groups select their victims strategically, "taking the time to research their target so they can maximize their chance of releasing higher sums of money through extortion."[17]

The ransomware ecosystem not only encourages carbon-copy attacks, but teaches new techniques and encourages their evolution and further replication. Many ransomware affiliates take more time to gauge a target's potential capacity to pay, and will hunt for backups to encrypt those as well, further complicating recovery and incentivizing payment.[18] About two years ago, the use of double-extortion ransomware—the encryption of data with the additional threat of data theft—was largely associated with a single actor, but has since been used in more than 1,200 incidents in 2020 alone.[19] In this incestuous ecosystem, innovation is sought and copied with speed. From blockers to asymmetric encryption to double extortion, competitive evolution has driven ransomware to dangerous heights.[20] Ransomware has become, as one commentor put it, a "pandemic of a different variety."[21]

The takeaway from these incidents, and the thousands like them, seems to be that US companies and the US government are not prepared as ransomware emerges from the soupy morass of contemporary cybercrime to become a real, tangible threat.

But, there is hope. Whereas the history of ransomware reaches back decades, the timeline of humans extorting each other for currency stretches back centuries. Extortion is a well-known criminal behavior that jeopardizes an entity of value to

[12] Eamon Javers and Amanda Macias, "Colonial Pipeline Paid $5 Million Ransom to Hackers," CNBC, May 13, 2021, https://www.cnbc.com/2021/05/13/colonial-pipeline-paid-ransom-to-hackers-source-says.html; Nicole Sganga, "JBS Paid $11 Million Ransom after Cyberattack," CBS News, June 10, 2021, https://www.cbsnews.com/news/jbs-ransom-11-million/; James Sullivan, "Ransomware: A Perfect Storm," Royal United Services Institute, March 29, 2021, https://rusi.org/explore-our-research/publications/emerging-insights/ransomware-a-perfect-storm.

[13] Ronny Richardson and Max M. North, "Ransomware: Evolution, Mitigation and Prevention," DigitalCommons at Kennesaw State University, January 1, 2017, https://digitalcommons.kennesaw.edu/facpubs/4276/.

[14] In the Colonial Pipeline ransomware incident, the pipeline operators utilized a legacy virtual private network without multifactor authentication enabled. Attackers were able to gain access by obtaining a single password. Jessica Resnick-Ault and Stephanie Kelly, "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators," Reuters, June 8, 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/; Trey Herr et al., *Broken Trust: Lessons from Sunburst, Atlantic Council*, March 29, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/.

[15] "The Security Poverty Line, Part 1—Wendy Nather—Scw #60," *Security Weekly*, February 2, 2021, https://securityweekly.com/shows/the-security-poverty-line-part-1-wendy-nather-scw-60/.

[16] Danny Palmer, "Ransomware as a Service Is the New Big Problem for Business," ZDNet, March 4, 2021, https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/.

[17] Danny Palmer, "Ransomware: Don't Pay up, It Just Shows Cyber Criminals That Attacks Work, Warns Home Secretary," ZDNet, May 11, 2021, https://www.zdnet.com/article/ransomware-dont-pay-the-ransom-it-just-encourage-cyber-criminals-that-attacks-work-warns-home-secretary/.

[18] Steve Ranger, "Ransomware Victims Thought Their Backups Were Safe. They Were Wrong," ZDNet, February 27, 2020, https://www.zdnet.com/article/ransomware-victims-thought-their-backups-were-safe-they-were-wrong/.

[19] Brianna Leddy, "Double Extortion Ransomware," Darktrace, May 19, 2021, https://www.darktrace.com/en/blog/double-extortion-ransomware/; Sullivan, "Ransomware: A Perfect Storm."

[20] Grustniy, "Ransomware: From Blockers to Cryptors and Beyond."

