Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack

The Honorable Joe R. Reeder
Cadet Tommy Hall

INTRODUCTION

In 2014, former NSA Deputy Director Chris Inglis prophetically observed that "if we were to score cyber the way we score soccer, the tally would be 462-456 twenty minutes into the game, i.e., all offense."[1] Recent events demonstrate that Inglis' warning is more urgent than ever, because our cyber defenses remain woefully inadequate. *The Washington Post* titled a feature article on July 11, 2021: "Would the US really answer cyberattacks with nuclear weapons?"[2] Even to broach this question would prompt a follow-up: Has the US undertaken every practicable effort it can make to insulate its assets from cyberattacks? The discussion below explains why the answer is a resounding "No."

On May 6, 2021, Colonial Pipeline was attacked by ransomware suspected to have originated in Eastern Europe or Russia,[3] allowing cyber criminals to penetrate a major utility with significant impact on the entire US eastern seaboard's economy. From the perspective of vulnerability, the Colonial Pipeline attack was a significant wake-up call–a Pearl Harbor moment for cybersecurity. Although Federal authorities eventually recovered $2.3 of the $4.3 million ransom paid, the DarkSide hacking group still gouged a seven-figure bitcoin profit. Headline news reported panic, social disruption, and a crippling lack of fuel delivery. This and other recent attacks referenced below highlight a serious and growing threat to national security. As such, this article discusses two related issues: (1) how much, and how, we as a nation must move to improve cyber defenses for critical infrastructure, and (2) some of the lessons we must apply to protect against increasingly disruptive cyber threats, with special focus on three aspects of cyber-security: protection and prevention, resilience and recovery, and deterrence. As facts (and attacks) continue to unfold, each of these areas can and should be the focus of deeper analysis.

Joe R. Reeder, a 1970 West Point graduate and 82nd Airborne Division soldier, served as the Army's 14th Under Secretary and Chairman of the Panama Canal Commission (1993-97). For the past 23 years he has been a leader and senior shareholder in one of the world's largest international law firms, Greenberg Traurig, LLP, with clients including public figures, entertainers, and nations.

As a general proposition, the Department of Homeland Security (DHS) orients much more toward cyber defense, while the Department of Defense (DoD) provides cyber offense. Yet our overall national policy remains quite uncoordinated, with several cyber "stovepipes" that have separate authorities and missions, for example: DHS, Department of Justice (DOJ)/Federal Bureaus of Investigation (FBI), DoD/US Cyber Command (CYBERCOM), NSA/Intelligence Community (IC). These stovepipes render coordination ad hoc at best, and more reactionary to cyber events as they arise. The FY21 National Defense Authorization Act (NDAA) created a National Cyber Director to help correct this weakness, but time now is of the essence.

A Brief History of Ransomware Attacks in the United States

On Friday, May 7, 2021, at 5:00 AM, a Colonial Pipeline employee found an electronic ransom note demanding millions of dollars in cryptocurrency.[4] Within seventy minutes of this discovery, Colonial Pipeline shut down all 5,500 miles of its pipelines.[5] On June 2, 2021, employees at JBS USA Holdings, Inc., one of the world's largest meat companies and a major beef supplier in the US, awoke to find a similar message. The CEO made the tough decision to pay $11 million in ransom.[6] Less than a day later, the ferry service that shuttles sightseers to Martha's Vineyard met the same fate. Along these same lines, even a global pandemic did not deter malicious actors from targeting facets of everyday life, from tourism to lifesaving medicines.[7]

While it is partially true that ransomware hackers began with low-profile targets and grew bolder over time, public health researchers may have been the first ransomware victims. In 1989, Joseph Popp, a Harvard-educated evolutionary biologist, delivered floppy disks to twenty thousand researchers worldwide that purported to include an informational program pertaining to AIDS.[8] This elaborate ruse succeeded in infiltrating researchers' networks and encrypting their files, and

Tommy Hall, a West Point senior, focuses his research on China, including how historical concepts of nationalism influences contemporary interstate relations, domestic politics, and Communist Party legitimacy. His other interests include US cybersecurity, refugees, and human rights policies. As a Stamps Scholar, Chinese language major, and West Point policy debater, Cadet Hall hopes to use his expertise to build diverse, interdisciplinary teams willing to tackle the complex challenges that intersect national security and human rights in the 21st century.

Popp's floppy disks demanded a fee for decryption. These initial ransomware attacks amounted to urgent messages and encrypted files in exchange for money, or "scareware" that bombarded computers with pop-ups and urgent messages such as "SECURITY WARNING!"[9] Computer operator victims, upon closing the warnings, found their files encrypted. The goal of such pioneer ransomware hacks mirrors the Colonial Pipeline attacker's: strangle the victim until it pays the ransom to unlock captive files.

Ransomware has become increasingly common and hard to defend against. Ransomware attackers can look for any vulnerability across a vast array of targets, exploit it, and extract a ransom. This general strategy is what makes ransomware, at its core, an opportunistic attack. Effectively thwarting it requires either defending every target (an unworkable solution) or undercutting the business model itself by exponentially raising financial costs. The US Government (USG) faces similar challenges with general cybersecurity. What is different with ransomware is that it is intentionally disruptive – a far cry from traditional attacks that prioritize stealthy and long-term network penetrations over all other considerations.

Both the number and magnitude of ransomware demands have exploded over the past decade. In 2015, the FBI estimated the US suffered a thousand daily ransomware attacks, a statistic that quadrupled by 2016[10]. A December 2019 USG report cited nearly a thousand ransomware attacks targeting a range of victims, from pipelines to schools to hospitals.[11] Accurate statistics on ransomware and other cyber-attacks remain elusive, in part due to lack of any standardized statistics that consolidate existing estimates, and, because, as discussed more fully below, the US is yet to commit to a nationwide, collective "buy-in" to the benefits of real-time reporting and cooperation with government cyber institutions. Similar to Dr. Anthony Fauci's efforts to motivate 100 percent COVID-19 vaccinations, catalyzing

cybersecurity "buy-in" is essential. By some accounts, literally millions of ransomware attacks go unreported, but these estimates vary wildly and many are based on one-off, educated guesses at best. See for example, Figure 1 below, which reports the number of global ransomware attacks during 2020 at 304.6 million.[13]

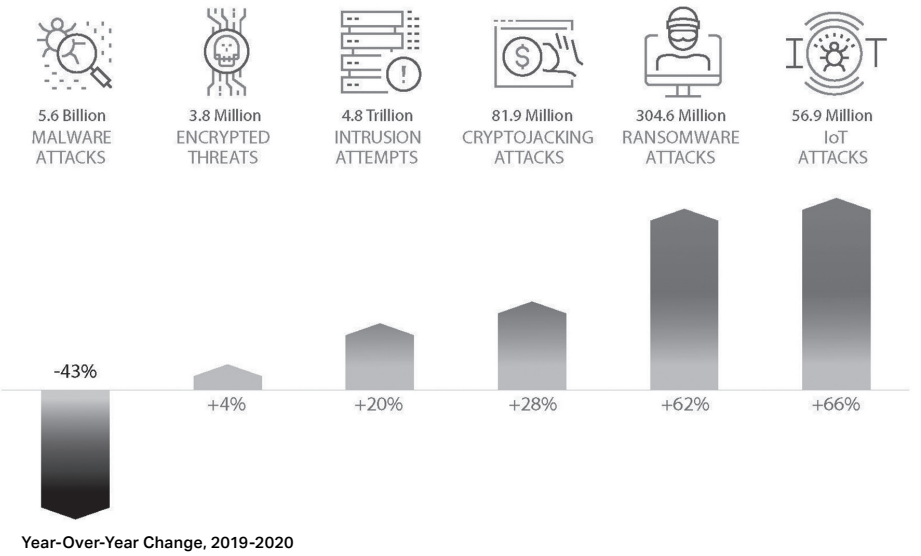

Figure 1. 2020 Global Cyberattack Trends Report by SonicWall

Without granulating based on the size of the victimized business, the average of all ransom demands by one account grew from a few thousand dollars in 2018 to $200,000 in 2020.[14] Hacker methods also have become far more sophisticated and often are timed to strike victims when they are most vulnerable and least able to survive interrupted operations (e.g., hitting schools in August and accounting firms during tax season).[15] The global pandemic gave hackers a golden opportunity to inundate emergency services and struggling businesses. For example, the strike on Universal Health Services and its chain of over 400 hospitals, on September 27, 2020, was the largest-ever medical cyber-attack in the US. *The New York Times*'s top cyber expert, Nicole Perlroth, in her superbly researched book underscores the disturbing rise of cyberattacks experienced during the COVID-19 pandemic.[16]

The White House has attributed the rapid expansion and professionalization of ransomware operations partly to cryptocurrencies' unregulated growth.[17] Bitcoin and other cryptocurrencies, while highly volatile, enhance operational security for money-laundering and ransom pay-offs. Cryptocurrency facilitates ransomware operations by shielding exchanges not tied to or controlled by a central bank, thereby cloaking digital ransom payments in anonymity.[18] Transactions are recorded on a public ledger but are not brokered by a middleman witness to the identity of either party.[19] Nor are offshore cryptocurrency exchanges governed by

anti-money-laundering laws, such as the US "know your customer" (KYC) laws,[20] that penalize those who facilitate financial transactions that facilitate crime.[21]

