2022

# Postpandemic Outlook for Organized Criminal Activities: Agility Across the Physical, Social, and Cyber Spaces

Jim Jones

Anthony Stefanidis
*William & Mary*, astefanidis@wm.edu

# A POSTPANDEMIC OUTLOOK FOR ORGANIZED CRIMINAL ACTIVITIES: AGILITY ACROSS THE PHYSICAL, SOCIAL, AND CYBER SPACES

Jim Jones and Anthony Stefanidis

*The global COVID-19 pandemic and response affected every aspect of our society, including the activities of criminal organizations. In this chapter, we discuss several examples of criminal organization agility during the pandemic, drawn from the physical, social, and cyber domains. We assess that criminal organizations are emerging from the pandemic stronger than before, the pandemic presents a unique opportunity to study criminal organization agility, and criminal organizations are more exposed after their pandemic-driven adjustments. We also assess that this adjusted criminal activity and other factors, including risky operations that expose discoverable data, create investigative opportunities that will enable a deeper understanding of criminal organization structure and will enhance our ability to disrupt and dismantle the organizations behind a broad range of illegal activity.*

## COVID-19 Disrupts Illicit Business

The effects of the COVID-19 pandemic on the global economy were substantial and broad reaching. Harvard economists David Cutler and Larry Summers estimated in 2020 that the combined financial cost of pandemic-related lost output, as well as current and long-term health expenses, amounted to $16 trillion in the United States alone,[1] making this the biggest economic crisis since the Great Depression. With the illicit economy accounting for a not insignificant part of the global economy—estimates put it at 5-10 percent of the global GDP[2]—it was expected that this subset too would be affected by the pandemic.

In addition to upending everyday life worldwide, pandemic-related disruptions affected numerous activities that are integral parts of the operations of transnational criminal organizations. For example. restrictions on travel, border closings, and worldwide lockdowns temporarily obstructed the global illicit drug supply chain.[3] As a result, the movement of drugs into and throughout the United States was temporarily disrupted, lowering the availability and raising the price of illicit drugs like heroin and fentanyl during the first half of 2020.[4]

But the disruptive effects of COVID-19 on illicit activities were complex and multifaceted. Human smuggling cartel operations, for example, were impacted by the COVID-19-induced restrictions on nonessential travel across the United States-Mexico border. U.S. Customs and Border Patrol (CBP) data suggest a massive drop in apprehensions of families from the Northern Triangle—comprising Guatemala, Honduras, and El Salvador—that attempted to cross the Southwest border into the United States in mid-2020 compared to a year earlier.[5] At the same time, however, the economic crisis in the United States resulted in a significant drop in remittances sent by migrant workers to their families back home in Mexico. This put these families in financial hardship and drove higher migration patterns

from Mexico to the United States, with the result of an actual increase in the number of Mexican families apprehended while crossing the border.[6] So, while the pandemic created obstacles for some manifestations of organized criminal activities, it also created opportunities.

In this chapter, we focus on the agility demonstrated by criminal networks around the world during the COVID-19 crisis, as they diversified their operational portfolio to take advantage of the opportunities emerging during the pandemic. We do so by examining illicit activities that relate to the trade of substandard health supplies and certain cybercrime activities that capitalize on the Zoom-dominated workplace environment that characterized the initial 12-month pandemic period. These representative examples of the agility and resourcefulness displayed by these organizations support an argument that we should be viewing such organizations as functional networks in pursuit of opportunities, rather than rigid structures that are exclusively pursuing specific types of operations.

## Illicit Activities Adapting to the Pandemic

The sensationalistic means and broad societal impact of illicit activities tend to dominate attention when we try to understand and respond to such activities. However, studying them under the light of economics principles provides additional insight on goals and methods, especially regarding organized illegal entities like cartels.[7, 8]

In that context, the disruptive effects of the pandemic tested the adaptability of illicit businesses. Businesses adapt for two reasons: to respond to changes in their business environment or to reshape existing environments[9, 10] in an effort to identify and capitalize on emerging market opportunities.[11] And illicit business pursued both.