[21] Hannah Knowles and Meryl Kornfield, "Ransomware Attacks Could Reach 'Pandemic' Proportions. What to Know after the Pipeline Hack," *Washington Post*, May 12, 2021, https://www.washingtonpost.com/business/2021/05/12/ransomware-attack/.

the target in exchange for something of value to the attacker. Hijacking, as a tactic, has not been used exclusively for extortion—as several terrible moments in history show. This analysis focused on the large and varied history of hijacking for extortion, where the value demanded is often a fraction of the target's worth. Extortion has a long and established history as a means for terrorist organizations and armed groups to finance their operations and even achieve strategic and political objectives.[22]

RANSOMWARE AND HIJACKING: LESSONS FROM HISTORY

As the authors have previously argued, cybersecurity strategy and policy can draw lessons from the study of counterinsurgency and counterterrorism.[23] This latter field offers a decades-long history of hijacking as a comparison point for ransomware and lessons from a surge in aircraft hijackings in the late 1960s and early 1970s. Hijacking was a popular form of extortion used by groups both to fund their operations and accomplish strategic objectives. Unlike all but the edgiest of ransomware cases, hijackings endanger human life, but both are popular with low-skilled operators, requiring little sophistication to accomplish the intended effect. Both experienced peaks and lulls in popularity with participating groups, with widespread success exhibiting a "contagion effect" breeding further imitators. Hijacking is risky, and sometimes complicated to resolve with brute force—witness the need for countries to develop specialized law-enforcement and military-counterterrorism capabilities to execute these operations. Ransomware provides an even more challenging brute-force scenario, with successful efforts almost always relying on a discovered flaw in the ransomware's encryption technique or recovery mechanism, rather than a flaw in the underlying cryptographic algorithm. Thus, while hijackings often present at least the thin possibility of recovery through direct action against the hijackers, comparable arrests, or kinetic action, against ransomware operators these are often of limited value.

Ransomware and hijacking also present a challenge to defenders because success for the attacker generally requires gaining access as little as one time; whereas success for defenders demands preventing every attempt for this access, or very rapidly detecting and rejecting it. Attackers are presented a relatively easier scenario. Effective defenses against both, thus, involve a mix of passive measures to raise the cost of an attack anywhere, and active measures to disrupt the formation and operation of groups launching these attacks. Importantly, this framework suits the needs of one defender or a single community of defenders, not all potential victims in time. Successful defense of one network or company could well result in ransomware groups shifting to other targets. Neither ransomware incidents nor aircraft hijackings emerge in a vacuum; they are, and emerge from, structural problems. As such, both methods of attack have been observed to occur in aggregate, and in rapid succession.

As ransomware attacks increase in prominence, if not frequency, this analysis looks back to the period between 1968 and 1972 when airlines experienced a peak in a then-ongoing surge of hijackings.[24] These hijackings became common due largely to their effectiveness in comparison to other methods, their minimal cost, and because the success of early groups taught and encouraged success by others. The most famous extortion hijacker is the infamous D. B. Cooper, who hijacked a plane from Portland, Oregon, and demanded a ransom of $200,000 and two parachutes.[25] After he received his demands, he forced the plane to take off once more and jumped out with the money, never to be seen again. Of the thirty-one hijacking attempts in the following year, "19 involved extortion and 15 were by hijackers who demanded parachutes."[26]

Particular hijackings did not just inspire and instruct those subsequent; they influenced the larger trends in the character and type of hijackings over this period. In early transportation hijackings, Cuba quickly established itself as a popular destination. This slowly gave way to transportation hijackings

[22] Mutlu Koseli et al., "Use of Kidnapping and Extortion as a Tool for Financing Terrorism: The Case of the PKK," Taylor & Francis Online, March 26, 2020, https://www.tandfonline.com/doi/pdf/10.1080/19434472.2020.1745257.

[23] Simon Handler, Emma Schroeder, and Trey Herr, "Cyber Security as Counter-Terrorism: Seeking a Better Debate," War on the Rocks, May 18, 2021, https://warontherocks.com/2021/05/cyber-security-as-counter-terrorism-seeking-a-better-debate/; Emma Schroeder, Simon Handler, and Trey Herr, "Population-Centric Cybersecurity: Lessons from Counterinsurgency," Modern War Institute, May 17, 2021, https://mwi.usma.edu/population-centric-cybersecurity-lessons-from-counterinsurgency/.