Many, if not most, of the recent high-profile attacks against the US were perpetrated by Russia-linked cyber-criminal organizations, and cryptocurrencies help conceal them from US intelligence and law enforcement. While the Kremlin's denials no longer seem plausible, Russia persists in fiercely denying any coordination, for example, with the DarkSide group or REvil. Whether or not our intelligence community still lacks conclusive proof as to any specific criminal, Eastern European- and Russian-based cyber-criminal syndicates continue to target US public and private entities with impunity and have yet to face meaningful repercussions.[22]

Assessment of Critical Infrastructure Defense Progress

Not until 2018 did the DoD designate protecting "US critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident,"[23] as a top cyberspace priority. Presidential Policy Directive 41 (PPD-41) defined a significant cyber incident as one conducted through a computer network likely to harm national security, foreign relations, and/or the US economy, and its definition also includes threats to civil liberties, public confidence, and public health and safety of US citizens.[24]

PPD-41 is a good start, but the US remains far short of its full potential to defend key infrastructure from crippling cyber-attacks, even after devoting a laudable, if not gargantuan, budget to this goal ($17.4 billion spent on cybersecurity-related activities in FY2020 alone).[25] The DoD has no statutory authority to "protect" critical domestic infrastructure, yet received $8-10 billion of this total. About $2 billion went to DHS's Cybersecurity and Infrastructure Security Administration (CISA), the agency statutorily charged with assisting to protect domestic critical infrastructure. Wholly aside from the resource allocation, obviously more must be done to prevent novice[26] criminals from being able to cripple the flow of gasoline over 5,000 miles of pipeline that supplies 45 percent of fuel along the entire East Coast for over a week.[27] More sophisticated criminals mounted a multi-country assault that threatened our food supply with the JBS ransomware attack.[28] Both Colonial Pipeline and JBS restored operations relatively quickly but not before paying multi-million dollar ransoms to criminals. These incidents also panicked millions of Americans and laid bare our nation's stark vulnerability and lack of resilience.

In the June 8, 2021 hearing on the Colonial Pipeline attack, Chairman Gary Peters of the US Senate Committee on Homeland Security and Governmental Affairs reflected the fears of the American public and the defense community in his questioning of the company's CEO: "Mr. Blount, I am glad your company continues to recover from this malicious attack and that the FBI was able to recover millions of dollars in ransom pay, but I am alarmed that this breach ever occurred in the first place and that communities from Texas to New York suffered as a result."[29] Mr. Blount explained that, "we responded swiftly to the attack itself and to the disruption that the attack caused ... We reached out to federal authorities within hours of the attack

and since that time we have found them to be true allies as we've worked quickly and safely to restore and secure our operations."[30]

This exchange reveals two truths that the American public, the USG, and critical infrastructure owners must face. First, cybersecurity weaknesses continue to make our country's infrastructure vulnerable to attack. In our increasingly interconnected world, cybersecurity vulnerability manifests itself in more disruptive economic costs, to the point of posing a credible threat to national economic stability. Second, the best, and perhaps only, corrective actions will require effective, real-time collaboration, from ground-level analysts up to senior management, among federal, state, and local governments, and, equally importantly, with the full participation of our private sector. The private sector manages up to 85 percent of all critical US infrastructure,[31] yet the bulk of the country's vital infrastructure does not receive the corporate and USG resources needed to defend against cyber criminals. That being stated, resources alone are not enough. Long-term success will require strong, focused USG leadership that is able to motivate a strong sense of urgency, and that provides clear and executable guidance, and collaboration with the private sector, characterized by genuine, two-way trust that rewards both sides with sharing of sensitive information in real time, specifically as to (a) strict adherence to basic cyber hygiene, (b) identification of all vulnerabilities,[32] (c) reporting of attacks, (d) coordinated response to such attacks, and (e) prompt sharing of evolving best practices. Notwithstanding anonymity guarantees and limited liability protection, voluntary sharing thus far has failed. The key public policy question we now face is not whether to require the sharing of information (through reporting), but rather, how to require information, and from whom.

LESSONS THE NATION MUST TAKE TO HEART

1. Start with Adhering to Cybersecurity Basics.

While there are no silver-bullet solutions to ransomware, three basic cybersecurity ground rules must always be followed: (1) require multi- or two-factor authentication (2FA); (2) integrate segmentation into cyber systems; and (3) adhere to routine "patch-Tuesday" industry- standard practices.[33] Sadly, Colonial Pipeline exemplifies one of many avoidable attacks in which the criminal organization exploited the company's lack of safeguards, specifically 2FA. While hardly a panacea safeguard against hacker penetration, 2FA would have prevented this one.[34] Using a single password obtained from the dark web to log into a VPN account connected to Colonial Pipeline's network, DarkSide hackers exploited the absence of this basic 2FA cybersecurity must.[35] One obvious lesson for Colonial Pipeline is clear: "Never again" violate any of the three cardinal hygiene basics.

In defending against malicious cyber-actors, both government and private sector players must adhere rigorously to all cybersecurity fundamentals. Along with embedding these cybersecurity basics, we also must establish simple digital literacy about commonly used network infiltration tactics for everyone having any role in protecting critical infrastructure.

Moreover, even after solid digital literacy and safeguards are in place, periodic audits and testing are essential.

Seasoned cyber experts also agree that most of China's and Russia's offensive cyber capabilities would die in the cradle if the US adhered to the three basic cybersecurity protocols.[36] These protocols will help protect against not only less sophisticated, non-state-sponsored cyber-attacks, but also near-peer nations that are armed with some of the world's more advanced hacking capabilities. On what was a more sophisticated operation calling for the immediate shut down of servers, *The Washington Post* on July 3, 2021 reported what it termed the largest non-nation state supply-chain ransomware attack ever, affecting over hundreds of businesses using managed IT services. The hackers armed themselves with two different ransom notes that demanded $50,000 of smaller firms and $5 million from larger ones.[37] This report also noted the rise of "hackers' band[ing] together and form[ing] cybercriminal gangs to extort...payment," gangs that begin by exploiting basic vulnerabilities before launching more sophisticated tactics.[38]

2. Protect the Nation's Critical Infrastructure by Elevating the USG's Aspirational Private-Public Partnership (PPP) as a Top Priority.[39]

Federal officials reportedly criticized Colonial Pipeline for not immediately involving CISA in post-attack investigation efforts,[40] revealing problems with collaboration and information sharing between the USG and private firms.[41] The roles and missions of the many involved USG agencies must be clarified so that infrastructure operators fully understand reporting protocols and ongoing collaboration.[42]

In contrast to CISA's reported frustrations, other agencies applauded Colonial Pipeline's close coordination.[43] On June 3, 2021, the DOJ formed the Ransomware and Digital Extortion Task Force in order to help centralize federal law enforcement efforts in combatting such cyber-attacks.[44] Within days after its launch, this Task Force seized 63 of the 75 bitcoins Colonial Pipeline paid to DarkSide as ransom, recovering over $2 million.[45] JBS paid nearly three times that ransom with no funds yet recovered. The FBI attributes the 3-country JBS attack to REvil, a far more sophisticated ransomware hacker than DarkSide.[46] Given the assets the USG can bring to bear, cyber-attacks almost always should trigger immediate federal agency reporting and cooperation.

Few seriously question the US prowess as a cyber trailblazer, but recent ransomware attacks demonstrate an abject failure so far to achieve critical private-public partnership (PPP) policy goals spelled out almost two decades ago in the National Strategy to Secure Cyberspace. This seminal cyber policy statement explained why protecting critical, Internet-connected infrastructure systems is impossible without a strong PPP.[47] A decade later, the Obama administration adopted the framework now in use to enhance PPPs—a voluntary partnership model that enunciates overlapping but also distinct goals for commercial cybersecurity and national security.[48]

The current voluntary PPP model continues to leave the US vulnerable, so the USG must consider complementing a better PPP with select mandated standards that appear to be working well for certain US allies. A good starting point might be to take a hard look at the insurance industry, that as of April 2021 was exposed to a $1 trillion in cyber insurance policy limits.[49] Unlike car insurance, cyber insurance thus far is voluntary. Making it mandatory, at least for certain critical companies, is a common sense step forward. The excellent, April 2021 Ransomware Task Force Report commissioned by the Institute for Security & Technology (IST) highlights the rapidly evolving role now played by privately placed cyber insurance. Less than 15% of global organizations have cyber insurance today, (including about 1/3 of all large US companies).[50] About 20 of the largest insurers dominate this market, and the (a) rising premiums, (b) coverage restrictions, and (c) more stringent underwriting requirements in the marketplace are quite telling. In a very positive way, these changes can and should lead to seismic shift among companies exposed to ransomware in terms of investment and vigilance.[51] In addition, some insurers have close connections with national and global law enforcement to facilitate the data-sharing and threat intelligence.[52]

Nicole Perlroth notes that several of the world's more digitized countries seem nowhere near as vulnerable to cyber-attack as the US.[53] She criticizes as wrong-headed US Chamber of Commerce lobbyists who complain that even voluntary standards are too onerous for private sector operators of our nation's critical infrastructure, and cites as proof several studies of the Scandinavian countries, Norway in particular (the world's fifth most digitized country), and Japan.[54] She urges the need for laws with "real teeth" that, in addition to the three cyber hygiene basics, mandate immediate replacement of antiquated and/or unsupported software. Perlroth also commends Norway's annual revisit and update of its 2003 national cybersecurity strategy, noting that Japan does the same with its "remarkably detailed" cybersecurity policies first established in 2005.[55]

Developing a much more integrated, effective PPP solution presents basic challenges, but none that are insurmountable. First, while profit-oriented private corporations are fully incentivized to pay what it takes to secure their own cyberinfrastructure, only the federal government can be expected to invest the time, effort, and resources that will secure the entire national security ecosystem, particularly against nation-sponsored adversaries. Vaughan Grant, former policy manager of the Australian Army's cyber operations, observed that "the social benefits derived from cybersecurity for critical infrastructure do not readily translate into economic benefits."[56] Colonial Pipeline and JBS executives would probably agree that effectively safeguarding their operations with no governmental support would be cost-prohibitive. The public's cybersecurity needs obviously are not driven by the profitability of any one or more companies, which is why the federal government's role in the PPP team is essential.