### *Taking Advantage of a New Business Environment*

The pandemic changed the business environment by making medical supplies a scarce and, therefore, highly profitable commodity. Events

in the early stages of the pandemic were indicative of individual illicit entrepreneurship, rather than organized efforts.

The World Health Organization declared COVID-19 a pandemic on March 11, 2020, and the United States declared a national emergency under the Stafford and National Emergencies Acts on March 13, followed on March 23 by Executive Order 13910, to prevent hoarding of health and medical resources, and eventually by the establishment of a Department of Justice (DOJ) COVID-19 Hoarding and Price Gouging Task Force.[12]

Despite these government efforts to anticipate such activities, medical supply scams were already underway. As early as April 1, 2020, the DOJ and the Department of Health and Human Services seized hundreds of thousands of masks (N95 and surgical) and other medical equipment from a price gouger in Brooklyn who was selling this equipment to doctors and nurses at prices as much as 700 percent above market price.[13] Comparable activities were concurrently evolving in cyberspace. As early as March 22, the DOJ filed an action against a website that was engaging in wire fraud and stealing credit card information by promising to ship COVID-19 vaccines,[14] a good eight months before the first announcement of such a vaccine was made. Numerous other scam websites started popping up offering nonexistent or counterfeit N95 masks, nonexistent COVID-19 tests, and other fraudulent COVID-19-related items.[15] While early efforts focused on stealing credit card information, an actual global industry emerged to produce and disseminate counterfeit personal protective equipment (PPE). From Turkey to Romania, counterfeit PPE goods were seized at their point of production or intercepted by CBP agents as the items were shipped to the United States. The UN Office on Drugs and Crime summarized, in a 2020 report, the wide global footprint spread by the illicit production and distribution of substandard and falsified medical products, spanning all continents and thousands of websites.[16]

### *Reshaping Business Environments*

Concurrently with illicit activities taking advantage of emerging business opportunities, criminal organizations saw the pandemic as a unique opportunity to strengthen their position within local communities. In a unique take on brand management, the Sinaloa Cartel invited BBC journalists to a safehouse to record the cartel packing tuna, rice, and toilet paper for Mexico's poor.[17] The packages, marked with the name of "El Chapo" Guzmán, were distributed publicly, some directly by the cartel and others through "El Chapo 701," the brand of Guzman's daughter Alejandrina. Although donating money to local communities was not unknown to the Sinaloa Cartel under El Chapo, even more brutal cartels, like the Cartel Jalisco Nueva Generación, quite remarkably joined this practice.[18] This narco-philanthropy serves a direct purpose: to offer these cartels community leverage, potentially strengthening their status as a local authority that rivals state authority.

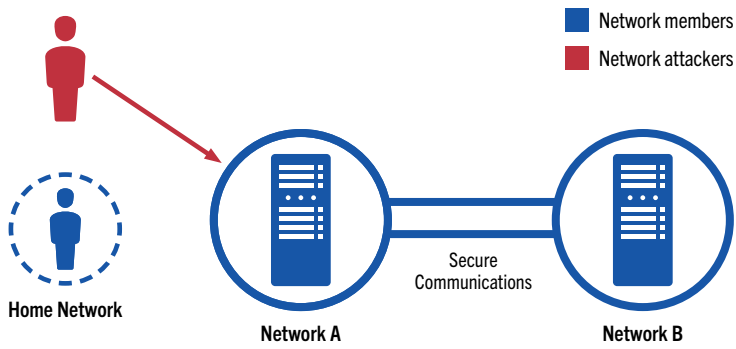
## Cybercrime's Evolution During COVID-19

Cybercriminal adaptation to the pandemic environment occurred in two distinct stages. First, email and web-based scams immediately pivoted to pandemic-related goods and services.[19] As noted previously, nonexistent test kits, PPE, and vaccines were all used as the basis for financial fraud and ruses for data collection as soon as these items or anticipated developments received attention in the public space. Considering the minimal cost to adapt existing scams to these new areas, and the well-established cybercriminal tendency and ability to adopt the fear of the day,[20] this is not surprising. The second adaptation stage included criminal activity that took some time to ramp up, either because of infrastructure or capability requirements, as in the case of counterfeit goods, or because the actions themselves took time, as in the case of computer system and network compromise. The subject of this section is this last activity: the circumstances, activities, and implications of cybercriminal system and network compromise during the pandemic.