[24] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *American Journal of Sociology*, January 1986, https://www.journals.uchicago.edu/doi/abs/10.1086/228353?journalCode=ajs.

[25] "D. B. Cooper Hijacking," Federal Bureau of Investigation, https://www.fbi.gov/history/famous-cases/db-cooper-hijacking.

[26] Holden, "The Contagiousness of Aircraft Hijacking."

to new locations. In later incidents, destinations in Europe became popular, such as when a fourteen-year-old boy, allegedly influenced by the media, attempted a hijacking and sought transport to Europe.[27]

Transportation gave way to pure extortion, with demands for prisoner release or money becoming central. The likelihood for a high return on investment for ransomware groups parallels the relative ease and low comparative cost for aircraft hijackers from 1968 to 1972. Individuals who desired to hijack planes could do so at little to no cost. Federal Aviation Administration (FAA) representative Irving Ripp testified in 1968 that "if you've got a man aboard that wants to go to Havana, and he has got a gun, that's all he needs."[28] Hijacking required no skill or training to accomplish, as passengers were not screened before boarding the planes. Installing metal detectors at airports was first proposed by Senator George Smathers in 1968, inspired by security measures at military facilities and maximum-security prisons, but was quickly rejected over concerns about passenger privacy and confidence. Due to concerns about passenger safety, the airlines themselves implemented policies requiring submission to, and full compliance with, hijacker demands. Demands grew throughout the period, including large financial transfers and the more sensitive release of prisoners and members of terrorist groups.

Swimming against this wave, myriad airlines and airport operators struggled to turn the tide as individual actors. A steady decline in hijackings was driven instead by a collective effort among victim states and the private sector, employing a cocktail of active and passive measures—all of which holds lessons for policymakers working to combat ransomware.

LESSON 1—BANNING PAYMENTS IS NOT A GOOD FIRST STEP

"If once you have paid him the Dane-geld, you never get rid of the Dane."[29] This line, written in 1911 by Rudyard Kipling and referring to the reign of an Anglo-Saxon king at the turn of the eleventh century, captures that attitude that persists today in ransomware discourse. While the payment of ransom demands has clearly long been the target of criticism, recognizing the existing pitfalls of such a move must be done with the understanding that payment often exists outside of other attractive options. Companies targeted with ransomware need viable alternatives to ransom payments, not blanket prohibitions against executing the one option that could avoid their economic ruin. Officially, the Federal Bureau of Investigation (FBI) does not support victims paying ransomware demands, as it does not guarantee the return of jeopardized data and could incentivize further harm.[30] Indeed, a 2021 report asserts that while the percentage of victims who chose to pay their ransom in 2020 increased from 26 to 32 percent, 29 percent of those who paid recovered less than half of their data, and only 8 percent were able to recover all their data.[31]

Ransomware attacks hold data and threaten economic harm. In most cases, unlike in aircraft hijackings, human lives are not on the line. But, ransomware attacks against hospitals and medical centers are a special case. In 2020, a woman in Germany was picked up by paramedics while suffering from an aortic aneurysm. She should have been transferred to the nearby hospital, but paramedics were blocked as the hospital was refusing new patients amidst an ongoing ransomware attack. The paramedics were rerouted an hour away to the

[27] David Phillips, *Skyjack: The Story of Air Piracy* (London: Harrap, 1973), https://catalogue.nla.gov.au/Record/1175483.

[28] Brendan I. Koerner, "How Hijackers Commandeered over 130 American Planes—in 5 Years," *Wired*, June 18, 2013, https://www.wired.com/2013/06/love-and-terror-in-the-golden-age-of-hijacking/.

[29] Rudyard Kipling, "Dane-Geld," *Poetry Lovers Page*, accessed August 12, 0221, https://www.poetryloverspage.com/poets/kipling/dane_geld.html

[30] "Ransomware," Federal Bureau of Investigation, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

[31] "The State of Ransomware 2021," Sophos, April 2021, https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx.

closest hospital, and the woman died shortly after arrival. Though the German courts were unable to prove that the woman would have lived if not for the further transfer, this case is an important reminder that, under the right circumstances, ransomware can be lethal.

