

BREAKING THE RANSOMWARE CYCLE

U.S. NATIONAL POLICY OPTIONS

by Christopher Ford and Charles Clancy

Holding objects of value hostage until a ransom is paid for their release is an ancient vice, but it has acquired special salience in the digital age, as cyber criminals in this era of internet-facilitated computer network dependencies have learned to take data itself hostage in return for ransom payments.

The explosive growth of "ransomware" attacks in recent years is the result of dynamics in which the cost and risk to attackers have all but disappeared, victims' incentives to pay promptly have increased, and the profitability of ransomware crime has duly exploded. Predictably, this has attracted steadily more predators to the "game" of digital ransom, and has produced a "feeding frenzy" of ransomware attacks, which U.S. officials have labeled a national crisis.

We will be unable to rein in the ransomware problem unless we directly address the game-theoretical incentive structures that have produced this crisis. By taking effective steps to realign these incentives—such as by incentivizing ransomware-resistant "best practices," ending victims' ability to pass cyber ransom costs along to insurance providers, imposing traditional "know your customer" and other associated banking regulatory practices upon cryptocurrency transactions, and taking steps to reduce cyber criminals' ability to rely upon safe haven in jurisdictions such as Russia—we may be able to break the vicious circle in which we presently find ourselves.

RANSOM: ANCIENT HISTORY

The tactic of seizing something of value and holding it for ransom has been around for a very long time. The earliest and best known manifestation of this phenomenon, of course, is the kidnapping of people in order to elicit payments of money for their return.

In 25 B.C.E., a young Julius Caesar was kidnapped by pirates in the Aegean Sea and ransomed for the huge sum of 50 Roman talents. (The kidnappers originally asked for only 20 talents, but the proud Roman aristocrat felt this sum insultingly low, and encouraged them to demand a higher figure.) It did not work out well for the pirates, however, for upon buying his freedom, young Julius promptly raised a naval force and had his former captors crucified.¹

Almost as famously, King Richard I of England ("The Lionheart") was seized by the Duke of Austria on his return from the Crusades in 1192, only being freed after England paid 150,000 silver marks to Holy Roman Emperor Henry VI for his release. Not for nothing do we speak today of a large sum of money as "a king's ransom," for this sum was considerably larger than the annual income of the English Crown at the time. With this ill-gotten windfall, Henry was able to pay for an invasion of Sicily.²

In an early high-profile case in the United States, a young boy named Charley Ross was abducted in front of his father's mansion outside Philadelphia in 1874 and held for \$20,000. (Unfortunately, Charley was never seen again.)³ Nearly 60 years later, the kidnapping of the infant son of aviation hero Charles Lindbergh created an even greater media sensation.⁴ More recently, criminal gangs have figured out that owners will sometimes pay remarkable ransoms for the freedom of kidnapped pets—a practice that has allegedly expanded during the COVID-19 pandemic.⁵

Yet kidnapping *things* for ransom seems historically to have been less common—no doubt since criminals who steal something of monetary value generally find it easier and more profitable to keep that thing, or sell it to third parties, than to go through the trouble of trying to ransom it back to its original possessor. Nevertheless, sometimes when a criminal seizes an object of special value to its owner, ransom

THE TACTIC OF SEIZING SOMETHING OF VALUE AND HOLDING IT FOR RANSOM HAS BEEN AROUND FOR A VERY LONG TIME. may be asked. In 1987, for instance, grave robbers broke into the tomb of former Argentine populist strongman Juan Peron in Buenos Aires, severed the hands from the corpse, and asked \$8 million for their return. (The ransom was not paid, and the hands were never recovered.)⁶

Even with all of these precedents, however, the kidnapping of information, as it were, appears to be a distinctly modern phenomenon. Yet holding data for ransom is exploding in both popularity and impact, creating a national crisis for the United States.

RANSOMWARE AND ITS MODERN EXPLOSION

The first documented instance of ransomware in the computer age appears to have been malware created by a Harvard-trained evolutionary biologist, who distributed it on diskettes to attendees at an international conference sponsored by the World Health Organization. After a certain number of computer reboots using these diskettes, his code encrypted directories and files on the host computer. To unlock this data, affected users were each told to send \$189.00 to a post office box in Panama.⁷

But what began small, through the clunky vector of hand-distributed computer diskettes, positively exploded with the global connectivity subsequently created by the expansion of the internet. With this connectivity, it soon became possible to scale the ransomware concept nearly to infinity. By about 2006, criminal organizations had begun using much more effective encryption – making their handiwork vastly more difficult to undo without paying them off for the key—and ransomware attacks became commonplace. By one estimate, the number of new ransomware programs detected more than tripled from late 2011 to late 2012, with the number more than quadrupling in the first quarter of 2015 in comparison with the third quarter of 2014.8 Such trends in ransomware volume have continued since then, with a more than two-thirds jump reported in the last quarter of 2020 alone.9

Nor is this increase merely volumetric, for ransomware has grown dramatically in its impact as well. In 2019–2020, ransomware attacks for a time shut down operations at a U.S. Coast Guard facility and a natural-gas pipeline operator, and halted critical city services in Baltimore. Some 560 health care facilities and nearly 1,700 educational institutions suffered ransomware attacks in 2020. ¹⁰ In the spring of 2021 alone, millions of Americans were affected by high-profile ransomware attacks that disrupted key industries and services. One attack paralyzed the Colonial Pipeline, which carries 45 percent of the fuel for the entire U.S. East Coast, causing a reduction of 4.6 million barrels in regional gasoline stockpiles, prompting panicked motorists into long gasoline queues, and creating the largest price spike in nearly seven years. (The company that owns the pipeline paid \$4.4 million in bitcoin to unlock its

frozen computer systems and restart the flow of gas.)¹¹ A subsequent ransomware attack disrupted the U.S. supply of meat by shuttering plants belonging to the world's largest meat-processing company.¹²

Russian-speaking criminals also began a ransomware campaign that targeted U.S. hospitals in 2020, demanding ransoms of up to \$1 million to unlock computer systems at institutions that were already dangerously stressed by the coronavirus pandemic. Both the Colonial Pipeline and meat-processing attacks were also apparently carried out by criminals based in Eastern Europe, with the Biden administration specifically singling out Russia in the latter case. 14

This has produced an increasingly untenable situation. As the *Washington Post* summarized in mid-2021,

"...the impact of these ransomware attacks is increasingly, unavoidably, real for everyday people. These crimes have resulted in missed chemotherapy appointments and delayed ambulances, lost school days, and transportation problems. ... [Even beyond the gas pipeline and meat processing attacks,] [I]ast fall, the Baltimore County Public Schools system was hit with ransomware and forced to halt classes for two days, which were being held virtually.

"As recently as Wednesday [June 2], ransomware attacks were causing problems across the country. In Martha's Vineyard, the ferry service transporting people to and from the Massachusetts island said it had been hit by a ransomware attack that disrupted its ticketing and reservation process. Ferries continued operating all week, but the ticketing system was still affected, causing delays, on Friday. ...

"[Robert Lee, chief executive of Dragos, an industrial cybersecurity firm, says] on average, there are likely 20 to 30 big ransomware cases happening behind the scenes in addition to the ones making headlines. ... The money at stake has changed drastically, however, inflating from thousands to millions of dollars, and the targets are more sophisticated as well. ... Hospitals have been particularly hard hit, as far back as 2016 when the Hollywood Presbyterian Medical hospital paid \$17,000 in bitcoin to a ransomware hacker. Last November, the University of Vermont Medical Center was hit by ransomware and it took nearly a month for it to regain access to its medical records. Chemotherapy patients had their treatments delayed, and were sent to other health centers where some had to recreate their medical history." 15

Once something that business leaders grappled with relatively quietly, ransomware has now openly arrived on the global stage, affecting ordinary people and entire economic sectors in full public view. Even leaving aside incidents that trigger broader societal effects, such as the Colonial Pipeline and meat-processing episodes, the scope and scale of ransomware attacks have been increasing extraordinarily fast. The average ransom paid¹⁶ and the average downtime cost to individuals or businesses per ransomware incident have both been rising, and 54 percent of security professionals at medium and large U.S. corporations report that their institution has been affected by ransomware within the last 12-month period.¹⁷ According to a threat analyst at the cybersecurity firm Emsisoft, the United States had more than 15,000 ransomware incidents in 2020, costing the country between \$596 million and \$2.3 billion in ransom payments, downtime, and remediation costs.¹⁸

In short, we now face a full-blown ransomware crisis. Moreover, things are likely only to get worse, with ransomware also expected to move increasingly into Internet of Things devices, social media, and utility infrastructure. ¹⁹ Not surprisingly, Commerce Secretary Gina Raimondo warned in early June 2021 that ransomware attacks are "here to stay." ²⁰ According to FBI Director Christopher Wray, in fact, there are some "parallels" between the magnitude of today's ransomware threats and the challenge presented by international terrorism in the early 2000s. As a result, there is "a developing consensus within the Biden administration that ransomware ranks among the gravest threats to national security the United States has ever faced." ²¹

THE AVERAGE RANSOM
PAID AND THE AVERAGE
DOWNTIME COST
TO INDIVIDUALS OR
BUSINESSES PER
RANSOMWARE INCIDENT
HAVE BOTH BEEN
RISING.