### *Exploitation Targets*

Prior to the pandemic, enterprise networks were in something of a steady-state environment. Broadly speaking, these systems had reasonably robust technical countermeasures in place to secure their digital assets against external attackers and to secure communications between themselves and business partners, and less-secure home users were somewhat isolated from enterprise networks, as suggested in Figure 1. Attackers (red in Figures 1-3) faced solid defenses at the enterprise perimeter and gained nothing against the enterprise by attacking home users. This is not to say that these enterprise systems had zero risk or that they were not being actively and sometimes successfully attacked via phishing and other means. Rather, the enterprise ecosystem had reached a sort of equilibrium where most had reasonable protections in place and were generally not viewed as low-hanging fruit by the cyber attacker community.

**Figure 1. The Prepandemic Attack Surface**

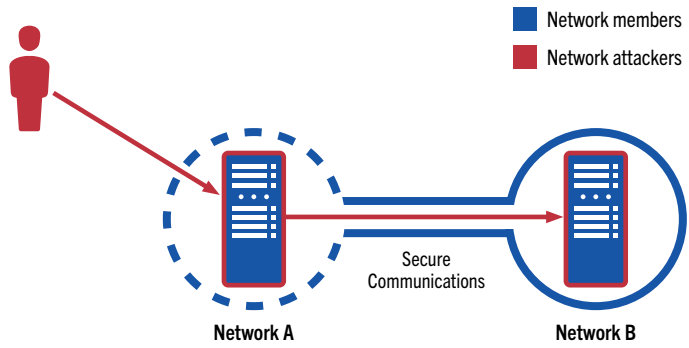



Perhaps only in retrospect can we make the statements above, as it is only by comparison to the current state of affairs that the prepandemic security posture of our enterprise systems looks good. The pandemic response drove a rushed, unplanned, and inconsistently executed move to provide enterprise-wide, remote access with tools

and technology that were not initially up to the task, performed by personnel often lacking the necessary skills and training to securely implement these inadequate tools and technology, and allowed a sense of urgency to bypass the best practices in risk assessment and risk management.[21]

This "rush-to-remote" increased the direct attack surface of nearly every system and network in the enterprise ecosystem. Even if implemented properly, instituting enterprise-wide remote access created multiple new attack vectors into a given network.[22, 23] If any errors were made, then these errors compounded the number of additional vectors, increasing even further the enterprise's risk exposure. Once in a network, attackers had increased access to the enterprise's partners as well (see Figure 2).

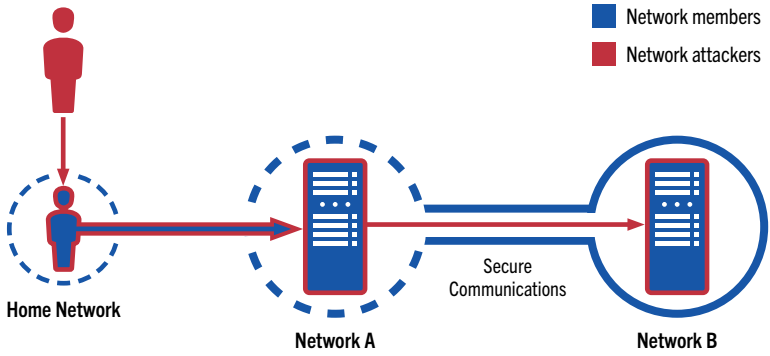
**Figure 2. The Postpandemic Direct Attack Surface**




To make matters worse, previously unconnected home users quickly became remote workers with privileged access to the enterprise network (see Figure 3). Where business partners had previously been screened to assess and ensure their cyber security posture—often enforced contractually—enterprises suddenly opened their entire networks to multiple endpoints with utterly unknown security postures and compromise states.[24] The typical home network

has multiple unmanaged devices on a single unpartitioned internal network with minimal physical security, mixed personal and professional accounts and devices, no controls limiting the introduction and removal of portable digital devices, no personnel security, no formal patch management process, no active monitoring, and uncertain network perimeter security.