Second, information sharing between private industries and the USG remains largely left up to private industry owner discretion.[57] Absent company permission, USG agencies cannot

properly access network information to assist corporate efforts that lessen vulnerabilities to attack, and/or otherwise help respond post-attack.[58] Again, what is now voluntary should become mandatory, with crystal clear ground rules as to what entities and what information must be reported, and to whom. Even if the USG worked much harder at the never-ending challenge of earning, and then holding, the trust of corporate America, "voluntary" may never work effectively. Nor do we have the luxury of time in which to experiment. The USG must take the lead, first by creating a clear and easily executable standard operating procedure with private sector partnership. The USG also must work to ensure that PPP "sharing" procedures do not compromise (a) security classifications, (b) competitive market realities, or (c) international laws. While due to US intelligence laws and not public-private information sharing, the mid-2020 European Court of Justice decision, Schrems II, invalidated the privacy shield after concluding that US law failed to protect data privacy.[59] Finally, and as a further inducement for private sector involvement, the USG should provide incentives (e.g., liability protection for those entities that have satisfied certain standards), and other reasons to trust the USG. Otherwise, a tightly integrated level of real-time, meaningful information sharing will never happen.[60]

The Obama administration in 2013 with E.O. 13636 groped with a fundamental challenge that still haunts the US—defining what constitutes truly critical infrastructure. Today eight years later, the definition of critical infrastructure has become so broad and unwieldly as to be meaningless. The Cyberspace Solarium Commission (CSC) sought to address this issue with the term Systematically Important Critical Infrastructure (SICI). Legislation is sorely needed to define this basic term. Lack of an accurate definition makes it literally impossible to determine the benefits to, and the burdens of such entities—benefits and burdens that also are in sore need of legislation. Also excluded in 2013 from E.O. 13636 was an effort to define was the IT sector. The devastating December 20, 2020, SolarWinds attack, has no doubt taught us that excluding IT as a protected SICI has left a glaring hole.[61] The USG cannot work closely with all of the hundreds of thousands of US entities vulnerable to cyber-attack, the vast majority of which are not truly critical, but we do need to get the definition right in order to protect what is essential.

Without a disciplined, workable definition of SICI, PPP cybersecurity efforts today cannot begin to build the essential high level of trust and integrated cooperation necessary. So, at best, what we have is a piecemeal, post hoc division of labor once crises surface. At worst, but still better than nothing, vaguely drawn, uncoordinated "boundaries" exist with respective private-public players bumping into each other, dusting off, and walking away—two separate, uncoordinated entities facing a common enemy without any collective plan of defense. The US sometimes performs more optimally, but *always* must become the goal. To achieve that ideal, a solid PPP must be developed with all SICI's, and it must extend well beyond pre-crisis agreement on respective responsibilities, to include collaborative exchanges from the bottom up in

each respective organization. The private sector can never shift all leadership responsibility to the federal government and then assume a passive "observer" status, because the first line of private-sector cybersecurity defense is, and will always be, the private sector that is privy to information no one in the USG has. Defense of critical infrastructure requires focus on highly collaborative and integrated *partnership*—the third of the three "Ps" in PPP. Serious leadership challenges face both partners: corporate leaders must be receptive towards the USG, and the USG must earn corporate confidence needed before gaining access to network and other highly sensitive commercial information. The USG can prove with the reward of success why private sector players should feel highly incentivized to collaborate fully, before, during, and following cyberattacks. Yet, this leadership challenge is more than simply providing rewards and, if mishandled, can degrade trust.[62]

Deconfliction is important, as is effective division of effort, but public-private collaboration at its best will require information sharing and task sharing without condition. Not always, but often, the US IC collaboration with international partners provides good examples. Ideally, ground-level analysts openly share experiences, even including hunches and insights. It should be likewise, with cybersecurity. Achieving this ideal will push us closer to 100 percent need-to-know transparency at each echelon of PPP organizations. The intelligence community may never allow 100 percent transparency, given the risk of compromising of sources, but to preserve trust, that should be the goal.

A joint DHS-private sector collaborative research project showcases examples of what should become our norm.[63] The Internet Security Alliance (ISA) independently singled out two partnership programs that embodied cohesive PPP, judged as successful initiatives by private industry and government: the CSRIC Working Group 4 program; and development of the NIST Cybersecurity Framework.[64] Best practices include: continuous interaction among key stakeholders constantly reinforced commitment to the partnership at all levels of the chain of command; and agreed-upon resourcing and collaboration in all goal-setting phases of operations.[64] The project also highlights the importance of trust-building among federal agencies and private-sector leaders to the success of coalition forces and joint operations among our military services. Ground-level trust among employees is also essential, since many threats can and should be resolved where the rubber meets the road. After all, it was a Colonial Pipeline control room operator who discovered the ransomware attack, not the CEO.

The USG has proven capability to build reliable and robust PPP teamwork, and greater USG attention to use in cybersecurity is long overdue. The Colonial Pipeline attack caused elements of the federal government and private industry to work hand-in-hand to mobilize available resources. Enemies and attack methods are improving dramatically. We are capable of meeting the task of defending against increasingly sophisticated cyber threats, but not without prioritizing those threats and resourcing our defenses with strong leadership that recognizes and fosters the trust and collaboration needed to build a joint USG-private sector cybersecurity team.

3. Improve Vigilance Across the PPP

The world watched a ransomware attack cripple the 5,000-mile East Coast pipeline and the ensuing pandemonium at tens of thousands of gas stations. Despite USG assurances that the fuel supply would swiftly return to normal, drivers panic-purchased gasoline (some even filling large plastic bags with fuel), gas prices at some pumps reached levels not seen since 2008,[66] then pumps ran dry at over 12,000 gas stations across the southeastern US as the panic-buying frenzy as consumers broadened their search radius for fuel. While only the first total shutdown of Colonial's gasoline pipeline system in its 57-year history,[67] we must make it the last.

Throughout the Colonial Pipeline attack and ensuing chaos, malicious actors worldwide were learning the economic and social costs that even immature hacking groups could cause. International adversaries, both revisionist and rogue states, observed firsthand how a single cyber-attack caused panic and disruption to energy delivery in the US. To deter such criminal activity successfully, we must ensure hacking groups can no longer expect to execute ransomware extortion operations with impunity and reap multi-million dollar payoffs. Secretary of Homeland Security Alejandro Mayorkas put US ransomware losses over the past year at over $350 million, along with a 300 percent increase in damages due to all cyber-attacks. Although the Colonial Pipeline attack was partially thwarted, more experienced hackers from well-funded revisionist regimes such as Russia or China still pose a formidable threat.

The FBI retrieved some stolen funds, but much remains to be done to avoid encore attacks. As is true of kinetic wars throughout history, defending against cyber-attacks[68] is and must remain an unending, iterative process of incorporating new data points and assumptions. Malicious cyber-attackers will increasingly be more sophisticated, bold, and attack with greater frequency, particularly if they perceive vulnerability. Paying hackers a ransom, while perhaps not always avoidable, obviously finances yet further attacks. It also encourages copycat attacks, as does the lack of adverse, credible consequences for non-state actors and adversarial host countries alike. UK's Home Secretary Priti Patel provided many reasons why paying ransoms in the long run is bad policy,[69] a sentiment increasingly accepted globally.