This risk was eminently clear in aircraft hijackings, even before it became more common for people to be killed. As noted earlier, the airlines themselves, due to concerns over passenger safety, in the late 1960s implemented policies requiring submission to and full compliance with hijacker demands.[32] In a potential life-or-death situation, no middle ground could viably be dug out. In ransomware cases, however, this middle ground is exactly what needs to be created.

If the paying of the Danegeld only encourages the Dane, then the answer seems obvious: end these payments. A profit-motivated attacker—who will use that profit to increase ransomware capability and fund other types of crime—will not seek profit where it no longer exists. However, the debate is far from settled. Michael Daniel, president of the Cyber Threat Alliance, argues that a legal ban on ransom payments may be necessary. Such bans could "take some burden off organizations, by removing payment as a legal possibility," but must be accompanied by a robust government program to provide companies with the support necessary to comply with the law, without jeopardizing their business.[33]

The authors, and others, argue that a ban would unfairly imperil those businesses that could ill-afford any time offline, including new and small businesses, as well as infrastructure operators and hospitals.[34] In a hearing before the Senate Judiciary Committee, FBI Assistant Director Bryan Vorndran said, "it's our position banning ransomware payments is not the road to go down."[35] Banning payments without a corresponding offer to victims to better defend their systems and mitigate the harms of these attacks punishes the wrong party. Moreover, defection from such a prohibition out of extraordinary need or overwhelming public sentiment—demands to simply "turn it back on" in the case of empty gas stations or a disabled hospital—risks undermining broader policy mandates and the credibility of public-sector agencies. These situations are not hard to imagine. And, the inevitable payment, despite a ban, would undercut cybersecurity authorities' commitments to enforce other behaviors.

Lesson: Banning ransom payments is an attractive potential solution—cutting off the lifeblood of ransomware gangs and halting the circular growth of their capabilities. But, disrupting the value criminals can obtain from ransomware involves more than just banning payments. Indeed, attempting to enforce such an unworkable ban may well strain the public-private links necessary to effectively counter these attacks, driving companies to hide incidents rather than report them in the face of fines and other penalties. In line with the Institute for Security and Technology's (IST) Ransomware Task Force recommendation, ransom payment should be a true last resort after other options are exhausted—and discouraged in general—rather than banned as a first step.[36] The United States and its allies should strive to empower companies to make choices that improve the security ecosystem without sacrificing their own interests. This includes helping to reveal more securely designed and supported products in the marketplace, enhancing the efficiency and efficacy of risk-transfer mechanisms like (but hardly limited to) cyber insurance, and markedly reducing the friction of operational collaboration between these victims' vendor companies and state law-enforcement agencies.

[32] Koerner, "How Hijackers Commandeered over 130 American Planes—in 5 Years."

[33] Joe Tidy, "Ransomware: Should Paying Hacker Ransoms be Illegal?" BBC News, May 20, 2021, https://www.bbc.com/news/technology-57173096.

[34] Tarah Wheeler and Ciaran Martin, "Should Ransomware Payments Be Banned?" Brookings, July 26, 2021, https://www.brookings.edu/techstream/should-ransomware-payments-be-banned/.

[35] "America Under Cyber Siege: Preventing and Responding to Ransomware Attacks," Senate Committee on the Judiciary, July 27, 2021, https://www.judiciary.senate.gov/meetings/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks.

[36] "Combating Ransomware," Institute for Security and Technology Ransomware Task Force, 2021, https://securityandtechnology.org/ransomwaretaskforce/report/.