**Figure 3. The Postpandemic Indirect Attack Surface**




In the prepandemic cyber world, business partners were often walled off to a limited section of the enterprise network, and they and other remote users underwent additional monitoring to detect misuse or system compromise. Walling off was not possible when the entire workforce became remote: as a group, they required access to the entire enterprise. Establishing individual user system and network permissions is unwieldy even when given plenty of time, and time was not a luxury that enterprise IT teams and risk managers had at the start of the pandemic. Furthermore, the best practice of increased monitoring for remote users—whether business partners or workforce—does not scale. In short, the increase in direct and indirect attack surfaces meant the prepandemic enterprise fortress became an open city with effectively no walls, moats, or gates.

From an attacker's point of view, home users who were of limited value as targets before the pandemic abruptly became easy gateways to enterprise targets of considerable value. Attackers could monitor the network endpoints of traffic on a shared medium (e.g., neighborhood, public WiFi, etc.) and establish likely individual-employer relationships even without access to the encrypted network traffic contents. If an attacker wanted to be a bit more direct about a target, a moderate amount of effort using open sources could identify the home locations of at least some employees from almost any organization.

### *Postpandemic Considerations*

Unfortunately, the risk posed by the rushed implementation of remote access is not limited to the pandemic timeframe. Considering the challenges faced by IT teams to implement remote access at the pandemic lockdown's outset, it is too much to hope that all steps taken were thoroughly documented so that they could be fully undone after the lockdown was lifted. These unintentional residual configurations, combined with the set of capabilities deliberately left in place,[25] present an undesirable departure from the prepandemic security posture of enterprise networks and systems. For those organizations desiring to retain work-from-home capabilities for their employees and contractors, much work remains to secure these endpoints and the systems they access.

Additionally, networks and systems *were* compromised during the lockdown,[26] and not all of these compromises are yet known or addressed. Over time, we expect to discover these compromises as they are leveraged by the attackers, or discovered by threat-hunting and remediation teams. As we learn more about recent and ongoing ransomware attacks, we may find that some of these attacks were facilitated by the circumstances of the lockdown and remote access. The Colonial Pipeline hack, for example, was reportedly initiated via a compromised VPN account.[27] The password for this account

was subsequently found connected to an unrelated breach on the Dark Web, raising the possibility that the same password may have been re-used on multiple systems and this was how the attackers compromised the account.[28] Prepandemic, not as many users had VPN accounts, and these accounts were more tightly controlled and monitored; however, in the resource-challenged pandemic times, it appears that an account was not fully disabled and VPN access was not carefully monitored, enabling the successful attack.

### *Other Considerations*

Fortunately, not all implications of the lockdown-driven, enterprise access changes are bad from a cybercrime investigation point of view. Cybercrime actors were more active during the pandemic lockdown, for example, performing reconnaissance activities against a greater number of targets. Expanding the target set increased not only the likelihood that cybercriminals might hit a honeypot, but the likelihood that investigators might discover this activity through routine detection, and in both cases gain a richer dataset for correlation and analysis. This richer dataset has increased our ability to discover and understand cybercriminal activities and infrastructure, both key aspects of preventing and mitigating attacks. Additionally, multiple non-cybercriminal organizations and others entered the cyberattack space with weak operational security and without the requisite skills, tools, and tactics. Returning to the Colonial Pipeline example, the attackers represented a loose coalition of at least two different cybercriminal groups, one writing the ransomware tool and another executing the attack. The ransom, paid in Bitcoin, was transferred through multiple Bitcoin wallets in the days after the attack, but a sizeable portion (about 85 percent) wound up in a wallet that the FBI was able to seize.[29] While not exactly a rookie mistake, transferring significant funds through a public ledger cryptocurrency and to an insecure account reveals the inexperience of at least some of the attackers. Put simply, amateurs make mistakes, and sometimes these

amateurs are connected to more sophisticated actors, making both of interest to analysts and investigators.

