Conventional Retaliation and Cyber Attacks

Sarah Chen
Dr. Jennifer Taw

INTRODUCTION

On July 27, 2021, President Joe Biden warned, in a speech at the Office of Director of National Intelligence, that "I think it's more than likely we're going to end up, if we end up in a war - a real shooting war with a major power - it's going to be as a consequence of a cyber breach of great consequence and it's increasing exponentially, the capabilities."[1]

Most analysts view the president's hypothetical scenario as unlikely for two reasons. First, attributing cyberattacks is often challenging, making retaliation difficult, if not impossible. Cyberattacks are commonly anonymous, hard to trace, and may be triggered long after they were set up. Moreover, they are often carried out not by states but by criminal entities, hacker groups, or other non-state actors, which sometimes but not always are affiliated with or sponsored by states. The practical and political window for overt retaliation closes if a cyberattack cannot be directly and timely attributed to a state. Second, and importantly, most cyberattacks do not have strategic effects. The preponderance of cyberattacks are either distributed denial-of-service (DDOS) attacks (meant to disrupt, blackmail, or extort), or they are efforts to collect information through a combination of hacking and malware. Even attacks attributable to a state usually fall below the threshold for conventional retaliation.

Yet we explain here why improvements in attribution capabilities, combined with cyberattacks' increasing potential to kill people, threaten military readiness, and wreak economic destruction are making it more likely that a cyberattack will trigger a conventional response. This is significant because, as foreseen by President Biden, it means that a cyberattack could be not only an element of war but a precipitating act of war.

Sarah Chen is a Rhodes Scholar pursuing a MSc in Social Science of the Internet at Oxford. She recently graduated from Claremont McKenna College with a dual degree in International Relations and Philosophy, Politics, and Economics. Her academic interest area is in cyberspace conflict and wargaming. During her undergraduate years, she worked on games with the Center for Naval Analyses, the Gould Center for Humanistic Studies, and the Office of the Director of National Intelligence.

This article summarizes how some states already anticipate this possibility, and reviews the conventional wisdom on the relationship among cyberattacks, retaliation, and escalation, with special attention to attribution. We then show accurate attribution is easier now, and that cyberattacks with strategic impact are somewhat more likely. We conclude with recommendations for considering this new level of cyber conflict.

STATES ANTICIPATE STRATEGIC CYBERATTACKS

Article 51 of the UN Charter allows the use of force "only in response to a certain kind of attacking force, specifically, an 'armed attack.'"[2] With respect to this, however, legal experts rely on effects-based analysis more than a definition-based one, looking at the "violent consequences of an attack which does not consist of the use of kinetic force" to determine whether it is equivalent to an armed attack.[3] A cyberattack that causes deaths or significant strategic outcomes - that, in effect, has an outcome equivalent to a conventional armed attack - arguably meets this standard.

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, published in 2017, is intended to assist in applying international law when interpreting cyber actions and developing appropriate responses. The manual, relied on by multiple individual states' doctrines on cyberspace, states that use of force, while generally forbidden, can be appropriate and justified in self-defense, depending on the context. The manual offers a framework for judging a cyberattack that includes the following criteria: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, presumptive legality.[4]

Many states have begun to identify circumstances appropriate for response to a cyberattack with non-cyber retaliation. Since 2011, US leaders, for example, have reserved the right to respond to hostile acts in cyberspace with "all necessary means – diplomatic, informational, military, and economic" although the US will "exhaust all options before military force whenever [it] can."[5] In a 2015 hearing, then-Deputy Secretary of Defense Robert Work stated that the US "reserves the right to respond to malicious cyber activity at a time, place, and manner of its choosing."[6]

In the German federal government's March 2021 position paper, "On the Application of International Law in Cyberspace," officials note the potential of cyberattacks with kinetic outcomes severe enough to trigger responses under international law. Cyber operations could "constitute an armed attack whenever they are comparable to a traditional kinetic armed attack in scale and effect."[7] German government officials lay out four response possibilities: retorsion, countermeasures, measures taken based on necessity, and self-defense. With self-defense, states can "resort to all necessary and proportionate means in order to end the attack" when a cyberattack is comparable to an armed attack. They also state that "there is no general obligation under international law as it currently stands to publicize a decision on attribution and to provide or to submit for public scrutiny detailed evidence on which an attribution is based."[8] That is not to say that accusations should not be substantiated, however, the German report concludes that the state should have discretion whether to publicize attribution.[9]