LESSON 2—EMPLOY BOTH ACTIVE AND PASSIVE MEASURES

The surge in airplane hijackings in the late 1960s and early 1970s was controlled through various measures aimed both at altering the patterns of vulnerability in the industry and at targeting the actors and enablers themselves. In 1970, New Orleans International Airport became the first airport to implement metal detectors to screen for metal weapons that could potentially be used in hijackings.[37] In 1973, the FAA required airports to implement magnetometers, x-rays, and baggage searches to screen passengers and their belongings. Later that decade, the United Nations' International Civil Aviation Organization followed suit. Some states have gone further to combat aircraft hijackings, even resorting to limited uses of force.[38] In September 1970, US President Richard Nixon ordered Defense Secretary Melvin Laird to bomb the Popular Front for the Liberation of Palestine's (PFLP) positions in Jordan in response to the group's hijackings of four commercial aircraft.[39] Though the order for airstrikes was subsequently dropped, citing Laird's concerns about the weather, Nixon ordered a portion of the Sixth Fleet to the Eastern Mediterranean Sea and placed the 82nd Airborne Division on a heightened state of alert, signaling the United States' willingness to take direct military action against the group responsible for the hijackings.

These actions represent a suite of both passive and active measures taken in response to the spate of aircraft hijackings in the late 1960s and early 1970s. They denied some groups outright and forced others to shift to different tactics; as a result, aircraft hijackings became relatively rare during the ensuing decades and remain so to this day.[40] Lessons learned and applied to quell the phenomenon should be considered and inform a counter-ransomware strategy. The examples of metal detection and x-ray screening are passive measures, actions taken to harden potential targets by both deterring would-be hijackers and defending against attempted hijackings. The implementation of passive security measures led to an appreciable decrease in hijackings, but also required continual evolution as attackers and hijackers adapted their methods to overcome such defenses.[41] The September 11, 2001, terrorist attacks involving the hijackings of four commercial aircraft in the United States, while not extortion hijackings, brought about significant further increases in passive aviation security measures across the globe.[42] Passive security provides a starting point for defense against hijackers. But, in a country like the United States, where public airports alone number in the thousands and security resources must be marshaled across a diffuse target set, security must be prioritized, and passive measures alone are insufficient.

Cyberspace offers avenues of attack that are nowhere near as constrained as airline flights. Therefore, the strategy of the United States and its allies in combatting ransomware should not be to attempt to defend against every attack, but to ruthlessly prioritize risk in order to limit harm at points of highest consequence.[43] Identifying and prioritizing products and potential victims based on their value is one approach, taking the perspective of what an adversary would find most valuable to hold at risk. Pushing for more defensible designs and improved security from widely used information-technology products is another, and can bring benefits to defenders without the requirement that policymakers identify the most consequential industries or those most preferred by attackers, which are inevitably moving targets. Regulatory approaches to drive these baseline improvements in the security and defensibility of these products could have effects far more influential than state action targeting specific victim industries and owners/operators.

[37] George C. Larson, "Moments and Milestones: Perfecting the People Filter," *Air & Space Magazine*, September 2010, https://www.airspacemag.com/history-of-flight/moments-and-milestones-perfecting-the-people-filter-1490080/.

[38] Terence Smith, "Hostages Freed as Israelis Raid Uganda Airport," *New York Times*, July 4, 1976, 1, https://www.nytimes.com/1976/07/04/archives/hostages-freed-as-israelis-raid-uganda-airport-commandos-in-3.html.

[39] "The American Response to the Hijackings," Public Broadcasting Service, https://www.pbs.org/wgbh/americanexperience/features/hijacked-american-response/.

[40] Nicola Clark, "Why Airline Hijackings Became Relatively Rare," *New York Times*, March 29, 2016, https://www.nytimes.com/2016/03/30/world/middleeast/airline-hijacking-history.html.

[41] Garrett M. Graff, "Pan Am Flight 103: Robert Mueller's 30-Year Search for Justice," *Wired*, December 27, 2018, https://www.wired.com/story/robert-muellers-search-for-justice-for-pan-am-103/; "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report)," US Government Publishing Office, July 22, 2004, https://www.govinfo.gov/app/details/GPO-911REPORT; "Phoenix-Bound Plane Turns Around After Receiving Bomb Threat," *Aviation Pros*, July 25, 2005, https://www.aviationpros.com/home/news/10433562/phoenixbound-plane-turns-around-after-receiving-bomb-threat.