4. Achieve More Effective Deterrence of State-Sponsored Cyber-Attacks by Clearly Defining "Red Activities," Not "Redlines."[70]

As the US grapples with how best to integrate cyber operations into existing concepts of interstate war and conflict, long-accepted modalities and paradigms require fresh analysis. Colonial Pipeline exemplifies how cyber-attacks blur long-accepted conflict boundaries. While few may attribute the pipeline attack to the Russian government itself, many reports finger Russia as affording sanctuary to DarkSide, an attacker that never targets Russian-speaking assets. Whether and how the Kremlin is ever conclusively linked to this attack, such future attacks, by states, state-sponsored actors, or even by state-tolerated actors can cause devastating consequences to the US. Attribution in kinetic military operations is often[71] sufficiently ambiguous to invite "plausible deniability." In contrast, ambiguity in cyberspace is a defining characteristic.[72]

Ambiguity combined with the breadth of ways that cyber-domain attacks and attackers harm their victims — physically, economically, politically, socially, and/or psychologically — raise questions as to when "redlines" make sense, and if so, how they should be drawn. A better response to cyber offenses, whether by state- or non-state criminal actors, might be a well-defined array of "red activities," each one or more of which will or simply "may" trigger serious consequences. What DarkSide perpetrated obviously would qualify as a red activity. Taking out and/or punishing DarkSide would be one response to this red activity, but what about Russia? While the public is not privy to all information at our intelligence agencies' disposal, we do expect that Russia should want to avoid consequences for the whole spectrum of its likely involvement, whether: (a) nonfeasance; (b) the actual perpetrator, with DarkSide (or the far more formidable REvil) fronting; (c) harboring the criminal hacker, and/or knowing in advance and/or facilitating the attack; (d) having advance knowledge and failing to deter; or (e) having no advance knowledge, but doing nothing after the fact to prevent future attacks on American soil. Perhaps the spectrum of Russia's possible complicity could be further granulated, but going forward, what is it we want to place squarely in Russia's decision-making calculus? Russia must want to avoid being in any US crosshair, for any aspect of DarkSide's crime, or the crimes of any other cyber crime syndicate—perpetrating, facilitating, harboring, tolerating, or even learning about it and doing nothing, after the fact. Each of these wrongs should constitute a red activity, and each should lead to a credible consequence. In their decision-making calculus, all actors should be highly motivated, if not even rewarded (or at least left alone), for proving innocence. As the lead *Washington Post* editorial on July 9, 2021, put it, "Does anyone really believe [the Kremlin] is incapable of doing anything at all about even the most prolific and prominent hackers within its borders?"[73]

Our posture of deterrence against nuclear, chemical, biological, or other existential threats, while less flexible and far less nuanced, can provide some context. Take as examples the recent attacks by DarkSide and REvil, and Russia. Whether or not Russia was the actual perpetrator, at a minimum it clearly toed any redline we would have drawn to a pipeline or other infrastructure attack. However, culpable conduct that may attempt to shroud itself in ambiguity might well be more effectively deterred, or countered, with ambiguous but telling consequence—the where, the when, and the how we reciprocate should be on our timetable and in our decision wheelhouse. Equally important, Russia should be highly incentivized to demonstrate innocence credibly. Obviously, the best way to do that would be for Russia to "out" DarkSide and REvil, prosecute them, and/or otherwise disable their ability to victimize US interests, which Russia clearly is capable of doing. On July 13, 2021, David Sanger's report "Russia's most aggressive ransomware group disappeared. It's unclear who made that happen," confirmed that, like DarkSide, following President Biden's warning call to Putin, REvil went dark, for one of three reasons: (a) Putin shut it down, (b) USCYBERCOM shut it down, or (c) it self-destructed.[74]

Another challenge posed by one-shoe-fits-all redlines, which are harder to tailor to the cybercrimes, is a fundamental difference between closed authoritarian countries and transparent

democracies. Conceptually, as President Obama learned in Syria, once drawn, a redline creates political pressure, put crudely, to satisfy bragging rights as to accountability—punishing the bad actor that crossed the line. Unlike conduct flagged as one of a list of "red activities," the very notion of the word "redline" exposed President Obama to what's commonly known as a "commitment trap." Once he drew a "redline," Syria's subsequent transgression demanded a concrete response in order to avoid domestic, indeed, worldwide political condemnation for weakness. A free press and citizens in a democracy likely would better understand and accept ambiguity if, instead of somewhat less flexible "redlines," we substituted a range of "red activities."

Clearly defining one or more red activities—unacceptable behavior in cyberspace that may or may not fall short of an act of war—is critically important, and the Colonial Pipeline attack highlights a handful of such activities that should open the door to retaliatory consequence. We must work to find ways to motivate nations to want to avoid harboring or providing sanctuary to cyber-attackers. Exposing them to consequence unless they shoulder the burden of demonstrating their innocence would help achieve that. Some countries care little about their reputations (e.g., North Korea), but other countries do care (e.g., China), and the best way to establish innocence is to take visible actions to pursue, punish, and otherwise eliminate any perpetrator of harm to other nations, including its infrastructure and its citizens. The most effective way to change Russia's decision-making calculus may be to impose an unbearably high cost if it chooses to go the wrong way, and "one size" clearly does not fit all transgressions. Rather, the response must be tailored to ramifications the offender truly cares about.

Determining how most effectively to impose costs on bad actors for implementing, or even merely tacitly approving, cyber-attacks on other nations or their citizens, would greatly benefit from the USG applying the three-layered cyber deterrence strategy urged by the 2020 Cyberspace Solarium Commission.[75] The Commission Report goes into each of these layers, described briefly in ascending order of gravity: (a) shaping behavior; (b) denying benefits; and (c) imposing costs. Recognizing the importance of PPP, layered cyber deterrence combines and extends many traditional deterrence mechanisms in a whole-of-nation approach to cybersecurity.[76] A facet of that first layer, deterrence by norms, includes partnering with reliable allies that are mutually motivated to define red activities and collectively impose costs on cybercriminals. The Commission also included in the first layer, for more neutral countries, deterrence by entanglement, wherein the USG creates beneficial engagements that could disappear for countries caught cyber misbehaving.

The second deterrent layer is a denial of benefits or rewards for cyberspace crimes, including intellectual property theft, malign influence operations, and significant attacks on critical infrastructure.[77] Deterrence by denial is enhanced by reinforcing private-public sector bonds through activities such as expanding operational collaboration and pooling data on cyber-attacks.[78] This layer impacts the adversary's decision-making calculus by ruggedizing US

assets—making them more resilient and impenetrable—to force malicious actors to weigh the efficacy of their current resources and capabilities.

The third and most severe of the three deterrent layers imposes escalates punitive consequences for increasingly serious cyber-attacks, particularly those that threaten US national security. All deterrent layers fall under an expanded and reimagined umbrella of DoD's "defend forward" cyber-operations doctrine. Full success will require employing these layers concurrently, continuously, and collaboratively, to include, if necessary clarity that crippling counter-cyber-attacks, and/or even use of military force are options that may become necessary at a time and place of USG choosing.[79]

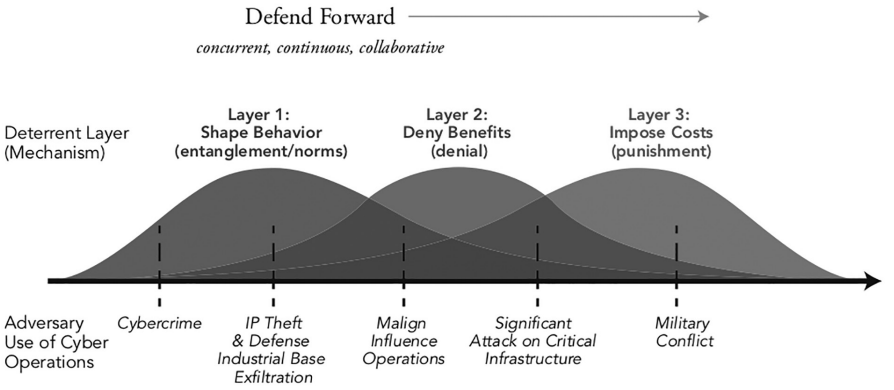

Figure 2. Layered Cyber Deterrence

These layered deterrence steps are best taken from left to right, integrating each deterrence building block, as shown in Figure 2, above.[80] This process starts with a clear and effective cyber-defense strategy and clear national security priorities, and ends with delivering swift and decisive consequences. Again, basic cybersecurity hygiene will clear the field of most amateur hacking to allow concentrated focus on more skilled actors and critical assets. Whereas the first layer on the left in the figure above may begin with detection, more active defense moving to the right by adding attribution, increases the overall the cost in the adversary's decision-calculus. Identifying red activities essentially works as an ocean-level berm that helps obviate the need to devote critical USG resources and energy chasing amateur hackers. It also lets near-peer adversaries know that more potent instruments of power are available, fully capable, and laser-focused on delivering punishing consequences.