THE GAME THEORY OF CATASTROPHE

It is not hard to see how things got so bad. Our current ransomware mess represents something of a "perfect storm" of coincidence between technological and geopolitical developments, which have upset older patterns of behavior and are now creating runaway effects.

The game theory of kidnapping people, at least, has received some academic attention. In a recent book, for instance, Anja Shortland of King's College London has explored the question in detail.²² Focusing principally upon bargaining dynamics with kidnappers, she argues that "the best response to a ransom demand is never to agree immediately to a kidnapper's demands," but instead to engage in a deliberate bargaining dance in which the game-theoretical optimum involves "[g]etting the right price" through

"haggling out a compromise that both satisfies the kidnappers and is affordable (and ethically acceptable) for the victims' representatives. Economic reasoning tells us where this undignified bartering ends: kidnappers will release when the cost of holding on to the hostage exceeds what they expect to gain from the next ransom increment."²³

That such bargaining is possible assumes several things about the incentive structures encoded in the ransom "game" that produce, if not an actual equilibrium, then at least a situation in which both sides have reason to converge upon a "moderate" approach in their negotiations. As one account based upon Shortland's book puts it,

"[a]s kidnappers do not want to be held legally responsible, they would be likely to prefer to free the victim whether negotiators pay or decide to hold out. Even in the case where negotiators hold out, kidnappers would be 'better off' to not kill the victim as they face greater risk of being punished by the law if they choose to kill. ... [T]he analysis of this game should establish the intuition for kidnappers to refrain from violence and for negotiators to barter the kidnappers down during negotiations. This kind of intuition steers negotiations towards an outcome where kidnappers would leave the victim unharmed if a reasonable amount of ransom (instead of the usually astronomical first ransom demand) is offered. ... It is helpful to think of this with economic cost-benefit reasoning: kidnappers will release the victim

when the cost of holding on to the hostage exceeds what they expect to gain from the next ransom increment. Thereby, it is best, when playing the game of ransom, to ... conduct negotiations with a firm, calm and cautious approach to bring the victim back safely with a price that ideally would only cover the costs of staging the kidnap."²⁴

By this account, at least, the parties' incentives combine to create a situation in which, while kidnapping remains potentially profitable—for otherwise economic rationality would tend simply to drive it out of existence—it tends not to be so profitable that it explodes. Hence Shortland's conclusion that traditional kidnapping rewards cautious bargaining by both sides. She warns, after all, that "a swiftly agreed, overgenerous ransom" incentivizes new entrants to the game on the criminal side, as "[n]ews of easy profits spread quickly in criminal communities and can cause local or regional kidnapping booms." (This is what occurred with Somali piracy when "nervous negotiators" decided to expedite releases by offering "million-dollar ransoms" to local pirates more accustomed to occasional "low six-figure sums.") In Shortland's account, at least, traditional kidnapping seems in most cases to resolve into a relatively moderate and prudential exchange of value.²⁵

But while Shortland may be right that the incentive structures in *traditional* kidnapping may conduce to such a quasi-equilibrium, it is not hard to see why *data* kidnapping via digital ransomware has exploded.

One crucial difference relates to the criminals' own incentives. As noted above, part of the game-theoretical outcome in Shortland's model is driven by the fact that traditional kidnappers place themselves at no small risk—*e.g.*, in physically seizing the victim, in hiding that person someplace from which the victim *could* be returned if ransom were paid, in engaging in ongoing two-way communications for purposes of negotiation, and in returning the hostage if such negotiation is successful. If the kidnappers actually kill their victim, this risk increases further, both in severity and in duration. (Criminal penalties for murder are generally more severe than for kidnapping, and there is generally no statute of limitations for murder.)

This risk to kidnappers is clearly not felt to be overwhelming, or else there would be no kidnapping in the first place. Nevertheless, Shortland envisions the risks as being real and significant enough to incentivize at least some prudential bargaining by criminal hostage-takers—and presumably enough also to mitigate the overall prevalence of attempted kidnapping.

ACCORDING TO THE
U.S. TREASURY
DEPARTMENT, THE
RUSSIAN SECURITY
SERVICE "CULTIVATES
AND CO-OPTS
CRIMINAL HACKERS
... ENABLING THEM TO
ENGAGE IN DISRUPTIVE
RANSOMWARE
ATTACKS AND PHISHING
CAMPAIGNS."

However, in the context of ransomware deployed through cyberspace and ransom payments made in cryptocurrencies such as bitcoin, the criminal faces an entirely different risk calculus. Often located thousands of miles away in foreign countries—and, of late, frequently in Vladimir Putin's Russia, which sneers at Western criminal inquiries into cybercrime and indeed seems to have a symbiotic relationship with cyber criminals, in which they are permitted to operate unmolested as long as they direct their malware abroad rather than at local targets²⁶—today's ransomware gangs seem to feel no particular risk at all.

According to a senior official in the Biden administration,

"Right now, criminal hacker groups operate with near impunity. Many of the ransomware rings are based in Russia or Eastern Europe, and countries like Russia ignore their activities as long as they don't target companies, people[,] or government agencies" inside their borders."²⁷

According to the U.S. Treasury Department, the Russian security service "cultivates and co-opts criminal hackers ... enabling them to engage in disruptive ransomware attacks and phishing campaigns." With such state entities at least providing safe haven—and perhaps even facilitating certain attacks—the "risk" factor for modern cyber criminals seems extraordinarily low.

Bitcoin-based ransom payments also largely eliminate the transaction costs and risks associated with traditional ransom payments (e.g., marked, sequentially numbered, otherwise potentially traceable banknotes, or the challenge of fencing other items of value), while digital transmission of ransomware encryption keys permits the "hostage" to be "freed" by remote control, without the traditional logistical and criminal-forensic risks to the hostage-takers. In this context, there is precious little risk to dampen a criminal's enthusiasm.

The potential payoff to such criminals has also increased, not merely in the sense that the average ransom payment has apparently been increasing, ²⁹ but also because ransomware technology and bitcoin payment allow such criminality to take place on an industrial scale—shifting, as it were, from the "retail" to the "wholesale" level. Gone are the days when a kidnapper actually had to physically seize something of value and conceal it somewhere until its return. Data kidnapping is essentially infinitely scalable, and the profits are huge.

The ransomware group known as "DarkSide," for example, has reportedly made \$90 million over the last six months, and ransomware

criminal gangs are said to be so profitable that some of them even specialize in developing zero-day vulnerabilities for specialized software. "Multimillion-dollar ransoms, paid in Bitcoin, now seem to be commonplace," and cyber criminals reportedly collected almost \$350 million in ransom payments last year, more than a 300 percent increase since 2019.

The availability of cryptocurrency payments such as bitcoin has played a major role in making this possible, particularly at the higher end of the spectrum such as the Colonial Pipeline incident. According to Nicholas Weaver at the International Computer Science Institute,

"There are only three existing mechanisms capable of transferring a \$5 million ransom—a bank-to-bank should be "transfer, cash[,] or cryptocurrencies". No other mechanisms currently exist that can meet the requirements of transferring millions of dollars at a time."³²

Of these three methods of making large-scale transactions, only cryptocurrency is well-suited to facilitate large transfers over thousands of miles into cyber safe havens such as Russia, and in ways highly resistant to law enforcement and regulatory surveillance and interdiction.

Nor are ransomware victims necessarily making such payments with their own money, either, for cyber insurance often covers the payment of ransom to cyber criminals for the release of data they have taken "hostage." According to one report, in the first half of 2020, ransomware attacks accounted for more than two-fifths of the total number of claims filed for cyber insurance. (Colonial Pipeline, for instance, reportedly has cyber insurance coverage through Lloyd's of London.³³) Cyber insurance policies often include coverage for ransomware incidents, including not just business interruption, data restoration, and incident response costs, but also the actual ransom payments themselves.³⁴ Such coverage makes it much easier for ransomware victims to agree quickly to criminals' terms³⁵ and, indeed, ransomware attacks are the most commonly reported cyber insurance claim, increasing by some 260 percent in the first half of 2020 alone.³⁶

The recent shift in ransomware attacks to include a much higher proportion of targets whose digital paralysis causes huge third-party externalities also serves to shift the game-theoretical ransomware incentive structure. Not long ago, the stereotypical ransomware attack was a quiet incident, in which criminals played upon a corporate victim's desire to resolve things before the world learned there was a problem and the company suffered the market and reputational damage of

being seen as a careless steward of its customers' information. In this context, modest ransom payments might be absorbed as a "cost of doing business" expense, in return for which corporate leaders could thereafter pretend that nothing untoward had ever happened.

The current trend in ransomware, however, is toward targets that produce dramatic effects, such as cutting off gasoline supplies for millions of motorists or the supply of meat available in supermarkets and restaurants. Such affairs are not quiet ones, and their undeniable and potentially accelerating impact upon third parties is less a "bug" than a "feature" from the criminals' perspective—for this impact gives powerful additional incentives for ransomware "victims to pay a huge sum, and as quickly as possible.