[42] "The 9/11 Commission Report"; Aviation and Transportation Security Act, 2001, https://www.govinfo.gov/content/pkg/PLAW-107publ71/html/PLAW-107publ71.htm.

[43] Ruthlessly Prioritize Risk recommendation from Herr et al., *Broken Trust: Lessons from Sunburst.*

Whether combatting hijacking or ransomware, recognizing the limitations of passive security is critical to establishing a comprehensive strategy, in which active measures complement passive ones in order to get at the root of the threat. Such a strategy should take the fight to ransomware groups, considering the economic, diplomatic, intelligence, and international legal levers necessary to debase the groups' freedom of operation. This helps defeat the mere shift in targets, from hardened to weak, or in tactics, from ransomware to other forms of cybercrime.

Lesson: For the United States and its allies, the response to the surge in ransomware activity must be comprehensive, encompassing both active and passive lines of effort. Passive measures like policy changes to force more defensible and secure design in widely used technologies, and resources to support the organizations where the damage is most impactful if targeted, include direct advisory support and financial resources from governments. Active measures include better and consistent identification of core ransomware-group personnel, alongside affiliates responsible for individual attacks, and escalating sanctions on these individual operators. Concerted law-enforcement activity to find, capture, and prosecute active ransomware groups should be supplemented and strengthened by targeted individual sanctions impose costs on operators, forcing them to live free only in an ever-shrinking number of jurisdictions and with significantly constrained financial freedom. A focus on raising the costs of this type of activity on ransomware operators themselves will discourage participation in these operations and disincentivize new entrants.

LESSON 3—SQUEEZE SAFE HAVENS

Both ransomware and aircraft hijackings are complicated by problems of geography. The initial location of the entity held for ransom frequently differs from the location where the payment or demand will be delivered. The target destinations, for payment and hijackers alike, are often popular safe-haven countries whose support may only be passive, but is more than sufficient for groups to realize value.[44] According to a Royal United Service Institute (RUSI) report, the majority of ransomware is launched against organizations based or headquartered in the United States, whereas most criminal ransomware groups are located outside of the country.[45] Understanding where these safe havens are and engaging with the international community to alter those states' behavior will be critical for limiting the operating sphere of ransomware attackers, and thereby slowing the surge of ransomware activity.

Due to the frequent use of cryptocurrency to collect payment, tracing the geographic location of identifiable individuals is difficult.[46] And, even when perpetrators are located, their resident host states are often either unable or unwilling to prosecute the crime. In rare cases, such as North Korea's Lazarus Group, the host state itself will sponsor, and go as far as to carry out, ransomware attacks.[47] More often, as in the case of Russia, the activity of ransomware groups aligns with the host state's strategic ends, leading to at least passive acceptance of ransomware activity being launched from within the state's dominion. Vladimir Putin appears to view criminal groups based in Russia as an extension of his

[44] Daniel L. Byman, "Confronting Passive Sponsors of Terrorism," Brookings, February 1, 2005, https://www.brookings.edu/research/confronting-passive-sponsors-of-terrorism/.

[45] Sullivan, "Ransomware: A Perfect Storm"; Steve Ranger, "Ransomware Just Got Very Real. And It's Likely to Get Worse," ZDNet, May 9, 2021, https://www.zdnet.com/article/ransomware-just-got-very-real-and-its-likely-to-get-worse/.

[46] Kartikay Mehrotra, "White House Urged to Address Surge in Ransomware Attacks," Bloomberg, April 29, 2021, https://www.bloomberg.com/news/articles/2021-04-29/white-house-urged-to-address-surge-in-ransomware-attacks.