5. Expand the Cybersecurity Defend Forward Doctrine

The 2018 DoD Cyber Strategy commits the US to "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[81] This aspect of the new cyber strategy adopts the age-old adage that the best defense is a good

offense. This strategy, however, has yet to prevent increasingly bold and frequent cyber-attacks on USG agencies and businesses. For example, the Russian-based Nobelium hacking group employed the same spearfishing tactic it unleashed in the 2020 SolarWinds operation to target human rights groups critical of Putin and the U.S. Department of State (DOS), starting in January 2021 and escalating four months later in May.[82] Ransomware tactics used against Colonial Pipeline were duplicated just weeks later in attacks on JBS and the Martha's Vineyard ferry. To those following US cybersecurity efforts, none of these attacks should be surprising. In 2019, the DHS published a report confirming critical infrastructure as an ideal target for both near-peer competitors and decentralized malicious cyber actors.[83] Indeed, well beforehand, cybersecurity experts envisioned a scenario like the Colonial Pipeline attack.[84]

Further efforts to formulate ransomware response strategy must more broadly define what it means to defend forward. The Biden Administration is seeking to build an international coalition to pressure those countries to hunt down and prosecute cyber-criminal syndicates they are harboring,[85] and increasing diplomatic pressure on ransomware criminals, by pressing for change to global financial policies relating to cryptocurrency. Specifically, it seeks to establish an international standard comparable to the U.S. Treasury Department's know-your-customer requirement, to eliminate the anonymity that hides malicious actors from the law, and add anti-money-laundering mandates.[86] Others have called for the US to deploy military and intelligence agencies in offensive cyber operations that target the technical infrastructure hackers use to employ cyber-attacks.[87] FBI Director Christopher Wray has compared a string of high-profile ransomware attacks to national security threats posed by the September 11, 2001, terrorist attacks.[88] Federal criminal justice and law enforcement agencies have become much more integrally involved in tackling ransomware cases. Indeed, the DOJ and FBI worked closely together, along with a ransomware law enforcement task force, to recover much of the ransom stolen from Colonial Pipeline by obtaining a warrant to seize a digital wallet containing much of the bitcoin ransom.[89]

Ramped up US participation in PPPs will require hard, continuous private and public sector work. A well-intended Treasury Department's Office of Foreign Assets Control (OFAC) advisory in October 2020 threatened fines for "facilitating payments to criminals." This advisory was intended to deter ransom payments that would encourage more hacker demands.[90] Even though reported ransoms paid declined in number, many viewed the OFAC advisory as unwise, because, unlike Colonial Pipeline and JBS, fewer victims would report paying ransom.[91] Some suggest that, rather than wielding sticks, the US would benefit more by dangling carrots. John Davis, a vice president of the cybersecurity firm, Palo Alto Networks, discourages punishing victims that pay ransoms, urging instead mandatory reporting of ransom payments to federal authorities and "creating a fund to support victims who refrain from paying ransoms."[92]

6. Create Standing Procedures in the PPP for Warp Speed Information Sharing When Key Ransomware Attacks Occur.

Colonial Pipeline deserves credit for promptly notifying federal law enforcement and government authorities of the ransomware attack. Cyber-attacks of this magnitude require an immediate communication, not an after-the-fact debrief.[93] A key difference between a cyber battlefield and a physical battlefield is the need for response time measured in nanoseconds, not hours or even minutes. Every moment lost gives time to adversaries to cover their tracks, launder stolen funds, and/or distribute or expose stolen confidential files. Nothing beats early and ongoing USG-private sector communication and cooperation as the first post-attack step for victims struggling to minimize losses.

Knowing how the USG will use and protect information should greatly allay private corporate concerns. At least four possibilities come to mind. First, the USG may want to impose a consequence on the private entity and hold the appropriate individuals accountable for allowing a major cybersecurity incident to happen—the "gotcha" reason, either regulatory or punitive, or both. Second, the USG may want to help shut down the attack and/or interrupt a ransom payment, as occurred with Colonial Pipeline—the "help you" rationale. Third would be sharing information in an effort to inoculate others against the same or similar threat. And fourth, and strategically over the long term, would be to help the USG develop and maintain a continually updated statistical basis to craft policy. While less important for assessing blame, timeliness is especially important for the second and third potential uses of information. Corporate counsel today often blocks the proactive information sharing urged here. The USG should ensure that the private sector understands the USG is truly seeking to help and is not asking the private corporation to indict itself or its leaders for having fallen victim to a cybercrime.

Demands and penalties work, but combining those with long-term incentives likely will result in better overall response and candor from the private sector. If the USG explains why quick notice and teaming greatly benefit the company, these incentives will reinforce the trust to team success. One huge incentive will be immediate USG feedback to the victim of anything the USG has seen that may differ from the victim's take. Private firms could be penalized for coming up short in their due diligence efforts before an attack, or for haphazardly built cybersecurity systems, but far more important is building a trusting team with buy-in from all sides. Certainly, beyond the unavoidable reputational damage already incurred, no firm should suffer for volunteering information to the USG about a ransom attack.

While not the focus of this article, technological superiority always will be key to any effective cyber defense, particularly given the sophistication of some adversary nation-states, and even other groups, like REvil. As important, however, is the human dimension, as is true whenever collaborative teaming is mission-critical. Before, during, and after an attack, attention must be paid to the ongoing human decision-making calculus, especially during the crisis. Take, for

example, the contrast between the 2013 Target and 2014 JP Morgan Chase cybersecurity data breaches. Target disclosed all known details of the cyber-attack to the public, even admitting gaps in its understanding of the attack and lack of a response plan. The press, public, and his board's backlash forced Target CEO Gregg Steinhafel to step down; Target was fined over $18.5 million in a multi-state lawsuit, and top information officers were fired.[94] Learning from Target's public crucifixion, when victimized by an even more serious data breach, JP Morgan Chase delayed the public announcement for many weeks while it quietly took corrective action.[95] The takeaways here are clear: If the USG prioritizes, or even harbors as a latent goal, hunting for whoever messed up, or stabbing the already wounded, such approaches will discourage early self-reporting to the USG, and companies must also consider their reporting requirements to shareholders and the public.

The USG has taken three nascent steps toward mandating self-reporting. First, within days following the Colonial Pipeline attack, President Biden issued his May 12 Executive Order (EO) (Improving the Nation's Cybersecurity), signed, requiring all defense contractors to self-report. This step indicates clear progress, but it leaves a gaping hole— it did not include non-defense contractors. The framework for increased information sharing, outlined above in Section 2, describes what should be mandated much more broadly, to include: (a) collection and preserving data relevant to IT systems controlled by the service provider; (b) sharing such collected data; and (c) collaborating with federal cybersecurity investigations.[96]

Second, the TSA released a May 27 directive requiring all pipeline owners and operators to (a) complete and submit cybersecurity assessments to both TSA and CISA within 30 days, (b) report all "confirmed and potential" cyber-attacks to CISA, and most uniquely, (c) appoint a 24/7-available cybersecurity coordinator to work with the USG on cyber-attack responses.[97] Like the President's EO, however, this DHS/TSA directive applies only to a select subset of private industry (i.e., critical infrastructure service providers).

Third, Chairman Mark Warner of the Senate Select Committee on Intelligence Committee spearheaded a proposed bipartisan bill that would mandate private industry reporting a cyber incident to CISA within 24 hours.[98] A statement by the Chairman underscores the obvious: "Voluntary sharing is no longer effective."[99] If enacted, this bill, anticipating private industry concerns, would exempt cyber notifications from Freedom of Information Act (FOIA) requests or use of such notifications in prosecuting service providers.[100]

CONCLUSION

This article takes an initial cut on lessons learned following the May 6, 2021 attack on Colonial Pipeline. More information about that attack and its aftermath undoubtedly will become public over time.[101] DarkSide sparked a national dialogue around what appears to be missing from our nation's cyber defense strategy. This article attempts to explain why recent attacks

reinforce the importance of focusing beyond the technical aspects of defense. Most essential is gathering people to work together, with strong leadership and leveraged talent, to secure against and respond to malevolent cyber activity. While the Executive Orders issued thus far are helpful as stop-gap interim measures, also essential are clear, executable legislation and inspired leadership, both for governance, and for motivation of all public and private stakeholders to meet this growing threat by embracing essential PPP collaboration that is integrated at every level of the partnership.

We have cited a clear example of one recent key cyber defense achievement in which a USG-created joint planning cell involving three relevant agencies led to demonstrable success. This example must become the rule and not the exception. We can no longer drag our feet on building an effective coalition among the nearly two dozen federal agencies now operating in cyberspace. Agency teamwork must be streamlined, and, vitally important, the USG team must partner broadly and deeply with all relevant private sector stakeholders, especially those that manage our infrastructure and that face increasingly sophisticated cyber defense threats. Required will be inspired leadership that broadens the aperture and embraces input from a very wide range of skills and personnel. Whenever America embraces its most valuable asset – the broad diversity of its citizenry and talent – it is victorious.[102] That timeless lesson is key to our cybersecurity, just as it has been to our military, our industry, our education, and everything important we have done. However, the US and all vibrant, free market democracies, are up against adversary countries that largely have retained public ownership of critical infrastructure, and also, that exercise far more control over their private sectors than does the USG.

Leadership includes sound management of talent, but it is much more. Defeating cyber adversaries will require cohesive, tested teams that are so conspicuous that they send an unequivocal message to all would-be adversaries. Sound cybersecurity is as much about getting the roles and responsibilities of each public and private stakeholder right as it is about state-of-the-art technology. While not the focus of this article, the US enjoys an enviable, perhaps unparalleled technological edge. Maintaining that edge is an existential imperative. The focus here is more on some key lessons that, if learned, will improve the human teaming element essential to a better defense—the cyber hygiene basics, the legislative clarity, the leadership, and the public-private partnerships and PPP buy-in all essential if we are to minimize the exposure and vulnerabilities inherent in any open, democratic society like ours.

The wakeup call in the first sentence of this article underscores the missing defense so desperately needed for the US to bring its adversaries' soccer cyber scores down from a whopping 456 points to single digits. For highlighted reasons, this defense will require multiple layers of prevention, resilience, and deterrence, along with our national resolve to leverage the full range of financial, legal, diplomatic, and defense assets at our disposal as we target and respond to increasingly formidable cyber-attackers.