The French government, in its cyber operations declaration, reserves the right to respond to cyberattacks and provides criteria for assessing whether or not a cyber operation is comparable to an armed attack: substantial loss of life, physical or economic damage, impact on critical infrastructure, number of victims, technological or ecological catastrophe.[10] The French add that, even if one cyberattack falls short of reaching a certain threshold of damage, multiple attacks and their effects can be aggregated (for instance, if an attack cripples electronic infrastructure in one area of the country and a different attack, sponsored by an actor working in conjunction with the first, damages water supply access in another

Jennifer Morrison Taw is Associate Professor of Government and International Relations at Claremont McKenna College, where she teaches International Relations, Security Studies, War, and U.S. Foreign Policy. Her publications include Mission Revolution: The U.S. Military and Stability Operations (Columbia University Press, 2012); "Preventive Force: The Logic of Costs and Benefits," Chapter 2 in Fisk, et. al, Preventive Force: Drones, Targeted Killing, and the Transformation of Contemporary Warfare (New York University Press, 2016); and "Colombia: A Case Study," chapter in Fair, et. al, Policing Insurgencies: Cops as Counterinsurgents (Oxford University Press, 2014). Taw is also coauthor of World Politics in a New Era, 6th edition, with Spiegel, et al., (Oxford University Press, 2014). Prior to teaching, Jennifer worked for ten years at RAND, where she focused on counterinsurgency, counterterrorism, peace operations, and special operations forces.

area jointly impacting a large number of citizens). Self-defense from such attack(s) can include conventional force and can also be preemptive. Like Germany, France prefers that each state decide if and when to share public attribution, and also what evidence is needed to support an accusation, and underscores that absence of public attribution is not necessary to justify a state's response to a cyberattack.[11]

While it has similar self-defense guidelines, the Netherlands categorizes attribution as technical, political, or legal, wherein states need only to disclose evidence for legal issues when an attacking state violates international law.[12] Dutch policy also holds that, if self-defense is required, there must be adequate and convincing proof of the actor's guilt and states must still meet requirements of necessity and proportionality: "the intention is to end the attack, the measures do not exceed that objective and there are no viable alternatives. The proportionality requirement rules out measures that harbor the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future."[13]

NATO Secretary-General Jens Stoltenberg wrote in 2019 that "a serious cyberattack could trigger Article 5 of our founding treaty" that triggers the collective defense agreement, placing cyberattacks in the same domain as any physical attack.[14] Stoltenberg cited the 2017 WannaCry virus's effect in the United Kingdom as an example of a major cyberattack: ransomware that shut down multiple hospitals and cost over £90 million.[15] Article 5 specifies that if an "armed attack" occurs against a NATO ally, then each member will assist the ally with "such actions as it deems necessary, including the use of armed force."[16] While Article 5 has yet to be triggered by a cyberattack, and while there is no consensus on the definition of the term 'armed' cyberattack, a kinetic response to a cyberattack—backed by a multilateral alliance—seems clearly possible. Eneken Tikk, a research lawyer at the Cyber Policy Institute, observes, however, that Article 5 poses a high threshold, for example, attacking critical infrastructure with effect comparable to an armed attack; below this threshold, he observes that even an attack resulting in casualties may not qualify.[17]

In 2010, anticipating this debate in NATO, Mark Rasch, former head of the U.S. Justice Department's computer crimes unit, suggested that Article 5's chief purpose is "to act as a massive deterrent…by establishing the rules of cyber war engagement, NATO is 'throwing down the gauntlet'."[18] Yet NATO eleven years later openly affirmed that cyberattacks could trigger Article 5, reiterating this in the response to the Russia-Ukraine conflict, and further declared that "the Alliance is determined to employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law."[19] NATO made the case that "ransomware incidents and other malicious cyber activity targeting our critical infrastructure and democratic institutions… might have systemic effects and cause significant harm."[20]

This brief review of NATO's and NATO members' anticipation of strategic cyberattacks demonstrates the seriousness with which many major military powers are planning for such eventualities, and considering circumstances that would justify conventional responses. Notably, such policies and deliberations serve not only to prepare and plan for strategic cyberattacks, but also to deter against them by forewarning a conventional response to certain types of attacks, based on the targeted victim, and the level of impact.