## Outlook: Challenges and Opportunities

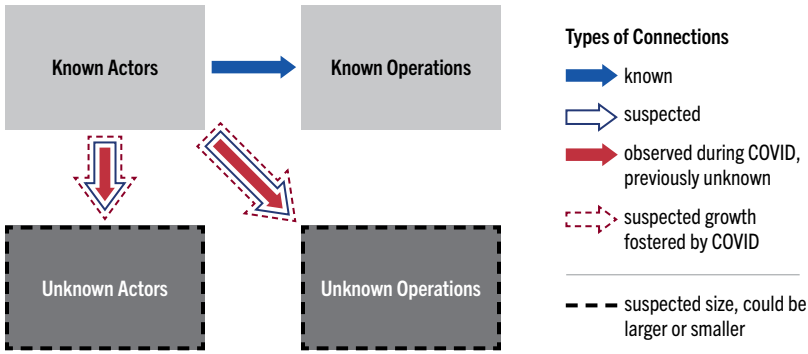
One way to describe the universe of illicit activities is through the taxonomy presented in Figure 4. The light-colored top boxes represent the aggregate of what we know about actors and operations, whereas the bottom darker boxes represent what is still unknown to us. One of the major challenges that criminal investigations face is that, while we have reasonable estimates for the size of the top boxes, our understanding of the size of the bottom two boxes is obviously miniscule. Furthermore, this taxonomy is characterized by the connections among its components. Some of these connections are known: we have an understanding of connections between known actors and operations (solid blue arrow). But some of the connections are only suspected: we suspect the connections between known actors and unknown actors and operations (blue-outlined arrow), but we do not know their full extent.

The pandemic affected the connections of this taxonomy in two ways. First, it broadened the previously unknown connections by adding novel links between known actors and unknown actors/unknown operations (red-outlined arrow). At the same time, we gained additional clarity on these connections, as some of them were revealed through apprehensions (solid red arrow).

Seen through an investigative lens, these developments have advanced our understanding by revealing new actors and operations, such as small-time opportunistic criminals engaged in price gouging or other illicit activities. Although these new insights are not expected to have lasting or substantial effects, the connections established during the pandemic between known actors and unknown actors/unknown operations can be viewed as both challenges and opportunities. Challenges because these previously known and unknown actors may be empowered, as may be the case when they

enjoy heightened support by local communities, or they may form more complex networks, with more sophisticated operational modi operandi and capabilities that were up to now untapped. At the same time, as some of these organized criminal networks may have stepped beyond their traditional operation spaces, we may gain additional opportunities to study them and advance our understanding of their structure and membership.

**Figure 4. A Taxonomy of Illicit Activities**




Returning to the question of criminal organization agility that we posed in this chapter's introduction, we find:

- *The cartels and other criminal organizations are strengthened and emboldened in the aftermath of the pandemic.* Many state-run institutions were weakened during the pandemic, both in terms of actual weakness (e.g., budgets, staffing, infrastructure) and in terms of public trust. This damage will take years to repair, and, in the interim, criminal organizations will continue to step in and exploit the current voids. Similarly, cybercriminals learned much during the pandemic and will use these new skills going forward; they also built a significant backlog of compromised systems for later exploitation.

- *The pandemic offered, and still does offer, a unique opportunity to study the agility of criminal organizations*. First impressions suggest that these actors are remarkably resilient and adaptable. On the other hand, the new activities and associated indicators have not been invisible. Ongoing and future research and analysis promise a better understanding of how these adaptations occur, what data and indicators we might collect and develop, and how we might detect and disrupt such activities in their early stages.
- *Criminal organization structure is more exposed than it was prepandemic*. As these organizations moved into new areas of activity, sometimes unprepared and ill-equipped to do so, we have found abundant data to support analysis and discovery of criminal network activity and structure. Analysis of these new areas will lead to connections, discovery, and understanding of previously stealthy activities, facilitating disruption and dismantling of the underlying criminal organizations behind the activities rather than simply addressing criminal activities in a surface and piecemeal fashion.