The head of the company that owns Colonial Pipeline, for instance, made no bones about this after Russian-speaking ransomware criminals cut off gasoline supplies for the entire U.S. East Coast, and American motorists fought each other for places in gasoline queues. "I know that's a highly controversial decision," he said, and "I didn't make it lightly. I will admit that I wasn't comfortable seeing money go out the door to people like this." Nevertheless, he quickly paid \$4.4 million in bitcoin to the criminals because, he claimed, "it was the right thing to do for the country."³⁷

These various developments collapse the prudential dynamics inherent in Shortland's game theory of traditional kidnapping, and explain ransomware criminals' current "feeding frenzy." Criminals operating out of quasi-safe havens abroad are able to use digital access, strong encryption, and bitcoin payment methods to scale up ransomware attacks to unprecedented levels. At the same time, victims find it comparatively easy to pass ransom costs along to insurers, and criminals' growing focus on targets with high third-party or even systemic impact creates powerful incentives for victims to pay up as quickly as possible, even as the scale of ransom demands increase.

Though based upon Shortland's understanding of kidnapping, such pessimistic conclusions are also supported by the related literature exploring the more general game theory of extortion.³⁹ Through this prism, as well, we can see how recent events have helped produce the current ransomware explosion.

Scholars often tend to understand extortion dynamics in terms of the famous "Prisoner's Dilemma" game. ⁴⁰ For purposes of understanding aggregate behavior in a society, however—*e.g.*, for our purposes, the

prevalence of ransomware attacks rather than just the outcome of any given ransomware attack—it is more useful to look at longer duration, *iterated* Prisoner's Dilemma games carried out at scale by players within a broader interacting population. In such contexts, it has long been felt that game-theory incentives will tend eventually to produce stable relationships of cooperative behavior. Specifically, at least in relatively large populations, it is felt that "extortion" behavior—defined for these purposes as a subset of so-called "Zero Determinant" strategies in which "any increase in one player's own payoff exceeds that of the other player by a fixed percentage"—will tend to be weeded out by the evolutionary selection pressure of game incentives. 41

According to Christian Hilbe and his colleagues, however, these same models also suggest that non-cooperative "defection" behaviors—in this context, extortion—can come to dominate within a population under certain conditions. Specifically, this can happen when the population of "players" is composed of subpopulations that have different rates of evolution over time as iterations of the game occur.⁴² Consequently, "[e] xtortioners can ... achieve a lasting (rather than short-lived) success if the rate of adaptation for the host population is much slower than that for the symbionts."⁴³

Another case in which extortion behaviors can come to dominate an iterated Prisoner's Dilemma environment occurs when some windfall becomes available to would-be extortionists, increasing the anticipated payoff for such behavior and undermining game-theoretical incentives that might otherwise eventually encourage cooperation. As Lutz Becks and Manfred Milinski summarize it, while in an iterated game in a large population extortion is normally "predicted to turn into generous [behavior] and disappear,"

"we show with human volunteers that an additional monetary incentive (bonus) paid to the finally competitively superior player maintains extortion. Unexpectedly, extortioners refused to become disciplined, thus forcing partners to accede. Occasional opposition reduced the extortioners' gain so that using extortion paid off only because of the bonus. ... Our findings [thus] suggest that extortion strategies can prevail when higher competitiveness is rewarded with extra gain. ... The message of the present study seems to be that extortion strategies may be expected, when there is an incentive to gain an extra bonus through being more competitive."

These game-theoretical observations about the dynamics of the subset of "Zero Determinant" strategies labeled as "extortion" thus seem to underline our point about ransomware. Arguably, the present-day ransomware environment represents an instance of both types of situation in which extortion behaviors can run rampant. First, it may indeed be that the population of ransomware attackers (i.e., cyber criminals) and the population of would-be ransomware victims (i.e., entities that store valuable data in networks "accessible to the internet" or otherwise depend upon such connectivity) can be regarded as separate groups that in their cyberspace behaviors "evolve" at different rates. Cyber criminals, after all, are notoriously agile in their approaches, while the broad universe of would-be cyber victims is notoriously slow in the uniform adoption of cybersecurity hygiene and responsive behaviors. (Some entities will react quickly to cybersecurity threats, "patching" vulnerabilities and bringing cyber hygiene standards up-to-date as threat awareness matures, but the universe of potential ransomware victims is huge, and there will always be laggards.) This would appear to open the door to the sort of extortion-dominance modeled by Hilbe and his colleagues.

At the same time, the ransomware environment is, as we have seen, one in which technological changes—tied to the development of strong cryptography, the infinitely scalable geography of internet communication, the existence of jurisdictional cybercrime safe havens such as Russia, and the ease of cryptocurrency payments—have created special windfall opportunities for malicious cyber activity beyond what one would traditionally have expected in a kidnapping/extortion environment. In effect, these changes may have produced the sort of "bonus" modeled by Becks and Milinski. If so, this would also help explain a sudden boom in the prevalence of extortionate behaviors within ransomware's societal iterated Prisoner's Dilemma environment. 45

No wonder, then, that we face such a "perfect storm" of ransomware. The risks are low, the profits are huge, and criminals are apparently flocking into the business even as their targets now include industries and infrastructures upon which millions of Americans depend.

RESPONSES

In response to the surge in high-profile ransomware attacks in early 2021, the Biden administration has announced a number of initiatives. The White House issued an open letter calling upon companies to treat ransomware with more urgency, and to report such instances to federal authorities, ⁴⁶ for instance, and the Department of Justice announced that it would henceforth approach ransomware investigations and prosecutions on a coordinated, government-wide basis much like it does with terrorism. ⁴⁷

The Justice Department has also created a new ransomware task force intended to help "disrupt the criminal ecosystem that fuels ransomware attacks," 48 and the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security began a campaign to press public and private-sector entities to do better in adopting cybersecurity "best practices" that would make them more resistant to ransomware attack. 49 (Guidance has been available for some time on what practices can help make an organization a "harder target" in this regard, but the complexity of some of this guidance and the sheer volume and pace of ransomware assaults has slowed adoption. 50) Citing recent attacks in Ireland, Germany, France, and the United Kingdom, White House press secretary Jen Psaki announced that the United States intends to build an international coalition against ransomware. 51 And beyond that, says Commerce Secretary Raimondo, officials are "considering all of our options." 52

Cryptocurrency is a focus of particular attention from the Biden administration, which hopes to work with an international coalition of governments to compel cryptocurrency exchanges operating offshore to report suspicious transactions, including the identities of the parties. In this vision, countries would cooperate internationally in ways analogous to how the enactment and enforcement of "know your customer" (KYC) policies and the filing of "suspicious activity reports" have for many years been used to fight money laundering, drug trafficking, and terrorist financing.⁵³

Indeed, governments around the world do seem to be increasingly alarmed by the impact cryptocurrencies are having in facilitating rampant cybercrime, by both criminals and rogue regimes such as North Korea, which uses hacking and cryptocurrency to help bankroll

THE WHITE HOUSE
ISSUED AN OPEN
LETTER CALLING UPON
COMPANIES TO TREAT
RANSOMWARE WITH
MORE URGENCY, AND
TO REPORT SUCH
INSTANCES TO FEDERAL
AUTHORITIES.

its weapons of mass destruction (WMD) programs.⁵⁴ Adding to this international concern is growing awareness of the climate impact of the huge quantities of often fossil fuel–generated electricity that is required to "mine" bitcoin—which, according to one recent estimate, amounts annually to more than 121 terawatt-hours, more than the entire country of Argentina consumes in a year.⁵⁵

Citing climate costs, as well as the use of cryptocurrencies by crime syndicates, officials in China have announced that they are cracking down on bitcoin mining and trading,⁵⁶ and banks in both the United Kingdom⁵⁷ and India⁵⁸ have begun blocking transfers to crypto-related accounts. With commentators suggesting that bitcoin is a cause of the ransomware epidemic,⁵⁹ it is increasingly common to hear calls for the outright prohibition of cryptocurrencies.⁶⁰

In April 2021, a task force organized by the Institute for Security and Technology made five key policy recommendations about how to reduce the prevalence and impact of ransomware activity. According to the Ransomware Task Force,

- a. "Coordinated, international diplomatic and law enforcement efforts must proactively prioritize ransomware through a comprehensive, resourced strategy, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.
- b. "The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House. In the U.S., this must include the establishment of 1) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; 2) an internal U.S. Government Joint Ransomware Task Force; and 3) a collaborative, private industry-led informal Ransomware Threat Focus Hub.
- c. "Governments should establish Cyber Response and Recovery Funds to support ransomware response and other cybersecurity activities; mandate that organizations report ransom payments; and require organizations to consider alternatives before making payments.
- d. "An internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks. In some under-

- resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to drive adoption.
- e. "The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading 'desks' to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws."

Building a Better Toolkit

Part of the effort to meet the challenges presented by the ransomware epidemic involves trying to give law enforcement and regulatory officials better tools to fight such cybercrime. In terms of both technical capabilities of law enforcement and legal authorities, various jurisdictions are scrambling to catch up with ransomware criminals.