LITERATURE REVIEW

In 2012, Thomas Rid published his article "Cyber War Will Not Take Place,"[21] and defined an act of war as being instrumental and political, with the potential to be lethal. He argued that, given that most cyberattacks were primarily acts of sabotage, espionage, or subversion, they were "tactical in nature" and only rarely might "have operational or even strategic effects."[22] Rid further observed that not a single cyberattack had met all three criteria.[23] A year later, John Stone responded with his own article, "Cyber War Will Take Place!" Stone wrote that "cyber war is possible in the sense that cyberattacks could constitute acts of war." Stone recognized, long before the crippling effects of large-scale attacks like NotPetya, that the application of force for an act of war "can break things, rather than kill people, and still fall under the rubric of war."[24]

More in keeping with Rid than with Stone, Martin Libicki in 2020 wrote "Correlations Between Cyberspace Attacks and Kinetic Attacks," in which he drew several conclusions: "a kinetic retaliation to a cyberattack is possible but cannot yet be deemed a likely consequence" and "rarely do events in cyberspace – much less escalation in cyberspace – lead to serious responses at all."[25] He continued, "while there could be cyberattacks consequential enough to induce echoes in the physical world, none have reached that threshold and it may well be that none could reach that threshold."[26]

In both theory and practice, the most common response to a cyberattack is also cyber, whether as defense or retaliation. Interestingly, even in this context, the expectation is that a cyberattack will be met with an equivalent response, rather than escalation. There are practical reasons for this, but it is also related to policymakers' and the public's perceptions. Jacqueline Schneider analyzed the Deterrence and Escalation Game in Review (annually conducted (2011-2016) with US foreign policy decision makers), concluding that decision makers "curtail their own use of cyber operations for fear of escalation, while not responding to similar adversary actions in cyberspace."[27] Similarly, Benjamin Jensen and Brandon Valeriano in 2017 looked at whether or not cyber operations resulted in a desire for an escalatory response.[28] US, Russian, and Israeli participants in a simulation and survey experiment were assigned to four groups and presented with a triggering incident (half had a cyber-based incident and half did not) and given the ability to respond (half were given the option of a cyber response and half were not). Jensen and Valeriano found that all three nationalities "preferred de-escalation more than escalation even when they had cyber options with which to respond. Escalation was not the norm."[29] Respondents across all four scenarios opted 40-50% for de-escalation, 30-50% for a proportional response, and less than 10% of advocated escalation.[30]

When retaliation to a cyberattack is going to occur, however, Aaron Brantly lists certain requirements for success: the state must identify the perpetrator, retaliate in a timely and proportionate manner, and employ a cyberweapon tailored for the specific target.[31] Timeliness is important because perpetrators expecting a delayed response may assume that "the risk of punishment for an attack is ... so temporally distant as to be discounted to the point of irrelevance."[32] Avoiding escalation renders proportionality critically important. Specificity and prompt response prevent "bleed" or "escape" by preventing a cyberweapon like malware or a virus from hopping to unintended servers or sectors.

This logic presumes that assured proportionate response will deter cyberattacks. Whether this is true is complicated by the aforementioned challenges of attribution. Unlike kinetic weapons and military movements, which are physical and often overt actions, cyberattacks are invisible and can remain undetected, and their effects may be attributed to other causes. When they *are* recognized as cyberattacks, it may be hard to trace their perpetrators or even to identify their scope. As Charles Glaser notes, cyberattacks are inherently covert,[33] requiring secrecy to increase success, reliant on finding vulnerabilities and 'zero-day' exploits.

These characteristics often muddle attribution. For instance, an attack could originate from servers in a state without that state's awareness; a non-state organization might utilize the servers or another actor could route through them.[34] In "Crisis and Escalation in Cyberspace," Martin Libicki describes how a state can plausibly deny responsibility for a cyberattack traced to its territory, claiming it was a non-state actor or a false-flag operation.[35] Without surety, a state victim of a cyberattack cannot retaliate, rendering perpetrators non-deterrable, thinking they can cover their tracks. Former U.S. Deputy Secretary of Defense Bill Lynn noted that traditional deterrence models are less effective in cyberspace due to the difficulty in identifying attackers; he holds deterrence must instead "be based more on denying any benefit to attackers than on imposing costs through retaliation."[36]

In "Cyber Deterrence," Jonathan Welburn, Justin Grana, and Karen Schwindt suggest, to the contrary, that deterrence can be effective if the defender signals – without specificity – that it has the cyber capacity to defend/retaliate against a cyberattack. In their model, Welburn et.al assume that: "1. The defender can only imperfectly attribute attacks. 2. The attacker has uncertainty over the defender's retaliatory and defensive capability. 3. The defender can signal its capability not by revealing its true capability, but through costless and unverifiable cheap talk."[37] The authors map out this model utilizing game theory and show that "it is never in the best interest of the defender to perfectly signal its retaliation capability."[38] However, if it can convince the attacker that it is signaling a strong, true capability without revealing its actual hand, this increases deterrence. Welburn et. al. also propose a model of "anti-deterrence," incentivizing an attacker to attack when the defending state has heightened readiness and in such a way that the attacker tips its hand, increasing the likelihood of correct attribution.[39] Their conceptualization of deterrence in a cyber context highlights the differences from classic deterrence: in the cyber realm, they suggest, states must coopt uncertainty, signaling indirectly, vaguely, and without technical proof.