[47] Shannon Vavra, "North Korean Hackers Are Stepping up Their Ransomware Game, Kaspersky Finds," CyberScoop, July 28, 2020, https://www.cyberscoop.com/north-korea-ransomware-lazarus-group-kaspersky-vhd/.

strength in cyberspace, and the Kremlin appears to tolerate their activities so long as they are directed externally.[48]

A large proportion of the aircraft hijackings between 1968 and 1972—especially toward the beginning of that period—were transportation hijackings, in which the hijacker would demand transit to a particular location.[49] During 1968, the year with the largest number of hijackings, all but two hijackers sought Cuba. These people were largely socialists who believed strongly in an idealized vision of post-revolutionary Cuba, some of whom were originally from the country and wanted to return.[50] It was not until 1973 that the United States and Cuba were able to reach a treaty of extradition, denying the hijackers the asylum they had once held in Cuba.[51] Extortion hijackings, too, leveraged these safe havens. In 1968, members of the PFLP, in cooperation with the government of Algeria, hijacked an Israeli flight and demanded the release of Palestinian prisoners in exchange for Israeli hostages.[52] In 1972, Palestinian terrorists from the Black September Organization (BSO) hijacked Lufthansa Flight 615, demanding that West German authorities release the three surviving BSO perpetrators of the Munich massacre from prison.[53] The West Germans complied with the demand in exchange for the hostages, and the hijackers flew the aircraft and newly freed prisoners to Tripoli, where Libyan president Muammar Gaddafi granted them asylum.[54] According to the US State Department's 1985 Patterns of Global Terrorism analysis, Gaddafi made terrorism, including aircraft hijackings, "one of the primary instruments of his foreign policy," providing training sites and ensuring a safe haven for hijackers.[55]

The US government, as well as the international community, eventually took steps to diplomatically, militarily, and economically isolate states such as Libya, Syria, and Iran, with the United States designating them as state sponsors of terrorism for their support of international organizations involved in aircraft hijackings (among other terrorist activities).[56] Following the 1968 PFLP hijacking, an international aviation boycott of Algeria successfully pressured the government into releasing the Israeli hostages who were held prisoner for forty days.[57] Concerns over the spiraling regional security implications of hijackings led the US government to take further steps to degrade hijacking safe havens throughout the 1970s and 1980s. In 1970, the Nixon administration supported Israeli military action to help drive the Palestinian Liberation Organization (PLO) from Jordan, where it had been exploiting territory as a semiautonomous safe haven from which to launch operations, and restrain encroaching PLO-supportive Syrian forces.[58] Israeli intervention never did occur. Nevertheless, an emboldened King Hussein ordered the Jordanian military on the offensive, eventually forcing a Syrian withdrawal and expelling the PLO from the kingdom in a civil war known as Black September. None of these steps were costless, and the same will be true of efforts to pressure Russia and, should those efforts prove successful, subsequent safe havens elsewhere in the world. It is important for the United States to work to codify the priority of ransomware harms, and to drive a coalitional approach to imposing costs against them.

Lesson: Rather than relying on directly prosecuting ransomware groups, the United States should prioritize

[48] Maria Korolov, "Russian Cybercrime: Is Extradition Ahead?" Data Center Knowledge, June 15, 2021, https://www.datacenterknowledge.com/security/russian-cybercrime-extradition-ahead; Frank Bajak, "How the Kremlin Provides a Safe Harbor for Ransomware," Associated Press, April 16, 2021, https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999.

[49] Holden, "The Contagiousness of Aircraft Hijacking."

[50] Libby Nelson, "The US Once Had More than 130 Hijackings in 4 Years. Here's Why They Finally Stopped," *Vox*, March 29, 2016, https://www.vox.com/2016/3/29/11326472/hijacking-airplanes-egyptair.

[51] "Airplane Hijacking," JRank, https://law.jrank.org/pages/7362/Hijacking-Airplane-Hijacking.html.

[52] Simcha Pasko, "On This Day: El Al Flight 426 Hijacked by PFLP," *Jerusalem Post*, July 23, 2021, https://www.jpost.com/israel-news/on-this-day-el-al-flight-426-hijacked-by-pflp-674735.

[53] "Arabs Hijack German Airliner and Gain Release of 3 Seized in Munich Killings," *New York Times,* October 30, 1972, https://www.nytimes.com/1972/10/30/archives/arabs-hijack-german-airliner-and-gain-release-of-3-seized-in-munich.html; "Massacre Begins at Munich Olympics," History.com, November 16, 2009, https://www.history.com/this-day-in-history/massacre-begins-at-munich-olympics.