Blockchain Analytics

Some of what is currently being done attempts to harness the peculiarities of the cyberspace medium to facilitate law enforcement activity. As we have seen, the advent of bitcoin has been a major boon for ransomware attackers, because it offers them key advantages compared to traditional modes of receiving ransom payments. Nevertheless, this new tool does not make criminals omnipotent, and law enforcement agencies are learning to take advantage of some aspects of cryptocurrency that can help facilitate the tracking of illicit transactions.

In particular, the public blockchain technology that underlies most cryptocurrencies can sometimes provide law enforcement officials with important opportunities. Without the state backing that governments provide to fiat currencies such as the U.S. dollar, cryptocurrencies typically preserve their transactional integrity and prevent the fraudulent expansion of their money supply (*i.e.*, crypto-counterfeiting) by maintaining a record of every transaction ever made involving any given cryptocurrency unit (*e.g.*, a bitcoin address). These records are kept, in encrypted form, in publicly accessible blockchains that anyone can access to verify the provenance of that unit. (The transactional records

A BITCOIN OWNER
IS GENERALLY
ANONYMOUS, AND
COINS ARE HELD IN
CRYPTO "WALLETS"
THAT OFTEN PROVIDE
OWNERS WITH A
SIGNIFICANT DEGREE
OF PRIVACY.

in the blockchain are encrypted in a way that makes them all but impossible to change.) This permits holders to verify the authenticity of any "coin" they happen to hold—its "lineage," as it were—but it also means that essentially anyone, including law enforcement authorities, has on-demand access to a full record of every transaction that has ever occurred involving that particular unit.⁶²

A bitcoin owner is generally anonymous, and coins are held in crypto "wallets" that often provide owners with a significant degree of privacy. Nevertheless, blockchains are visible to the public, and their progressive and very visible elaboration as transactions occur—which is not optional, but rather is an intrinsic property of cryptocurrency—can allow investigators to watch "coins" move between IP addresses and through the cryptocurrency exchanges where users buy or sell them, or cash out their cryptocoin for "real" assets. Cryptocurrency units that have become "dirty" through being used in ransom payments can thus sometimes be tracked across the internet for years, and in principle it is possible to tell forever afterwards whether any given "coin" has been tainted in such a fashion through careful study of its blockchain. In some respects, therefore, cryptocurrency can be easier to track than the unmarked, non-sequential banknotes of traditional ransom.⁶³

To be sure, this is no magic bullet. A user's bitcoin address is an account number unique to a particular user, but being able to see that account in action—in association with specific transactions that are recorded permanently in the blockchain—is not necessarily the same thing as being able to identify the user. Nonetheless, a bitcoin address can be analogized to a traditional bank account number, in that any reputable cryptocurrency exchange or "wallet" service is likely to maintain records somehow linking that address to a real-world entity, just as a bank would record the owner of a specific bank account.⁶⁴

This can provide law enforcement with opportunities to seize ill-gotten ransomware gains after payment has been made, and even to support the prosecution of those responsible. Today, law enforcement agencies are increasingly able to team with private-sector entities that specialize in monitoring crypto transactions, analyzing the interplay of bitcoin addresses and overlaying diverse sources of publicly available and proprietary information on such patterns to spot suspicious activity and perhaps discern user identities. (The *intentionally* public and permanent nature of blockchain transactional records, moreover, makes such analysis possible irrespective of jurisdictional boundaries, avoids many of the problems of data retention that often plague law

enforcement efforts to access other records, and sidesteps "third-party doctrine" complexities related to the degree to which user privacy rights make search warrants necessary to conduct such analysis. ⁶⁶) As a result, it is increasingly the case that "[c]riminals of all flavors ranging from drug traffickers to money launderers and tax evaders are routinely brought down by blockchain analysis."⁶⁷

Such techniques apparently contributed to the success of U.S. law enforcement officials in recovering about \$2.3 million in bitcoin out of the \$4.4 million paid in the Colonial Pipeline ransomware incident. Not all of the story has yet been publicly disclosed, but press accounts suggest that the FBI was able to use a publicly visible bitcoin ledger to track at least some of the bitcoins paid in ransom to a specific virtual address, which the Bureau was somehow able to access and for which it obtained a seizure warrant. (In court documents, the FBI said that it had obtained the private key for that address, though it did not explain how.)⁶⁸

Such blockchain-based transaction tracking was apparently also used in the arrest of a Russian-Swedish national who allegedly operated the cryptocurrency "tumbler" or "mixer" service known as Bitcoin Fog. 69 Such "tumblers" are services that comingle bitcoins from various users and generate large numbers of transactions in order to make it harder to "follow the money" through monitoring blockchain activity; in this context they are essentially money-laundering services. 70 Despite these precautions, however, blockchain analytics—undertaken by law enforcement officials with help from a specialist private-sector contractor—were apparently able to identify enough "dirty" transactions to support an indictment of the site's administrator for running a money-laundering operation. 71

While bitcoin mixers have been prosecuted as money launderers before, the use of blockchain evidence to identify Bitcoin Fog's administrator was apparently an innovation. The Nevertheless, authorities' employment of such tools seems to be becoming increasingly common, and these "[i]mproved law enforcement techniques make cryptocurrency transactions more traceable every day. The According to the Wall Street Journal, "law-enforcement officials in recent years have established a track record of tracing cryptocurrency and at times seizing it."

"Justice Department officials in November [2020] said they had seized roughly \$1 billion in cryptocurrency associated with the Silk Road online black market. In January [2021], law-enforcement officials said that the Justice Department had seized more than

\$454,000 in crypto from a ransomware group known as NetWalker.

"Federal officials have previously dismantled illicit crypto networks operating abroad, including the August seizure of accounts and funds tied to al Qaeda and the Izz ad-Din al-Qassam Brigades, the armed wing of Palestinian militant group Hamas. An Internal Revenue Service agent traced transactions intended to fund the groups to Turkish money launderers who had additional customers based in the U.S. or were using U.S.-based exchanges..."

The law enforcement toolkit is clearly now expanding, and "[i]t is likely that many enforcement agencies around the world are similarly retaining private-sector blockchain tracking firms," not least because the Financial Action Task Force has begun "pressuring member nations to effectively police cryptocurrency." Various other regulatory and oversight agencies are also working to increase cryptocurrency transparency and accountability. In the United States, the Treasury Department's Financial Crimes Enforcement Network is currently considering tougher KYC regulations and reporting obligations for cryptocurrency transactions in excess of \$10,000, specifically to

"allow law enforcement to watch and trace, in real time, the flow of those crypto funds on public blockchain ledgers (and to trace a user's complete prior transaction history, irrespective of the size of those prior transactions)."⁷⁶

Meanwhile, the chairman of the Securities and Exchange Commission (SEC) has signaled the likelihood of SEC enforcement actions, and the Internal Revenue Service is expected to pursue tax evasion actions against those trying to hide crypto-derived gains. The Federal Deposit Insurance Corporation (FDIC) has published a request for information about how banks are handling digital assets, and the FDIC and the Federal Reserve are reportedly considering establishing an interagency group to examine crypto policy.⁷⁷ Draft legislation also exists that would force the SEC and the Commodity Futures Trading Commission (CFTC) to clarify rules about when cryptocurrency falls under SEC jurisdiction (as a security) and when it falls under the CFTC (as a commodity).⁷⁸ These various steps could have significant implications in the months and years ahead.

Various U.S. states are also trying to improve law enforcement and regulatory authorities for dealing with cryptocurrency, beginning at least as early as 2017, when Florida brought virtual currencies within the reach of its money-laundering criminal statutes. Arkansas, Indiana,

and Kentucky have also taken steps to update long-established legal and regulatory frameworks to cover cryptocurrency more clearly, while Arizona, North Dakota, Hawaii, and Wyoming are reported to be studying what changes they may need to make.⁷⁹

With such a broad range of moves apparently now underway, the *New York Law Journal* has noted,

"it is likely that crypto privacy levels and expectations will continue to erode with increased regulatory scrutiny, clearer regulatory frameworks ... and evolved law enforcement techniques."80

Particularly given the high-level attention to the issue in the wake of the Colonial Pipeline incident, there would seem to be a strong "demand signal" for effective measures to break the game-theoretical cycle that has led to today's ransomware explosion.

BREAKING THE RANSOMWARE CYCLE

The recommendations of the Ransomware Task Force (see above) are eminently reasonable, and we urge attention to the Task Force's report by both U.S. national policymakers and their foreign counterparts. To help focus and guide the policy community's response to the ransomware crisis, however, we suggest that policymakers focus explicitly upon trying to break the game-theoretical vicious circle into which technological and geopolitical developments have so far trapped us.