Considering the foregoing, it might seem unlikely that a cyberattack could be expected to trigger a conventional response. But some of the conditions have changed since these analyses were conducted. As will be discussed, attribution technology and capabilities are improving, thus facilitating retaliation and, of course, deterrence, by obviating the comfort perpetrators may have that they will not be identified. Secondly, while the preponderance of cyberattacks remains tactical, the potential for strategic cyberattacks is increasing and it is, therefore, worthwhile to consider when a cyberattack could become a precipitating cause of war.

Stone and Rid classify a cyberattack as an act of war if it corresponds to a strategic economic attack, a strategic military attack, or a lethal civilian attack, thus potentially justifying a conventional response. While in their 2018 article "Determinants of the Cyber Ladder," Nadiya Kostyuk, Scott Powell, and Matt Skach saw cyber capabilities as unready to deal an existential blow to a major power,[40] they offered a useful escalation ladder for conceiving of the requirements of doing so. In their model, an act of war would involve a "major damaging attack – targeted military interference and overt disabling and/or destruction of military targets or infrastructure; catastrophic attacks – permanent damage to civilian infrastructure (mass destruction of critical data, infrastructure control, software, banking infrastructure); and existential attacks" equivalent to "limited contingency operations, major military operations, and nuclear war."[41] The range of attacks that could spark a conventional response short of war will likely be broader.

In short, the literature suggests that a conventional response to a cyberattack will only occur if the attribution challenge is resolved and if the cyberattack deals a strategic blow leading to severe military or economic damage or to civilian deaths (above a certain threshold, if Tikk is correct) – while casting some doubt that a nation would choose to escalate to that threshold.

ATTRIBUTION AND IMPACT

Attribution

Attribution techniques are becoming more accurate and rapid. Attribution occurs on multiple levels of granularity: assigning attacks to a group, country of origin, and identification of specific groups or people. The second level is the country of origin – the level required for state-level retaliation, and "the most common level of attribution"; about 85% of the 130 identified groups in public analysis reports are linked with a country.[43] Timo Steffens in "Attribution of Advanced Persistent Threats," breaks down the initial phases of the attribution processes: data collection and clustering, which both have seen technical improvements in recent years.[44] Resources like the Common Vulnerability Exposure dictionary and the YARA pattern-matching malware tool are widely used to create a common ground for compiling and sharing information on previous attacks.[45]

Artificial intelligence (AI) tools and machine learning are also advancing attribution. AI can analyze massive amounts of attack data to find patterns and similarities for actor identification.[46] The Department of Defense sponsored Rhamnousia, an algorithmic methodology that attempts to change manual attribution, which can takes weeks and months, into machine learning programs.[47] A cyber threat attribution framework can use a machine learning model, trained off publicly available cyber threat intelligence reports, to recognize attack patterns with about 50% higher precision than other publicly available profiles.[48] Another such model, developed on the Amazon Web Services Honeypot dataset, exceeded 95% accuracy.[49]

Public-private sector sharing and cooperation regarding information on vulnerabilities and actors has improved, both through formal and informal mechanisms. State-level attribution can be initiated by private security firms first identifying and investigating the issue, creating a collective knowledge base, and then building into a private-public effort for attribution.[50] The US introduced the Cyber Threat Framework to create a consistent common language for cyber threat activity sharing, across models and observations.[51] The Cybersecurity and Infrastructure Security Agency (CISA) also has networks for information sharing, and a recent bill, the Cyber Incident Reporting for Critical Infrastructure Act signed in March 2022, creates obligations for private sector reporting.[52]