ACKNOWLEDGEMENTS

While the authors take full responsibility for any well-intended but incomplete or misguided thoughts in this article, we are deeply grateful to incoming National Cybersecurity Director Chris Inglis, a Cyberspace Solarium Commissioner, for sharing inspiration and invaluable leadership insights from which we fashioned these takeaway lessons from the Colonial Pipeline ransomware attack. West Point cadets and Naval Academy midshipmen over the years owe a great debt of thanks to this Air Force Academy graduate for the thousands of hours he has devoted, teaching them. For their editorial guidance we also give special thanks to John Costello (now with the Center for a New American Security (CNAS) and also a Cyberspace Solarium Commissioner), and formerly Deputy Assistant Secretary for Intelligence and Security at the Department of Commerce, Victoria Lee (Princeton University, 2021), Charlie Lewis (West Point, 2004), Chip Leonard & Bill Spracher (West Point, 1970), and Greenberg Traurig attorneys Paul McQuade & Scott Schipma.

NOTES

1. Dan Geer, "Cybersecurity as Realpolitik," quoting General Chris Inglis, August 6, 2014, http://geer.tinho.net/geer.blackhat.6viii14.txt.
2. Scott Sagan and Allen Weiner, "Would the U.S. really answer cyberattacks with nuclear weapons?" *The Washington Post*, July 11, 2021, https://www.washingtonpost.com/outlook/2021/07/09/cyberattack-ransomware-nuclear-war/.
3. Dustin Volz, "U.S. Blames Criminal Group in Colonial Pipeline Hack," *Wall Street Journal,* May 10, 2021, https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720.
4. Brian Fung and Geneva Sands, "Ransomware attackers used compromised password to access Colonial Pipeline network," *CNN*, June 4, 2021, https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html.
5. Joseph Blount, "Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company," *Hearing Before the United States Senate Committee on Homeland Security & Governmental Affairs,* June 8, 2021, https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack.
6. Jacob Bunge, "JBS Paid $11 Million to Resolve Ransomware Attack," *Wall Street Journa*l, June 9, 2021, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.
7. Heather Kelly, "Ransom attacks are closing schools, delaying chemotherapy and derailing everyday life," *The Washington Post*, June 5, 2021, https://www.washingtonpost.com/technology/2021/07/08/ransomware-human-impact/.
8. Rachel Monroe, "The Go-Between: Negotiating with the hackers and the hacked," *New Yorker*, June 7, 2021, 22, https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.
9. Ibid., 23.
10. Ibid.; see also Lee Matthews, "2016 Saw an Insane Rise in the Number of Ransomware Attacks," *Forbes*, February 7, 2017, https://www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/?sh=3070f86a58dc. This 2017 *Forbes* article quantified worldwide ransomware attacks in 2016 at 638 million—a 167 times increase from 2015.
11. Robin L. Fontes, Erik Korn, Doug Fletcher, Jason Hillman, Erica Mitchell, and Steven Whitham, "Jack Voltaic: Bolstering Critical Infrastructure Resilience," *The Cyber Defense Review* 5, no. 3 (Fall 2020), 45, https://www.jstor.org/stable/10.2307/26954872, citing Sarah Nelson, "Report: Local Gov Cyberattacks Reach Critical Level," *Government Technology*, December 18, 2019, https://www.govtech.com/security/Report-Local-Gov-Cyberattacks-Reach-Critical-Level.html.
12. Monroe, "The Go-Between," 23, 26.
13. Terry He, Rhoda-Mae Aronce, Lalith Dampanaboina, Justin Jose, Michael King, and Edward Cohen, *2021 SonicWall Cyber Threat Report* (Milpitas, CA: SonicWall, Inc., 2021), 5, https://www.sonicwall.com/2021-cyber-threat-report/#form.
14. Ibid.
15. Ibid., 24.
16. Nicole Perlroth, *This—The Cyber-weapons Arms Race—Is How They Tell Me the World Ends,* (Bloomsbury Publishing, 2021), citing Dmitry Galov, "Remote Spring: The Rise of RDP Brute force Attacks," *Kaspersky Labs,* April 29, 2020, www.securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820. Hacking of vaccine data is further discussed in David Sanger and Nicole Perlroth, "U.S. to Accuse China of Hacking Vaccine Data," *The New York Times*, May 11, 2020.
17. Ellen Nakashima, Hamza Shaban, and Rachel Lerman, "The Biden administration seeks to rally allies and the private sector against the ransomware threat," *The Washington Post*, June 4, 2021, https://www.washingtonpost.com/business/2021/06/04/white-house-fbi-ransomware-attacks/, accessed July 10, 2021.
18. Ibid.
19. Ibid.
20. Ibid.
21. Yaya Fanusie, "FinCEN's New Proposed Rule Rushes the Inevitable," *Forbes,* December 28, 2020, https://www.forbes.com/sites/yayafanusie/2021/12/28/fincens-new-proposed-rule-rushes-the-inevitable/?sh=59b9480c4a6f. In December 2020, FinCEN proposed new rules, such as know-your-customer (KYC) requirements on "unhosted wallets," which were not but should have been adopted.

NOTES

22. "Putin is a pro at making arrests," *The Washington Post*, June 11, 2021. The US IC has not publicly confirmed the suspected coordination, but President Biden's statements following the US-Russia summit underscored tension over the Colonial Pipeline ransomware attack: "I looked at him and said: 'How would you feel if ransomware took on the pipelines from your oil fields?'" Accompanying this targeted question, the President reaffirmed the option of offensive and/or retaliatory cyber strikes as a part of the Defend Forward strategy, stating, "I pointed out to [Putin] that we have significant cyber capability. And he knows it"; see also Vladimir Soldakin and Steve Holland, "Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control," *Reuters*, June 16, 2021, https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/; see also Perlroth, "Cyber-weapons Arms Race," 365, quoting Russian cybercrime expert Tom Kellermann: "There's a pax mafiosa between the Russian regime and its cyber cartels. Russia's cybercriminals are treated as a national asset who provide the regime free access to victims of ransomware and financial crime. And in exchange, they get untouchable status. It's a protection racket and it works both ways."
23. Department of Defense, *Summary: 2018 Department of Defense Cyber Strategy* (2018), 3.
24. U.S. President, "Presidential Policy Directive 41 on United States Cyber Incident Coordination of July 26, 2016," 3, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
25. While there are several reasons for this failure, the authors believe the two most important are (a) the lack of truly effective public-private partnering discussed later in this article, and (b) over-reliance by the USG on voluntary as opposed to mandatory standards. Both are essential.
26. Natasha Bertrand, Evan Perez, Zachary Cohen, Geneva Sands, and Josh Campbell, "Colonial Pipeline did pay ransom to hackers, sources now say," *CNN,* May 13, 2021, https://www.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html. This source cites three federal officials as stating, "Among the signs that the [DarkSide] hackers were novices is the fact that they chose a high-risk target that deals in a low-margin business, meaning the attack was unlikely to yield the kind of payout experienced ransomware actors are typically looking for, the sources told CNN." The DarkSide hackers' apologetic response to the unintended consequence of sparking a White House investigation further indicates their amateur status.
27. United States Office of Management and Budget, "Cybersecurity Funding," *Government Publishing Office,* March 11, 2019, 305, www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf; see also Collin Eaton and Amrith Ramkumar, "Colonial Pipeline Shutdown: Is There a Gas Shortage and When Will the Pipeline Be Fixed?" *Wall Street Journal,* May 13, 2021, https://www.wsj.com/articles/colonial-pipeline-cyberattack-hack-11620668583.
28. Eric Rosenbaum, "JBS cyberattack: From gas to meat, hackers are hitting the nation, and consumers, where it hurts," *CNBC,* June 2, 2021, https://www.cnbc.com/2021/06/02/from-gas-to-burgers-hackers-hit-consumers-where-it-hurts.html.
29. *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack Hearing Before the United States Senate Committee on Homeland Security & Governmental Affairs,* June 8, 2021 (statement of Joseph A. Blount, CEO of Colonial Pipeline), https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack.
30. Ibid.
31. Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review* (2017), 494.
32. This article does not flesh out how federally-sponsored Tiger Teams would benefit here, e.g., by testing, auditing, assessing critical infrastructure, and/or providing rigorous hardware and software recommendations. However, like national safety programs, if not mandated, Tiger Teams could be incentivized by amnesty periods for repairing deficiencies or otherwise curing cybersecurity vulnerabilities.
33. It is unclear as to this third cardinal cyber hygienic maxim—patching soft-ware glitches—how long in advance IT software firm Kaseya knew of its patching vulnerability before the devastating cyberattack that crippled up to 1,500 businesses. As the July 7, 2021, *The Washington Post* lead editorial explained: "The firm was aware of the vulnerability exploited [by REvil] and was working to patch it; the problem was the hackers got there first"; see also, Editorial Board, "Opinion: Biden said we'd 'find out' whether Putin would act on ransomware. Now we have," The Washington Post, July 7, 2021, https://www.washingtonpost.com/opinions/2021/07/07/biden-said-wed-find-out-whether-putin-would-act-ransomware-now-we-have/.
34. Josephine Wolff, "Five myths about ransomware," *The Washington Post,* June 10, 2021, https://www.washingtonpost.com/outlook/five-myths/five-myths-about-ransomware/2021/06/10/b1e00344-c8b1-11eb-81b1-34796c7393af_story.html.
35. William Turton and Kartikay Mehrotra, "Hackers breached Colonial Pipeline using compromised password," *Bloomberg News,* June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. Mr. Blount's testimony to the Senate Committee on Homeland Security and Governmental Affairs provides more clarity, as follows: "[W]e believe the attacker exploited a legacy virtual private network (VPN) profile that was not intended to be in use. We are still trying to determine how the attackers gained the needed credentials to exploit it... We have shut down the legacy VPN profile, and we have implemented additional layers of protection across our enterprise. It remains unclear why this profile did not require 2FA or why it still even existed." See also *Testimony of Joseph Blount.*