As outlined above, the ransomware explosion has resulted from the coincidence of several factors: (1) the creation of jurisdictional safe havens for ransomware criminals in Russia and elsewhere; (2) the easy availability of cryptocurrency payment methods that can handle large transfers at low risk across any distance; (3) cyber insurance coverage of ransom payments; and (4) the increasing prevalence of ransomware attacks on high-impact targets, the nature of which tends to deny victims time and negotiating options. The U.S. national counter-ransomware strategy—and that of our likeminded international partners—should focus as methodically as possible upon picking apart the toxic web of incentive structures that have made it ever more attractive for criminals to mount ransomware attacks and ever more easy and attractive for their victims to pay up.

Mindful that the "feeding frenzy" in today's ransomware "market" derives from the incentive structures facing both ransomware criminals and their victims, policy responses should address the problem from both directions.

Reduce Victims' Payment Incentives

From the victim side, those subjected to ransomware attack need to have more credible alternatives to paying ransom, and fewer incentives to do so. Absent some breakthrough in cryptography that would enable ransomware to be "unlocked" without obtaining the key from criminals—thus essentially immunizing organizations against ransomware, at least where the would-be victim had the knowledge and resources to access such decryption capabilities – it should be an

objective of national policy to lower the cost and difficulty of recovery from a ransomware attack without paying ransom (i.e., even if the data kidnappers "kill" their informational "victim"), and to reduce the moral hazard problems created by the ease with which victims can pass ransom costs along to insurance carriers.

To lower the cost of recovery, we need to do more to encourage or compel public and private-sector organizations to adopt strong "best practices" in protecting themselves against ransomware—not merely in the sense of maintaining effective cybersecurity hygiene to make them more resistant to hacker intrusions, but also in adopting effective practices for timely data backup and for the restoration of critical data in the event of loss. Trade associations, cyber-focused Information Sharing and Analysis Centers (ISACs), 2 and Critical Infrastructure and Key Resources Sector-Specific Agencies (SSAs) and Il play important roles in sharing information about and encouraging anti-ransomware best practices, and in coordinating response and recovery assistance. Cyber insurance carriers could also do more to provide incentives for adopting best practices in this respect, such as by providing discounts for their implementation or by restricting or denying coverage where customers fall short.

Cyber insurance providers should also stop making it so easy for ransomware victims to pay off criminals using other people's money. This would have the double benefit of reducing the cash flows that incentivize criminals to engage in ransomware, and incentivizing would-be victims to take more precautions against being victimized. Perhaps unsurprisingly given the current environment, some of this is already happening for market reasons, with major cyber insurers such as AXA declining to reimburse companies in France for ransomware payments. The insurance industry needs to establish norms whereby insurance covers response and recovery costs but will *not* cover paying ransoms, with premiums based on potential impact and the degree to which the customer can demonstrate adoption of effective antiransomware hygiene and crisis-recovery practices.

More robust action by various national authorities against ransomware gangs (see below) could also be leveraged to strengthen the incentives facing would-be victims of ransomware to make themselves "hard targets" and avoid paying the ransoms demanded by cyber criminals if and when malware intrusions are successful. Already, where ransomware attacks are undertaken by organizations designated under U.S. sanctions authorities by the Treasury Department's Office of

CYBER INSURANCE
PROVIDERS SHOULD
ALSO STOP MAKING
IT SO EASY FOR
RANSOMWARE VICTIMS
TO PAY OFF CRIMINALS
USING OTHER
PEOPLE'S MONEY.

Foreign Assets Control (OFAC), private organizations that pay ransoms to such designated entities could expose themselves to U.S. sanctions penalties as well.⁸⁵

For example, the designers of the "Cryptolocker," "SamSam," "WannaCry 2.0," and "Dridex" ransomware programs have all been designated under OFAC's cyber-related sanctions authorities. This means that anyone who "materially assists" or "provides financial support" to such entities may *also* be subject to U.S. sanctions⁸⁶— and such support to Specially-Designated Nationals (SDNs) could easily include making a ransom payment. OFAC, in fact, is expressly using the threat of such penalties to incentivize stronger private-sector postures against ransomware. Its October 2020 "Advisory" on the subject declares that

"OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations. This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations."

To combat the traditional tendency of corporate managers to try to keep ransom payments quiet for fear of reputational and market damage, OFAC also uses its sanctions authorities to encourage reporting incidents to federal authorities. In the event of sanctions exposure due to involvement in a ransom payment to a designated entity, OFAC advises that it will "consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor." (A company's "full and timely cooperation with law enforcement both during and after a ransomware attack" is also described as "a significant mitigating factor when evaluating a possible enforcement outcome.")89

Through these and other positive and negative incentives—which are likely to become more compelling to the degree that federal authorities continue to deploy sanctions against ransomware gangs, thus raising the possibility of "secondary sanctions" against anyone who provides such criminals with money through a ransom payment—U.S. officials may be able to encourage the development of a general corporate culture much more cautious about paying off the criminals who conduct ransomware attacks. Shifting corporate culture in this fashion, from regarding ransom payments as just another "cost of doing business" to one that sees there is a very significant legal exposure that must be forestalled by rigorous due diligence practices, would do much to suppress moral hazard problems on the victim side. (In time, one might even imagine that future legislation would actually prohibit paying ransom.⁹⁰)

Continue to Increase Criminal Transaction Costs

On the criminal side, as recommended by the Ransomware Task Force, still more can be done to extend to cryptocurrencies the extensive corpus of KYC, AML, and CFT practices and regulations that apply to traditional banking. In theory, such rules already do apply to currencies such as bitcoin, but "cryptocurrency exchanges, crypto kiosks, and OTC trading desks where criminals 'cash out' their cryptocurrency from ransomware payments ... are not consistently compliant" and do not consistently report suspicious transactions to law enforcement and government regulators. ⁹¹

As the Ransomware Task Force also recommends, the SEC should pursue enforcement against "cryptocurrency businesses that fail to register as broker-dealers, transfer agents, clearing agencies, and money service businesses (MSBs), with particular focus on mixing services that obfuscate criminal transactions with local traffic." U.S. officials should also work with likeminded foreign partners to ensure adoption of analogous measures in other national jurisdictions, and to develop effective means and habits of cross-border cooperation and coordination against ransomware gangs.

It is not our view that cryptocurrencies are intrinsically problematic, but at present they clearly create grave externalities in the net social costs of the ransomware epidemic they are facilitating. An international campaign to apply existing transparency and accountability approaches to cryptocurrency could help turn this situation around. Such regulation

LAWS CRIMINALIZING
RANSOMWARE ACTIVITY
AND CRIMINAL
CONSPIRACIES RELATED
THERETO NEED TO BE
CLEAR AND STRONGLY
ENFORCED, AND THE
PROSECUTION OF SUCH
CRIMES GIVEN THE
PRIORITY THEY NOW
CLEARLY DESERVE.

would further legitimize cryptocurrency as a recognized financial instrument, helping to give it a greater degree of long-term price stability, and it would also reduce the reputational taint—and the very real substantive harms—created when cyber criminals and rogue regime WMD programs rely upon cryptocurrencies as a low-cost, risk-free way to do harm.

Meanwhile, law enforcement should continue to expand its emphasis upon sophisticated blockchain analysis and its partnerships with private-sector specialists who are already playing a critical role in identifying "dirty" cryptocurrency transactions and tracking the flows of illicit ransom payments. This field seems to be still in its infancy, and better access to high-end tools, familiarity with cryptocurrency markets, and partnerships with private-sector entities and relevant federally funded research and development centers can greatly expand the law enforcement "toolkit" in the years ahead, at the state, federal, and international levels.

Criminal and administrative law should also keep pace with these developments, ensuring that law enforcement officials have the investigative and seizure authorities they need to keep up with cyber criminals in the technological and methodological arms race now underway between them. Laws criminalizing ransomware activity and criminal conspiracies related thereto need to be clear and strongly enforced, and the prosecution of such crimes given the priority they now clearly deserve. Associated penalties may also need to reflect the severity of the ransomware crisis—perhaps including aggravated penalties when cyber criminals actually end up "killing their victim" by deleting or permanently precluding access to the data they have tried to hold hostage.

Deny or Deter Safe Havens for Criminals

Another critical element of our collective response to the ransomware epidemic must be to reduce the degree to which cyber criminals can rely upon safe haven jurisdictions, such as Russia, that protect them from consequences. ⁹³ Given the economic impact of today's ransomware "feeding frenzy," it ought to be possible for U.S. officials to do more under the International Emergency Economic Powers Act ⁹⁴ to impose sanctions penalties not merely upon ransomware gangs and those who provide "material support" to such groups, but also upon the states (or instrumentalities thereof) that give such criminals safe

harbor or fail to cooperate in reining them in. At least to the degree that ransomware attacks are *not* actually state-sponsored or state-encouraged acts, ⁹⁵ U.S. and other foreign sanctions pressures could perhaps elicit greater cooperation from law enforcement and regulatory agencies in at least some erstwhile safe haven states.