## About the Authors

**Jim Jones** has been a cyber security and digital forensics practitioner, researcher, and educator for over 25 years in industry, government, and academia. Currently the director and digital forensics lead for George Mason University's DHS Center of Excellence for Criminal Investigations and Network Analysis (CINA), Dr. Jones' research focuses on the extraction, analysis, and manipulation of full and partial digital artifacts to support criminal investigations and intelligence analysis. Research sponsors have included the Defense Advanced Research Projects Agency, the Intelligence Advanced Research Projects Activity

(IARPA), and the National Science Foundation (NSF). He has a bachelor's degree in systems engineering, a master's in mathematical sciences, and a Ph.D. in computational sciences and informatics.

**Anthony Stefanidis** is a Professor of Computer Science and a Special Advisor to the President for Research Partnerships at the College of William & Mary. He is also a member of the Academic Advisory Board of the CINA Center of Excellence. His areas of academic expertise include the geosocial analysis of social media and crowdsourced content, network analysis, and the analysis of digital imagery and video, and he has authored over 100 journal and conference publications on these topics. Research sponsors for his activities include DHS, IARPA, NSF, the National Geospatial-Intelligence Agency, and the National Aeronautics and Space Administration. Dr. Stefanidis holds Ph.D. and master's degrees from The Ohio State University, and a Dipl. Eng, from the National Technical University of Athens, Greece.

## Endnotes

1 David M. Cutler and Lawrence H. Summers, "The COVID-19 Pandemic and the $16 Trillion Virus," JAMA 324, no. 15 (2020): 1495-96, https://jamanetwork.com/journals/jama/fullarticle/2771764.

2 World Economic Forum, "State of the Illicit Economy," Briefing Papers (2015), http://www3.weforum.org/docs/WEF_State_of_the_Illicit_Economy_2015_2.pdf.

3 United Nations Office of Drugs and Crime (UNODC), "COVID-19 and the Drug Supply Chain: From Production and Trafficking to Use," Research Brief (2020), https://www.unodc.org/documents/data-and-analysis/covid/Covid-19-and-drug-supply-chain-Mai2020.pdf.

4 U.S. Drug Enforcement Administration, "2020 National Drug Threat Assessment," DEA-DCT-DIR-008-21, March 2, 2021, https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

5 U.S. Customs and Border Protection, *U.S. Border Patrol Southwest Border Apprehensions by Sector: Southwest Border Family Unit Encounters by Country*,

accessed on June 15, 2021, https://www.cbp.gov/newsroom/stats/southwest-land-border-encounters/usbp-sw-border-apprehensions.

6 John Gramlich, "Migrant Apprehensions at US-Mexico Border Are Surging Again," Pew Research Center, March 15, 2021, https://pewrsr.ch/3fjlGDO.

7 Alexis Jacquemin and Margaret E. Slade, "Cartels, Collusion, and Horizontal Merger," Chapter 7 of *Handbook of Industrial Organization*, Vol. 1 (Amsterdam: North Holland Publishing Co., 1989), 415-73.

8 John M. Connor and Robert H. Lande, "Cartels as Rational Business Strategy: Crime Pays," *Cardozo Law Review*, 34 (November 2012): 427, file:///C:/Users/Owner/Downloads/SSRN-id1917657.pdf.

9 John Child, "Strategic Choice in the Analysis of Action, Structure, Organizations and Environment: Retrospect and Prospect," *Organization Studies* 18, no. 1 (January 1997): 43-76.

10 Matti Tuominen, Arto Rajala, and Kristian Möller, "How Does Adaptability Drive Firm Innovativeness?," *Journal of Business Research* 57, no. 5 (May 2004): 495-506.

11 Balaji S. Chakravarthy, "Adaptation: A Promising Metaphor for Strategic Management," *The Academy of Management Review* 7, no. 1 (January 1982): 35-44.