NOTES

36. Many, including General Inglis during our interview, project that the vast majority of attacks would be thwarted by these three basics. While a US vulnerability gap would still exist, thwarting the vast majority of all malicious attacks would be a huge improvement over what we face today with only partial adherence to these basics.
37. Gerrit de Vynck and Rachel Lerman, "Widespread ransomware attack hits hundreds of businesses," *The Washington Post*, July 3, 2021, https://www.washingtonpost.com/technology/2021/07/02/kaseya-ransomware-attack/.
38. Ibid. Before this article went to print, a broad supply-chain attack widely reported in the news on July 6, 2021, locked hundreds of small and mid-sized businesses, and tens of thousands of computers. The notorious (and highly sophisticated hacker), REvil, took credit and demanded $70 million in ransom; see also Robert McMillan, "Ransomware Hackers Demand $70 Million to Unlock Computers in Widespread Attack," *Wall Street Journal,* July 5, 2021, https://www.wsj.com/articles/ransomware-hackers-demand-70-million-to-unlock-computer-in-widespread-attack-11625524076?mod=searchresults_pos4&page=1.
39. While the first of the 3 Ps in PPP typically refers to "public," flipping the order could help underscore what we believe to be the importance, at least on many fronts, of equality of these two partners, notwithstanding the primacy of the USG in overall national security policy. Moreover, as we endeavor to explain, our legislative and executive branches of government are both essential to that. However, the backbone of success, as was true with the private sector in World War II, will be the private sector's performance in this cybersecurity partnership.
40. Zachary Cohen, Natasha Bertrand, Kevin Liptak, and Geneva Sands, "Biden administration officials privately frustrated with Colonial Pipeline's weak security ahead of crippling cyberattack," *CNN*, May 11, 2021, accessed June 7, 2021, https://www.cnn.com/2021/05/11/politics/biden-administration-ransomware-frustration/index.html.
41. In addition to the newly created White House Office of National Cybersecurity Director, some of the many other governmental players in what is now a confusing mix of nearly two dozen agencies relevant to infrastructure attacks (many involved in the Colonial Pipeline attack) include: the FBI, Cyber Security and Infrastructure Security Agency (CISA), Department of Justice (DOJ), National Security Council (NSC), Department of Energy (DOE), Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center (NCCIC), Pipeline and Hazardous Materials Safety Administration (PHMSA), National Infrastructure Coordination Center (NICC), Federal Energy Regulatory Commission (FERC), Energy Information Administration (EIA), Critical Infrastructure Partnership Advisory Council (CIPAC), Environmental Protection Agency (EPA), National Institute of Standards and Technology (NIST).
42. In addition to the newly created White House Office of National Cybersecurity Director, some of the many other governmental players in what is now a confusing mix of nearly two dozen agencies relevant to infrastructure attacks (many involved in the Colonial Pipeline attack) include: the FBI, Cyber Security and Infrastructure Security Agency (CISA) (within Department of Homeland Security (DHS), Department of Justice (DOJ), National Security Council (NSC), Department of Energy (DOE), National Cybersecurity and Communications Integration Center (NCCIC), Pipeline and Hazardous Materials Safety Administration (PHMSA), National Infrastructure Coordination Center (NICC), Federal Energy Regulatory Commission (FERC), Energy Information Administration (EIA), Critical Infrastructure Partnership Advisory Council (CIPAC), Environmental Protection Agency (EPA), and National Institute of Standards and Technology (NIST).
43. Cohen, "Officials privately frustrated." Although this article does not specify the number of officials and extent of their frustration, key quotes attributed to CISA definitely reveal significant frustration. CISA's Brandon Wales softened comments saying, "We [CISA] have had historically good relationship with both Colonial, as well as the cybersecurity firms that are working on their behalf." Yet other quotes pin down potential points of frustration: "They did not contact CISA directly...We were brought in by the FBI after they were notified about the incident... I think that there's a benefit when CISA is brought in quickly because the information that we glean, we work to share it in a broader fashion to produce other critical infrastructure." This quote indicates that Colonial Pipeline contacted some but not all agencies early on. For several reasons, the authors respectfully hold the USG, not Colonial Pipeline, responsible here. First, certain responsible USG authorities appear to have been timely notified. Second, it should be the USG's responsibility, not private industries, to identify clearly those agencies that require notification, and that was anything but clear on May 6. Third, once a responsible USG official is notified, that official, not the ransomware victim, best knows which other USG agencies require notice, and that official should give that notice. Fourth, and also important, relevant USG and corporate officials alike in the midst of battle (or even after) should refrain from taking public potshots that could undermine trust or divert attention from the attacker—something CISA's Brandon Wales appears to have recognized.
44. Carlie Porterfield, "Department of Justice Creates New Task Force to Take On Ransomware Attacks," *Forbes*, June 3, 2021, https://www.forbes.com/sites/carlieporterfield/2021/06/03/department-of-justice-creates-new-task-force-to-take-on-ransomware-attacks/?sh=396e976a4b80.

NOTES

45. Christopher Bing, Joseph Menn, and Sarah N. Lynch, "U.S. seizes $2.3 mln in bitcoin paid to Colonial Pipeline hackers," *Reuters*, June 7, 2021, https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/.
46. Ryan Gallagher and Alyza Sebenius, "JBS cyber attack raises questions about preparedness," *Bloomberg*, June 8, 2021, https://www.farmprogress.com/business/jbs-cyber-attack-raises-questions-about-preparedness.
47. Larry Clinton, "Best Practices for Operating Government-Industry Partnerships in Cyber Security," *Journal of Strategic Security* 8, no. 4 (2015), 52, DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456.
48. Ibid., 54.
49. "A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," Institute for Security and Technology (April 2021), 60, https://securityandtechnology.org/ransomwaretaskforce/.
50. Ibid., 58.
51. Ibid., 60 and 80, citing "Aon's E&O | Cyber Insurance Snapshot," https://www.aon.com/cyber-solutions/wp-content/uploads/Aon-errors-and-omissions-cyber-insurance-snapshot.pdf; "Cyber may never experience another soft market: Gallagher Re," Intelligent Insurer, April 14, 2021, https://www.intelligentinsurer.com/news/cyber-may-never-experience-anothersoft-market-gallagher-re-25350; 2021 Cyber Insurance Market Conditions Report, https://www.ajg.com/us/news-andinsights/2021/jan/2021-cyber-insurance-market-report.
52. Ibid., 61 and 81, citing to Jeff Stone, "FBI turns to insurers to grasp the full reach of ransomware," Cyberscoop, March 30, 2020, https://www.cyberscoop.com/ransomware-fbi-insurance-companies-data/; Sean Lyngaas, "Inside the FBI's quiet 'ransomware' summit," Cyberscoop, November 16, 2019, https://www.cyberscoop.com/fbi-ransomware-summit/.
53. Perlroth, *The Cyber-weapons Arms Race*, 398.
54. Ibid., 398-99. Norway broadly defines those companies that provide "basic national functions," to include: financial services, electricity, health services food supply, transportation, heating, media platforms, and communications, and penalizes companies that fail to perform penetration testing, threat monitoring, and other basic security measures. In addition to strict standards for government employees, Norwegian companies have made cybersecurity training a cornerstone of their culture.
55. Ibid.
56. Vaughan Grant, "Critical Infrastructure Public-Private Partnerships: When Is the Responsibility for Leadership Exchanged?" *Security Challenges* 14, no. 1 (2018), https://www.jstor.org/stable/26488490.
57. Siobhan Gorman and Julian E. Barnes, "Iran Blamed for Cyberattacks," *Wall Street Journal*, October 12, 2012, https://www.wsj.com/articles/SB10000872396390444657804578052931555576700. In 2012, the Iranians attempted to cyberattack the US in its financial heart. By one account, during a Joint Chiefs of Staff meeting following Iran's probing cyber strikes on Wall Street, one high-profile attendee, questioning the decision requiring private corporations to cyber defend themselves, sardonically asked, if North Korea fired a missile, the US should first determine whether the missile was targeting US troops or US corporation assets before the USG would act. While the question was partly in gest, today, over a decade later, the private sector, indeed all Americans, should know the answer is clear—any attack on any part of the US will be met with swift and unequivocal response of our choosing, on our timetable, and it will be a unified, public-private coordinated response calculated not only to protect but also to punish and otherwise strongly disincentivize any encores.
58. Zachary Cohen and Geneva Sands, "Four key takeaways on the US government response to the pipeline ransomware attack," CNN, May 11, 2021, https://www.cnn.com/2021/05/11/politics/colonial-pipeline-cyber-hearing-senate-homeland-security-committee/index.html.
59. In their research article titled "An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure," *Public Administration Review* (2020), Sean Atkins and Chappell Lawson of the Massachusetts Institute of Technology concluded, following dozens of in-depth interviews, that use of non-profit Information Sharing Analysis Centers (ISAC's) has proven invaluable in facilitating inter-company and public-private information exchange, both within given sectors and even across different sectors. https://www.researchgate.net/publication/346496117. For those interested in why and how whole-of-government policymaking also requires sector-specific tailoring in order to optimize cybersecurity, Professor Lawson's and Dr. Atkins' superbly insightful study is a must.
60. Grant, "Critical Infrastructure Public-Private Partnerships," 41.
61. Tasha Jhangiani and Graham Kennis, "Protecting the Critical of the Critical: What is Systemically Important Critical Infrastructure?" *Lawfare,* June 15, 2021, https://www.lawfareblog.com/protecting-critical-critical-what-systemically-important-critical-infrastructure.
62. Ibid., 45.