An additional step might be to leverage the existing "defend forward" concept articulated in the U.S. Department of Defense's *2018 Cyber Strategy*, to undertake offensive cyber operations that disrupt the ongoing operation of ransomware gangs or even impose costs against safe haven states that harbor or facilitate their activity. According to the *Cyber Strategy*, it is U.S. policy to "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." This approach is said to envision operations to "halt or degrade cyberspace operations targeting the Department" and to "leverag[e] our focus outward" to stop such threats, but it does not expressly limit itself only to cyber threats affecting the Department of Defense.⁹⁶

If the Biden administration is indeed as focused upon the ransomware threat as it appears to be—with the FBI Director describing current ransomware challenges as requiring a "9/11"-style response⁹⁷—such "defend forward" leverage against cyber criminals would seem quite appropriate. There is already precedent not merely for the FBI to engage in "its own active defense through 'a court-authorized operation to copy and remove malicious web shells from hundreds of vulnerable computers in the United States,' left behind by Chinese spies," but also for U.S. military cyber activity to disrupt Trickbot, "the world's largest botnet" and one commonly "used ... to drop ransomware."

Granted, those precedents were not strictly law enforcement operations, and one would not want military officials routinely acting in support of what are fundamentally law enforcement objectives. Nevertheless, particularly where state-level adversaries provide safe haven for the worst ransomware criminals, there is surely something to be said for occasional doses of active defense. Figuratively at least, it may be useful to remember the precedent suggested by young Caesar's response to the Aegean pirates who had held him for ransom.

CONCLUSION

IF WE DO NOT ACT,
HOWEVER, THERE IS
NO REASON TO EXPECT
THIS EPIDEMIC WILL
DO ANYTHING BUT
WORSEN.

The modern epidemic of ransomware attacks has clear causes that are rooted in the development of facilitating technologies and geopolitical safe havens that incentivize aggressiveness by cyber criminals, as well as in the existence of various factors that incentivize victims to make quick payments as a matter of course. Yet the "attacker" and the "victim" sides of this equation can be affected by the policy choices U.S. officials and their foreign counterparts make in an attempt to address the ransomware challenge. By focusing specifically and directly upon changing the game-theoretical dynamics that have led to the current crisis, we should be able to reduce the incidence and impact of ransomware attacks substantially in the months and years ahead. If we do not act, however, there is no reason to expect this epidemic will do anything but worsen.

The hopeful side of this equation, however, is not merely that the ransomware crisis to some degree can be brought back under control. It is also that "cleaning up" cryptocurrency—that is, taking steps to make it a legitimate, accepted, trusted, and routine form of monetary interaction, rather than the lawless "Wild West" mess of money-laundering, rogue regime WMD finance, rampant speculation, and cybercrime that it is in danger of becoming today—may be a key to allowing the "financial revolution" of virtual coinage to finally live up to its full potential as an answer to the age-old human challenge of commercial exchange. After all, as one observer of the cryptocurrency scene has noted,

"[t]he overwhelming majority of people who care about Bitcoin are interested in the blockchain's potential to be transformative and want to see it thrive for legitimate users and uses. For that to happen, Bitcoin cannot become the 'currency of criminals'; on the contrary, we must make the blockchain a place where criminals feel less safe and less secure. For that reason, all of us in the 'Bitcoin ecosystem' have a role to play in helping law enforcement continue to advance up its learning curve [in order to police abuses]"¹⁰¹

"Mainstream adoption" of cryptocurrency, in other words, "will depend in some part on crypto being seen as 'normal,' like cash or more traditional assets." Once cryptocurrency has been "mainstreamed" by becoming understood to be "clean" and trusted, it can live up to "its vast potential in terms of digital, peer to peer payments, and the future of currency."

Endnotes

- See, e.g., Plutarch, "Caesar," at ¶¶ 1-2, in *The Parallel Lives* (Cambridge: Loeb Classical Library, 1923), available at https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Plutarch/Lives/Caesar*.html.
- *See, e.g.,* Chris Carter, "4 February 1194: Richard the Lionheart is ransomed," *MoneyWeek* (February 4, 2021), *available at* https://moneyweek.com/425142/4-february-1194-richard-the-lionheart-is-ransomed.
- 3 See Heather Thomas, "The Kidnapping of Little Charley Ross," U.S. Library of Congress (April 23, 2019), available at https://blogs.loc.gov/headlinesandheroes/2019/04/the-kidnapping-of-little-charley-ross/.
- 4 See Douglas Linder, "The Trial of Richard 'Bruno' Hauptmann: An Account" (2005), available at http://law2.umkc.edu/faculty/projects/ftrials/Hauptmann/AccountHauptmann.html.
- 5 See, e.g., Lucy Thornton & Claire Miller, "Sick gangs tell owners to 'pay or the dog dies' amid lockdown pet theft epidemic," *Mirror* (April 25, 2021), *available at* https://www.mirror.co.uk/news/uk-news/dog-owners-put-through-emotional-23979882.
- 6 See "5 Arraigned in Theft of Juan Peron's Hands," *LAT Archives* (September 1, 1987), available at https://www.latimes.com/archives/la-xpm-1987-09-01-mn-5366-story.html.
- Kieran Laffan, "A Brief History of Ransomware" (undated), *available at* https://www.varonis.com/blog/a-brief-history-of-ransomware/.
- 8 Laffan, supra.
- 9 McAfee Labs, "Threats Report 4.21," (April 2021), available at https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html.
- Institute for Security and Technology, Ransomware Task Force, "Combatting Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force" (April 30, 2021) [hereinafter "Task Force Report"], at 8-9, available at https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.
- 11 Collin Eaton & Dustin Volz, "Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4 Million Ransom," *Wall Street Journal* (May 19, 2021), *available at* https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.
- Julie Creswell, Nicole Perlroth, & Noam Scheiber, "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business," *New York Times* (June 3, 2021), *available at* https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html.
- Ellen Nakashima & Jay Greene, "Hospitals being hit in coordinated targeted ransomware attacks from Russian-speaking criminals," *Washington Post* (October 29, 2020), *available at* https://www.washingtonpost.com/national-security/hospitals-being-hit-in-coordinated-targeted-ransomware-attack-from-russian-speaking-criminals/2020/10/28/e6e48c38-196e-11eb-befb-8864259bd2d8 story.html.

- See Dustin Volz, "U.S. Blames Criminal Group in Colonial Pipeline Hack," *Wall Street Journal* (May 10, 2021), *available at* https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720?mod=article_inline; Creswell et al., *supra*.
- Heather Kelly, "Ransomware attacks are closing schools, delaying chemotherapy and derailing everyday life," Washington Post (June 5, 2021), available at https://www.washingtonpost.com/technology/2021/07/08/ransomware-human-impact/
- According to a recent task force report, the average ransomware payment had risen to over \$300,000 by early 2020 alone, a more than 170 percent increase from 2019. Task Force Report, *supra*, at 7.
- 17 Safety Detectives, "Ransomware Facts, Trends & Statistics for 2021" (February 3, 2021), available at https://www.safetydetectives.com/blog/ransomware-statistics/. Not all ransomware efforts result in the actual encrypting of victim data by the attackers, but according to a survey of IT professionals carried out in 2020, some 73 percent of cases do reach that stage. Task Force Report, https://www.safetydetectives.com/blog/ransomware-statistics/. Not all ransomware efforts result in the actual encrypting of victim data by the attackers, but according to a survey of IT professionals carried out in 2020, some 73 percent of cases do reach that stage. Task Force Report, https://www.safetydetectives.com/blog/ransomware-statistics/.
- Brian Fung & Zachary Cohen, "DOJ signals plans to coordinate anti-ransomware efforts with the same protocols as it does for terrorism," *CNN* (June 3, 2021), *available at* https://www.cnn.com/2021/06/03/politics/doj-ransomware/index.html.
- 19 Safety Detectives, supra.
- David Cohen, "Cyberattacks 'are here to stay,' Commerce secretary says," *Politico* (June 6, 2021), *available at* https://www.politico.com/news/2021/06/06/ransomware-attacks-commerce-secretary-492005.
- 21 Brian Fung, Geneva Sands, Rachel Janfaza, & Zachary Cohen, "FBI director sees 'parallels' between challenge posed by ransomware attacks and 9/11," *CNN* (June 4, 2021), *available at* https://www.cnn.com/2021/06/04/politics/christopher-wray-cyberattacks-9-11/index.html.
- Anja Shortland, *Kidnap: Inside The Ransom Business* (Oxford: Oxford University Press, 2019), *available through* https://global.oup.com/academic/product/kidnap-9780198815471?cc=gb&lang=en&.
- Anja Shortland, "Inside the ransom business—why kidnapping rarely pays," *The Conversation* (February 8, 2019), available at https://theconversation.com/inside-the-ransom-business-why-kidnapping-rarely-pays-110678.
- 24 See "Game Theory & Why Kidnapping Rarely Pays," Cornell University Course Blog (September 17, 2019), available at https://blogs.cornell.edu/info2040/2019/09/17/game-theory-why-kidnapping-rarely-pays/.
- 25 Shortland, "Inside the ransom business—why kidnapping rarely pays," *supra*.