12 Marissa Rydzewski, "Price Gouging During a Pandemic: The Federal Government's Response," *DttP: Documents to the People* 48, no. 4 (2020): 33-38, https://journals.ala.org/index.php/dttp/article/view/7480/10332.

13 Alexander Mallin, "Medical Supplies Seized From Alleged Price Gouger to be Distributed to Hospitals," ABC News, April 2, 2020, https://abcnews.go.com/Politics/medical-supplies-seized-alleged-price-gouger-distributed-hospitals/story?id=69938363.

14 U.S. Department of Justice, "Justice Department Files Its First Enforcement Action Against COVID-19 Fraud: Federal Court Issues Temporary Restraining Order Against Website Offering Fraudulent Coronavirus Vaccine," Press Release, March 22, 2020, https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud.

15 Matt Binder, "Coronavirus Sparks Black Market Filled with Fake and Stolen N95 Face Masks," Mashable, April 10, 2020, https://mashable.com/article/coronavirus-face-mask-scams/.

16 UNODC, "COVID-19-related Trafficking of Medical Products as a Threat to Public Health," Research Brief (2020), https://www.unodc.org/documents/data-and-analysis/covid/COVID-19_research_brief_trafficking_medical_products.pdf.

17 "Coronavirus: How Mexican Cartels Are Taking Advantage of Pandemic," BBC News, July 10, 2020, https://www.bbc.com/news/av/world-latin-america-53343599.

18 Vanda Felbab-Brown, "Mexican Cartels Are Providing COVID-19 Assistance. Why That's Not Surprising," The Brookings Institution, April 27, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/04/27/mexican-cartels-are-providing-covid-19-assistance-why-thats-not-surprising/.

19 INTERPOL, *Cybercrime: COVID-19 Impact*, General Secretariat Report, August 2020, https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

20 Harjinder Singh Lallie et al., "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-crime and Cyber-attacks during the Pandemic," *Computers & Security* 105 (June 2021), file:///C:/Users/Owner/Downloads/2006.11929.pdf.

21 Cedric Nabe, "Impact of COVID-19 on Cybersecurity," Deloitte, accessed on June 7, 2021, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

22 Danny Bradbury, "Criminals Exploit Pandemic with Brute-Force RDP Attacks," *InfoSecurity*, June 29, 2020, https://www.infosecurity-magazine.com/news/pandemic-bruteforce-rdp-attacks/.

23 Kelly Sheridan, "RDP Attacks Persist Near Record Levels in 2021," DARKReading, March 17, 2021, https://www.darkreading.com/threat-intelligence/rdp-attacks-persist-near-record-levels-in-2021/d/d-id/1340444.

24 Jim Boehm et al., "Cybersecurity Tactics for the Coronavirus Pandemic," McKinsey & Company, March 2020, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20tactics%20for%20the%20coronavirus%20pandemic/Cybersecurity-tactics-for-the-coronavirus-pandemic-vF.ashx.

25 PulseSecure, "New Research Indicates 84% of Businesses Will Likely Increase Work-from-home Capacity Beyond Pandemic Despite Security Concerns," Intrado Global Newswire, May 27, 2020, https://www.globenewswire.com/news-release/2020/05/27/2039222/0/en/New-Research-Indicates-84-of-Businesses-Will-Likely-Increase-Work-from-home-Capacity-Beyond-Pandemic-Despite-Security-Concerns.html.

26 Arielle Waldman, "10 of the Biggest Cyber Attacks of 2020," TechTarget, January 5, 2021, https://searchsecurity.techtarget.com/news/252494362/10-of-the-biggest-cyber-attacks.

27 Stephanie Kelly and Jessica Resnick-ault, "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/.

28 William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," *Bloomberg*. June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

29 David Uberti, "How the FBI Got Colonial Pipeline's Ransom Money Back," *Wall Street Journal*, June 11, 2021, https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981#:~:text=on%20May%208%20paid%20roughly,Investigation%20followed%20the%20digital%20money.&text=On%20Monday%2C%20the%20Justice%20Department,million%20of%20Colonial's%20initial%20ransom.