NOTES

63. Internet Security Alliance, "Best Practices for Cybersecurity Public-Private Partnerships," in *Input to the Commission on Enhancing National Cybersecurity*, 61, https://www.nist.gov/system/files/documents/2016/09/16/isa_rfi_response.pdf. This research was conducted by both the IT Sector Coordinating Council and DHS. Using a modified critical-incident method that incorporated six case studies, the joint research team developed an agreed list of a dozen best practices that embody successful PPP.
64. Ibid., 62.
65. Clinton, "Best Practices," 68. The author lists nine other best practices in this study: involve industry by using the process known as NIPP; contact stakeholders early on, ideally at the "blank page" stage; continuous and regular government-private sector stakeholder interaction; provide all stakeholders (both public and private) ample time to review and input; establish and encourage co-leadership programs; consensus partnership decision-making; communicate a genuine interest in stakeholder input; robust engagement from federal agencies in addition to DHS; government follow-through on all partnership-related decisions; and adequate, properly resourced, competent support services.
66. Will Englund and Ellen Nakashima, "Panic buying strikes Southeastern United States as shuttered pipeline resumes operations," *The Washington Post*, May 12, 2021, https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/.
67. William Turton and Kartikay Mehrotra, "Hackers breached Colonial Pipeline using compromised password," *Bloomberg News*, June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.
68. Cohen and Sands, "Four key takeaways."
69. Danny Palmer, "Ransomware: Don't pay up, it just shows cyber criminals that attacks work, warns home secretary," May 11, 2021, https://www.zdnet.com/article/ransomware-dont-pay-the-ransom-it-just-encourage-cyber-criminals-that-attacks-work-warns-home-secretary/.
70. Observations and conclusions throughout this article are those of the authors. The notion of "red activities" in lieu of "red-lines" in response to cyber misbehavior was inspired by our interview of General Inglis.
71. Peter Apps, "West struggles with Russia's 'ambiguous warfare' tactics," *Reuters*, November 27, 2014, https://www.reuters.com/article/us-russia-nato-security/west-struggles-with-russias-ambiguous-warfare-tactics-idUSKCN0JB0BU20141127. A prominent example of Russia's ambiguous warfare tactics that facilitated plausible deniability is the implementation of "Little Green Men," deployed to Crimea and Eastern Ukraine in 2014. These Russian assets either wore uniforms without insignia or plainclothes.
72. The Stuxnet attack (discovered in 2010) against the Iranian nuclear centrifuges is a classic example. While there are many reports attributing this highly successful attack to some combination of the US and Israel, today, nearly twelve years later, no one knows for sure who did what. Indeed, Iranians for many months, mistaking destroyed centrifuges as normal attrition of equipment, did not even know Iran had been attacked.
73. Editorial Board, "Biden said we'd 'find out.'"
74. David Sanger, *The New York Times*, July 13, 2021, https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html.
75. Senator Angus King and Representative Mike Gallagher, *United States of America Cyberspace Solarium Commission*, March 2020, 1, https://www.solarium.gov/report. The three ways to achieve the stated end state of reducing the probability and impact of cyber-attacks of significant consequence are (1) shape behavior, (2) deny benefits, and (3) impose costs. The first way relies on US collaboration with allies and partners, the second relies on US collaboration with the private sector, and the third relies on military cyber force projection as outlined in the defend forward strategy. Each of the three ways involves a separate deterrent layer, aiming to increase American cybersecurity by altering adversaries' cost/benefit analysis in choosing to engage in cyber-attacks.
76. Ibid., 23-24. This report explains how a layered cyber deterrence "increase(s) the costs and decrease(s) the benefits that adversaries anticipate when planning cyber-attacks against American interests."
77. *Cyberspace Solarium Commission*, 25.
78. Ibid., 24.
79. Ibid., 25.
80. General Inglis created the excellent "layered cyber deterrence" chart in the text above for his service academy classrooms, which also was used for the same purpose by the Cyberspace Solarium Commission; see also Ibid.
81. *2018 Department of Defense Cyber Strategy*, 2.

NOTES

82. "Russia Isn't Listening," *The Washington Post*, Sunday, May 30, 2021, http://thewashingtonpost.newspaperdirect.com/epaper/viewer.aspx.
83. Fontes, "Jack Voltaic," 45.
84. Ibid., 6.
85. Ibid., 16.
86. Ibid.
87. Alan Suderman, "Global war on ransomware? Hurdles hinder U.S. response,"*Associated Press,* June 5, 2021, https://apnews.com/article/europe-hacking-health-coronavirus-pandemic-technology-5d69e46750abd3b40fc9adf395869c7d. As it relates to Russia, the US could also penalize companies that provided "bullet proof" hosting services in Russia (and elsewhere) for these attackers through what is known as the IaaS executive order (currently unused). Furthermore, US companies could be barred from using Russia-based cloud service providers until Russia takes ransomware criminals more seriously; see also, U.S. President, "Executive Order 13984 of January 19, 2021, Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.
88. Aruna Viswanatha and Dustin Volz, "FBI Director Compares Ransomware Challenge to 9/11," *Wall Street Journal,* June 4, 2021, https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003.
89. Evan Perez, Zachary Cohen, and Alex Marquardt, "First on *CNN*: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers," CNN, June 8, 2021, https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html.
90. Monroe, "The Go-Between," 28.
91. Ibid.
92. Ibid. The authors believe that, to ensure victimized businesses remain committed to devoting resources needed to stay ahead of cyber criminals, USG reimbursement must cover only part, not all, of the losses caused by an attack.
93. Testimony of Joseph Blount.
94. Eyder Peralta, "In Wake of Massive Data Breach, Target CEO Steps Down," *NPR*, May 5, 2014, https://www.npr.org/sections/thetwo-way/2014/05/05/309723454/in-wake-of-massive-data-breach-target-ceo-steps-down.
95. Emily Glazer, "J.P. Morgan's Cyber Attack: How the Bank Responded," *Wall Street Journal,* October 3, 2014, https://www.wsj.com/articles/BL-MBB-27792.
96. Scott A. Schipma and Paul F. McQuade, "Executive Order on Improving Nation's Cybersecurity: An Ambitious and Timely Call for a Broad Range of Cybersecurity Improvements," Greenberg Traurig, LLP, May 24, 2021, https://www.gtlaw.com/en/insights/2021/5/executive-order-improving-us-cybersecurity-ambitious-timely-call-cybersecurity#main-content.
97. Brad D. Williams, "DHS Cyber Order Signals Shift to 'Mandatory Measures," *Breaking Defense*, May 27, 2021, https://breakingdefense.com/2021/05/dhs-cyber-order-signals-shift-to-mandatory-reporting/.
98. Brad D. Williams, "Mandatory Cyber Reporting Within 24 Hours: Sen. Warner Bill," *Breaking Defense,* June 21, 2021, https://breakingdefense.com/2021/06/mandatory-cyber-incident-reporting-within-24-hours-sen-warner-bill/.
99. Ibid.
100. Ibid.
101. Thomas Brewster, "$12 Billion Government Contractor Booz Allen Facilitates Ransomware Payments Even Though the FBI Says Never Pay," *Forbes*, June 28, 2021, https://www.forbes.com/sites/thomasbrewster/2021/06/25/major-government-contractor-booz-allen-helps-cyber-victims-pay-ransoms---exactly-the-opposite-of-us-policy/?sh=687730984ced. Colonial Pipeline has yet to make any comment about pertinent details discussed in this Forbes article, neither on the ransom nor on its recovery.
102. One of innumerable examples is the USG in WWII tapping private industry to build tanks; see David Vergun, "During WWII, Industries Transitioned From Peacetime to Wartime Production," *DOD News,* March 27, 2020, https://www.defense.gov/Explore/Features/story/Article/2128446/during-wwii-industries-transitioned-from-peacetime-to-wartime-production/. Another example was the emergency production in 1991 of engines by Detroit Diesel under Roger Penske's leadership during the Gulf War. See Joseph Siano, "AUTO RACING: The Penske Machine Is Rolling Right Along," *The New York Times*, May 31, 1994, https://www.nytimes.com/1994/05/31/sports/auto-racing-the-penske-machine-is-rolling-right-along.html, which recounts Penske's response to an urgent "ask" by General Norman Schwarzkopf.