- See generally, e.g., Tim Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals," Slate (February 2, 2018), available at https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html; Andrei Soldatov & Irina Borogan, The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries (New York: Public Affairs, 2015), at 333–35; and Mathew J. Schwartz, "Russia's Cybercrime Rule Reminder: Never Hack Russians," BankInfo Security (March 27, 2020), available at https://www.bankinfosecurity.com/blogs/russias-cybercrime-rule-reminder-never-hack-russians-p-2888. In June 2017, moreover—just weeks before unleashing the "NotPetya" malware against Ukraine, a state-level cyberattack structured as if it were criminal ransomware—Putin told reporters that he considered Russian hackers to be "like artists," who "[i]f they have patriotic leanings ... may try to add their contribution to those who speak badly about Russia." Nicole Perlroth, This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race (New York: Bloomsbury, 2021), at xvi.
- 27 *Quoted by* Ellen Nakashima, Hamza Shaban, & Rachel Lerman, "The Biden administration seeks to rally allies and the private sector against the ransomware threat," *Washington Post* (June 4, 2021), *available at* https://www.washingtonpost.com/business/2021/06/04/white-house-fbi-ransomware-attacks/.
- U.S. Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority" (April 15, 2021), available at https://home.treasury.gov/news/press-releases/jy0127.
- 29 Safety Detectives, supra.
- Nicholas Weaver, "The Ransomware Problem Is a Bitcoin Problem," *Lawfare* (May 27, 2021), *available at* https://www.lawfareblog.com/ransomware-problem-bitcoin-problem.
- Jen Ellis & Chris Painter, "When it comes to ransomware, it's time to think globally and act now," *The Hill* (April 27, 2021), *available at* https://thehill.com/opinion/technology/550445-when-it-comes-to-ransomware-its-time-to-think-globally-and-act-now.
- 32 Weaver, supra.
- "Colonial Pipeline has cyber insurance policy," *Reuters* (May 13, 2021), *available at* https://www.reuters.com/business/energy/colonial-pipeline-has-cyber-insurance-policy-sources-2021-05-13/.
- 34 Task Force Report, *supra*, at 13.
- Lindsey O'Donnell, "Cyber-Insurance Fuels Ransomware Payment Surge," *ThreatPost* (June 1, 2021), *available at* https://threatpost.com/cyber-insurance-ransomware-payments/166580/.
- 36 Task Force Report, *supra*, at 13.
- 37 Quoted by Eaton & Volz, supra.
- 38 Fung & Cohen, *supra* (*quoting* Brett Callow of the cybersecurity firm Emsisoft).

- 39 *Cf.* Linda Linsefors, "The Game Theory of Blackmail," *LessWrong* (March 22, 2019) (interpreting blackmail as a game of "chicken" and a subcategory of Prisoner's Dilemma games), *available at* https://www.lesswrong.com/posts/wm2rdS3sDY9M5kpWb/the-game-theory-of-blackmail. (Note that much of the literature on this topic uses the term "blackmail" to refer to what might more properly be termed "extortion.")
- In such a scenario, two players each get to choose between "cooperation" and "defection," with the players' respective payoffs being symmetrical if the parties cooperate or defect *simultaneously*, but greatly favoring one party if it manages to take advantage of the other by defecting *alone*. Defection is felt to be the dominant behavior in single-play episodes of the Prisoner's Dilemma in which the parties do not otherwise communicate with each other, with such games having a "defect-defect" outcome as their Nash Equilibrium. *See, e.g.,* "Prisoner's Dilemma Glossary," *University of Pennsylvania, School of Arts and Sciences* (undated), *available at* https://www.sas.upenn.edu/~haroldfs/540/handouts/french/dirigism/pdgloss.htm.
- See, e.g., Christian Hilbe, Martin A. Nowak, & Karl Sigmund, "Evolution of extortion in Iterated Prisoner's Dilemma games," Proceedings of the National Academy of Sciences (April 23, 2013), available at https://www.pnas.org/content/110/17/6913. Experimental studies indicate that players will eventually "punish" or "discipline" extorters, while extorters will also tend to encounter mutual defection when encountering other extorters. Models suggest that this will over time reduce the payoff to extortion strategies, eventually prompting would-be extorters to "switch to more cooperative, generous strategies"—with the result that "[w]e thus expect again to see nice and cooperative strategies prevailing." Lutz Becks & Manfred Milinski, "Extortion strategies resist disciplining when competitiveness is rewarded with extra gain," Nature Communications (February 15, 2019), available at https://www.nature.com/articles/s41467-019-08671-7. (Although "extortion is disfavored by evolution as soon as the population size exceeds a critical level," however, in very small populations, evolutionary dynamics apparently favor extortion behaviors. Hilbe et al., https://www.nature.com/articles/s41467-019-08671-7. (Although "extortion is disfavored by evolutionary dynamics apparently favor extortion behaviors. Hilbe et al., https://www.nature.com/articles/s41467-019-08671-7. (Although "extortion is disfavored by evolutionary dynamics apparently favor extortion behaviors. Hilbe et al., https://www.nature.com/articles/s41467-019-08671-7.
- 42 Hilbe et al., *supra*.
- 43 *Id*
- Lutz & Milinski, supra. "When both players can reach the bonus," they write, "the use of extortion is less pronounced."
- An alternative framing, making essentially the same point, might be that these technological developments had the net effect of increasing ransomware cyber criminals' bargaining power vis-à-vis potential victims, lowering the costliness of carrying out a threat, increasing the extortionist's credibility, and lowering the risk to the perpetrator—a classic recipe for making crime attractive through the prism of the basic game-theoretical dynamics outlined years ago by thinkers such as Thomas Schelling and Daniel Ellsberg. *See, e.g.,* Thomas Schelling, "The Strategy of Conflict: Prospectus for a Reorientation of Game Theory," *Journal of Conflict Resolution,* vol. 2, no. 3 (September 1958), at 240; Daniel Ellsberg, "The Theory and Practice of Blackmail," *RAND Corporation* (July 1968), at 23–37, *available at* https://www.rand.org/content/dam/rand/pubs/papers/2005/P3883.pdf.
- Alex Marquardt & Geneva Sands, "White House pushes for companies to take ransomware more seriously after high-profile cyberattacks," *CNN* (June 3, 2021), *available at* https://www.cnn.com/2021/06/03/politics/white-house-open-letter-ransomware-attacks-businesses/index.html.

- 47 Fung & Cohen, supra.
- Nakashima, Shaban, & Lerman, *supra; see also* Vanessa Romo, "How A New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back," *NPR* (June 8, 2021), *available at* https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac. A similar "best practices" push was undertaken by CISA to help harden election-related computer systems against ransomware intrusions prior to the 2020 U.S. elections.
- 49 CISA, "CISA Launches Campaign to Reduce the Risk of Ransomware" (February 16, 2021), available at https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware.
- See generally, e.g., Ransomware Task Force, *supra*, at 18 (noting that "with so much information and noise surrounding this threat, time- and resource-constrained organizations and individuals struggle to identify the most relevant and accurate sources of useful information" to provide "guidance that is truly actionable and feels relevant to their needs").
- 51 Fung & Cohen, supra.
- 52 Quoted by Cohen, supra.
- 53 Nakashima, Shaban, & Lerman, supra.
- See, e.g., Robert McMillan & Aruna Viswanatha, "North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says," *Wall Street Journal* (February 17, 2021), *available at* https://www.wsj.com/articles/u-s-authorities-charge-north-koreans-in-long-running-hacking-scheme-11613581358.
- 55 Cristina Criddle, "Bitcoin consumes 'more electricity than Argentina," *BBC News* (February 10, 2021), *available at* https://www.bbc.com/news/technology-56012952.
- See Caitlin Ostroff & James T. Areddy, "Bitcoin, Ether Prices Continue Falling After China Spurs Regulatory Fears," Wall Street Journal (May 21, 2021), available at https://www.wsj.com/articles/bitcoin-ether-prices-continue-falling-on-regulatory-fears-11621611655?mod=article_inline; Elaine Yu & Chong Koh Ping, "China's Latest Crackdown on Bitcoin, Other Cryptocurrencies Shakes Market," Wall Street Journal (May 24, 2021), available at https://www.wsj.com/articles/chinas-latest-crackdown-on-bitcoin-other-cryptocurrencies-shakes-market-11621853002.
- 57 See Dale Hurst, "British Banks Crack Down on Crypto Transfers Amid Financial Crime Fears," Yahoo!Finance (May 30, 2021), available at https://finance.yahoo.com/news/british-banks-crack-down-crypto-113758078.html.
- See Anna Baydakova, "Banks Are Already Cracking Down on Crypto, Indian Traders Say," *Crypto Long & Short* (May 14, 2021), *available at* https://www.coindesk.com/indian-banks-turn-hostile-to-crypto.
- 59 See, e.g., Weaver, supra ("...[I]n the end, we don't have a ransomware problem, we have a Bitcoin problem.").
- See, e.g., Lee Reiners, "Ban Cryptocurrency to Fight Ransomware," *Wall Street Journal* (May 25, 2021), *available at* https://www.wsj.com/articles/ban-cryptocurrency-to-fight-ransomware-11621962831.
- 61 Ransomware Task Force, *supra*, at 6.