[54] Yael Greenfeter, "Israel in Shock as Munich Killers Freed," *Haaretz*, November 4, 2010, https://www.haaretz.com/1.5134761.

[55] Corri Zoli, Sahar Azar, and Shani Ross, "Patterns of Conduct: Libyan Regime Support for and Involvement in Acts of Terrorism," Institute for National Security and Counterterrorism, 2010, https://securitypolicylaw.syr.edu/wp-content/uploads/2012/09/Libya-Report-27-April-2011-final-with-Cover.pdf.

[56] Dianne E. Rennack, "State Sponsors of Acts of International Terrorism—Legislative Parameters: In Brief," Congressional Research Service, May 4, 2021, https://fas.org/sgp/crs/terror/R43835.pdf.

[57] "When Plane Hijackings Were Palestinian Terrorists' Weapon of Choice," *Haaretz,* March 29, 2016, https://www.haaretz.com/israel-news/after-egyptair-four-hijackings-that-shook-israel-1.5424289.

[58] "Jordan: From 1967 to Civil War," Encyclopædia Britannica, https://www.britannica.com/place/Jordan/From-1967-to-civil-war#ref41508.

applying pressure on the states that provide safe harbor or passive support to these groups. In so doing, the United States must involve allies and partners to be successful. Aiming this pressure will rely on detailed attribution efforts, but this is only the starting point. Allied states, including those heavily affected by ransomware, must apply economic and diplomatic pressure against identified safe havens, through sanctions and repudiation of these activities. The role of safe-haven states is a compelling case for the application of international norms and offers a direct case in which the consensus that international law applies to cyberspace could yield tangible benefits as states harbor entities causing direct harm abroad.

CONCLUSION

Ransomware is not a new phenomenon. As with hijackings, addressing the root causes of ransomware requires a multifaceted approach, mixing active and passive measures to block the realization of value by criminal groups and deny groups their safe havens. The role that Russia plays as a safe haven looms large, but ransomware is not exclusively caused by one state, nor will it be solved by policy toward one state alone.

Ransomware payments cannot be considered in the binary—to ban or not to ban—because that action alone is both insufficient and potentially harmful. What is needed is to change the incentive structure of those targeted by ransomware, giving them more realistic alternatives. The incentive structure of ransomware operators, too, must be targeted with both active and passive measures. These include improving the cybersecurity posture of US companies, making it more difficult to deploy ransomware effectively, and identifying and pursuing ransomware groups to the full legal extent. A large part of the legal restriction is the problem of safe-haven states that house these groups outside of accessible jurisdiction. Ameliorating the problem of safe havens will require the concerted diplomatic and economic efforts of the United States, its allies, and any targeted state that would benefit from the abatement of ransomware.

As in all problems in the cybersecurity landscape, there is no silver bullet. Ransomware is a complex and multifaceted problem that will require an equally varied response. As the IST Ransomware Task Force found in its report, the framework for action against ransomware must be multifaceted, encompassing prevention, remediation, and response.[59] Preventing every attack immediately is unrealistic. But, by slowly reshaping the ecosystem that ransomware gangs have exploited and bent to their advantage, the United States can help itself and others to incrementally improve their batting average and, in time, reduce the frequency and consequences of these attacks.

ABOUT THE AUTHORS

Simon Handler is an assistant director with the Atlantic Council's Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security, focused on the nexus of geopolitics and international security with cyberspace. He is a former special assistant in the United States Senate, where he worked on foreign policy issues.

Emma Schroeder is an assistant director with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. Her focus in this role is on developing statecraft and strategy for cyberspace that is useful for both policymakers and practitioners.

Frances Schroeder is a Young Global Professional Intern at the Atlantic Council's Cyber Statecraft Initiative. She is currently a rising senior studying Symbolic Systems and International Relations at Stanford University.

Dr. Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on the role of the technology industry in geopolitics, cyber conflict, the security of the internet, cyber safety, and growing a more capable cybersecurity policy workforce.

[59] "Combating Ransomware."

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org