- 62 See generally, e.g., Duane King & Peter Warrack, "Real Considerations for Law Enforcement in Seizing Virtual Currency," ACAMS Today (June 26, 2018), available at https://www.acamstoday.org/real-considerations-for-law-enforcement-in-seizing-virtual-currency/; Andrea O'Sullivan, "No, the federal seizure of Colonial Pipeline ransomware payments did not 'break' bitcoin," USA Today (June 15, 2021), available at https://www.usatoday.com/story/opinion/2021/06/15/bitcoin-ransom-colonial-pipeline-ransom-hackers-regulation-cryptocurrency/7688503002/; Michael Katz, "FBI Arrests Alleged Operator of Longest-Running Bitcoin Laundering Service," Chief Investment Officer (May 5, 2021), available at https://www.ai-cio.com/news/fbi-arrests-alleged-operator-of-longest-running-bitcoin-laundering-service/.
- 63 See generally, e.g., Jason Weinstein, "How can law enforcement leverage the blockchain in investigations?" Coin Center (May 12, 2015), available at https://www.coincenter.org/education/policy-and-regulation/how-can-law-enforcement-leverage-the-blockchain-in-investigations/; David Uberti, "How the FBI Got Colonial Pipeline's Ransom Money Back," Wall Street Journal (June 11, 2021), available at https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981; Julia Magas, "Law Enforcement's Guide to Policing Cyber Crimes," Cointelegraph (February 19, 2020), available at https://cointelegraph.com/news/the-law-enforcements-guide-to-policing-crypto-cybercrimes.
- See Weinstein, supra. Improving KYC procedures now reportedly means that "most of the platforms that work with digital assets require proof of identity and address before granting access." Magas, supra. This information, in turn, "may be available to law enforcement upon service of a warrant, production order[,] or subpoena." King & Warrack, supra. See also generally Philip Larratt, Paul Taylor, David S. Wall, Syed Naqvi, Matthew Shillito, & Rob Stokes, "Policing Bitcoin: Investigating, Evidencing and Prosecuting Crimes Involving Cryptocurrency," N8 Policing Research Partnership (July 13, 2017), available at https://n8prp.org.uk/wp-content/uploads/2017/08/N8-Cryptocurrency-Report.pdf.
- See Brett Wolf, "US law enforcers partner with cryptocurrency tracking firm to fight financial crime," *Thompson-Reuters* (December 23, 2020), available at https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/cryptocurrency-financial-crime/; Larratt, et al., supra; Magas, supra.
- 66 Weinstein, supra.
- 67 O'Sullivan, supra.
- 68 See, e.g., Romo, supra; Uberti, supra; see also O'Sullivan, supra.
- 69 Katz, supra.
- See Kenneth M. Breen, Phara A. Guberman, & Kenneth P. Herzinger, "Prosecutions of Bitcoin Mixers Raise Crypto Privacy Questions," *New York Law Journal* (May 17, 2021), *available at* https://www.law.com/newyorklawjournal/2021/05/17/prosecutions-of-bitcoin-mixers-raise-crypto-privacy-questions/.
- 71 Katz, supra.
- 72 Breen, et al., supra.

- Katz, *supra*. Katz reports, for instance, that "a federal court recently authorized the IRS to serve a 'John Doe Summons' on a crypto exchange requiring the identification of any U.S. taxpayer customer who conducted at least \$20,000 in crypto transactions on that exchange from 2016 to 2020."
- 74 Uberti, supra.
- 75 Wolf, supra.
- Breen, et al., *supra*; *see also* Nikhilesh De, "State of Crypto: Federal Regulations Are Coming Into Focus," *Coindesk* (June 1, 2021), *available at* https://www.coindesk.com/biden-administration-crypto-regulation-hints.
- 77 De, "State of Crypto," supra.
- Nikhilesh De, "U.S. Lawmakers Introduce Bill to Clarify Crypto Regulations," Coindesk (March 9, 2021), available at https://www.coindesk.com/lawmakers-digital-asset-regulation.
- See Heather Morton, "Cryptocurrency 2021 Legislation," *National Conference of State Legislature* (May 14, 2021), available at https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2021-legislation.aspx; King & Warrack, *supra*. The U.S. Senate has also considered crypto-regulatory legislation, though one bill appears to have foundered as a result of confusion over one provision that would have purported to regulate the notoriously borderless medium of cryptocurrency at the U.S. "border." *See* J.D. Alois, "Whatever Happened to the Senate Legislation That May Kill Crypto Innovation in the U.S.?" *Crowdfund Insider* (April 7, 2018), *available at* https://www.crowdfundinsider.com/2018/04/131054-whatever-happened-to-the-senate-legislation-that-may-kill-crypto-innovation-in-the-us/.
- 80 Breen, et al., supra.
- Magas, *supra* ("... [P]revention is the most effective defense against ransomware, and it is critical to comply with the rules of internet security and information stored on devices. In general, organizations should upgrade outdated programs, execute regular patching, apply the "least privileges" approach, segregate the network perimeter, and implement effective backup practices.").
- 82 See, e.g., National Council of ISACs, "About ISACs" (undated), available at https://www.nationalisacs.org/about-isacs.
- See, e.g., Federal Emergency Management Agency, "Critical Infrastructure and Key Resources Support Annex" (January 2008), at Table A-1 (listing SSAs for various critical infrastructure sectors), available at https://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf.
- Robert Lemos, "Cyber Insurance Firms Start Tapping Out as Ransomware Continues to Rise," *Dark Reading* (May 24, 2021), *available at* https://www.darkreading.com/risk/cyber-insurance-firms-start-tapping-out-as-ransomware-continues-to-rise/d/d-id/1341109.
- See Kelly Jackson Higgins, "US Treasury Warns of Sanctions Violations for Paying Ransomware Attackers," Dark Reading (October 1, 2020), *available at* https://www.darkreading.com/risk/us-treasury-warns-of-sanctions-violations-for-paying-ransomware-attackers/d/d-id/1339066.

- 86 U.S. Department of the Treasury, Office of Foreign Assets Control, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (October 1, 2020) [hereinafter "OFAC Advisory"], at 2, available at https://home.treasury.gov/system/files/126/ofac ransomware advisory 10012020 1.pdf.
- An SDN is any person or entity on OFAC's list of individuals and companies owned or controlled by, or acting for or on behalf of, countries the U.S. sanctions, as well as individuals, groups, and entities—such as terrorists and narcotics traffickers—designated under non-country-specific sanctions programs. See generally, e.g., U.S. Department of the Treasury, "Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists" (June 2, 2021), available at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.
- 88 OFAC Advisory, supra, at 3-4.
- 89 Id. at 4.
- 90 See, e.g., Joe Tidy, "Ransomware: Should paying hacker ransoms be illegal?" BBC.com (May 20, 2021), *available at* https://www.bbc.com/news/technology-57173096.
- 91 Ransomware Task Force, supra, at 29.
- 92 Id. at 30.
- 93 See, e.g., Frank Bajak, "How the Kremlin provides a safe harbor for ransomware," *Associated Press* (April 16, 2021), *available at* https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7e b3841be45dff2d93ed3102999.
- 94 50 U.S.C. §§ 1701 et seg.
- Sanctions in response to hacking activity by state organs such as the Russian GRU, or to cyber-facilitated intellectual property theft undertaken by or in support of China's People's Liberation Army, apparently have yet to penalize such mischief enough to overcome perceived state incentives to engage in it. Cf. Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 1, 2015), available at https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m; Executive Order 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (December 28, 2016), available at https://www.federalregister.gov/documents/2017/01/03/2016-31922/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.
- 96 U.S. Department of Defense, *Department of Defense Cyber Strategy 2018*, at 1-2, *available at* https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
- 97 See Fung, Sands, Janfaza, & Cohen, supra (quoting FBI Director Wray).
- Jason Healey, "When Should U.S. Cyber Command Take Down Criminal Botnets?," *Lawfare* (April 26, 2021), *available at* https://www.lawfareblog.com/when-should-us-cyber-command-take-down-criminal-botnets.

- Ellen Nakashima, "Cyber Command has sought to disrupt the world's largest botnet, hoping to reduce its potential impact on the election," *Washington Post* (October 9, 2020), *available at* https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10 story.html.
- 100 See, e.g., Bobby C. Lee, *The Promise of Bitcoin: The Future of Money and How It Can Work for You* (New York: McGraw Hill. 2021).
- 101 Weinstein, supra.
- 102 De, "State of Crypto," supra.
- 103 Christopher Ciabarra, "The Promise of Bitcoin," Wired (undated), *available at* https://www.wired.com/insights/2014/03/promise-bitcoin/.

About the Authors

Dr. Christopher Ford is Senior Advisor for Geopolitical Policy and Strategy at MITRE Labs. He previously served as U.S. Assistant Secretary of State for International Security and Nonproliferation, and performed the duties of the Under Secretary for Arms Control and International Security.

Dr. Charles Clancy is Senior Vice President at MITRE, General Manager of MITRE Labs, and MITRE's Chief Futurist. Before joining MITRE, he served as the Bradley Professor of Cybersecurity at Virginia Tech and as Executive Director of the Hume Center for National Security and Technology.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and FFRDCs, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