Many cyberattacks in the three years ending in 2020 were publicly attributed, with improvements to digital forensics.[53] In an analysis of the Council on Foreign Relations (CFR) dataset of state-sponsored cyber incidents from 2014-2018, Mueller, et al., found that out of eighty-two incidents, 85% were publicly attributed to a government, private actor, or both.[54] CFR reported seventy-six operations in 2019 that were confirmed or suspected to have been state-sponsored, 77% of which were attributed to China, Russia, Iran, or North Korea,[55] and one hundred nineteen such incidents in 2020.[56] Some of the largest hacks that occurred within the last year: Solarwinds – malicious code that affected US government infrastructure,[57] Colonial Pipeline – a ransomware-triggered shutdown of a large oil pipeline,[58] JBS – ransomware attack against a global meat processing company,[59] and Kaseya – another ransomware attack that affected hundreds of supply chains,[60] were all state-sponsored or attributed by link within weeks or months of discovery. The US was also able to quickly attribute cyberattacks against Ukraine to Russia, showcasing an improved attribution arsenal.[61]

The Dyadic Cyber Incident and Campaign Database (DCID), which publishes known cyber incidents between rival dyads from 2000-2020, tracked 429 incidents that have steadily increased in severity of impact and volume annually, which suggests more attacks or improved attribution, or both, for cyber incidents.[62] The average severity has risen from most attacks being classified as a level three in impact, “stealing targeted critical information from one network” to level four, “widespread government, economic, military, or critical private-sector network intrusion, multiple networks.”[63] In short, in the past few years, most of the large-scale cyberattacks that approach the conditions for triggering a conventional response have been directly attributed to specific hacker groups and, in some instances, to states or state sponsors, which suggests some combination of better attribution methods and greater public-private cooperation for attack response and analysis, and faster attribution to adversarial cyber nation-states.

Impact

Civilian Deaths

In 2020, the first reported 'direct' cyberattack death occurred: misdirected ransomware targeting Heinrich Heine University hit a hospital in Düsseldorf, Germany instead, resulting in a patient dying before reaching an alternative hospital. The attacker withdrew its extortion demand and sent a decryption key upon discovering the error, to no avail.[64] This death was accidental, but confirms that cyberattacks can kill. More recently deaths have resulted from cyberattacks on power grids in Ukraine, and crippled hospital infrastructure in the United Kingdom (UK) and the US, but none of these events led to an escalatory response from the targeted countries.[65] So far at least, it appears a deadly cyberattack will not lead to a conventional response unless it was deliberately undertaken by a state or non-state violent actor and kills a certain threshold number.

The link between retaliation and deaths relates in part to public perception and political expectations. Sarah Kreps and Debak Das found in 2017 that US public support for a retaliatory air-strike increased by about 32% when a cyberattack causes casualties beyond economic injury.[66] A 2021 multi-country study by Ryan Schandler, Michael Gross, Sophia Backhaus, and Daphna Canetti likewise found that only lethal terrorist cyberattacks led to public expectations of military retaliation. By running randomized survey experiments with UK, US, and Israel civilians, Schandler, et al, identified a "lethality threshold for cyber terrorism effects, wherein the outcome of the attack must meet a minimum level of destruction in order to produce national responses equivalent to those for conventional terrorism."[67] The researchers found that, considering lethal and non-lethal conventional terrorist attacks and lethal and non-lethal cyberterrorist attacks, conventional attacks and cyberattacks with fatalities were more likely to engender demands for retaliation. Building on Kreps' and Schneiders' 2019 work, in which the researchers found that "individuals are far more reluctant to escalate in the cyber domain than for corresponding conventional or nuclear attacks," Shandler, et al, concluded from their own experiment that the public would expect retaliation for attacks causing at least seven deaths.[68]

Destruction of Military Capabilities

Cyberattacks can trigger kinetic effects that reduce the military's capabilities. In 2007, Idaho National Laboratory researchers found that from a remote location, with just thirty lines of code, they could blow a diesel generator attached to an electrical grid.[69] Damage in this instance was machine alone, but overpowering an electrical grid at a military base and causing permanent kinetic damage or even injury to soldiers can be viewed as acts of war.

As important as kinetic outcomes from cyberattacks, and more likely, are cyberattacks' destruction of elements of the military's technical ability. Non-kinetic attacks, such as disablement of weapon systems' command-and-control, drone hacking or corruption of targeting systems, or even damage to satellite and surveillance ability, can seriously undermine military operations. Even without any direct loss of life or kinetic damage, they can directly interfere with a nation's ability to defend itself or achieve military objectives.

A Microsoft report that tracked the first few weeks of the Russia-Ukraine war, from February 23 to April 8, observed "nearly 40 discrete destructive attacks that permanently destroyed files," with over 40% targeting "critical infrastructure sectors that could have negative second-order effects on the government, military, economy, and people."[70] A stand-out hack was the targeting of Viasat, a US satellite company, which wiped data and destroyed thousands of terminals, effectively crippling Ukraine's military communications, characterized as "the most concerted effort to disable Ukrainian military capabilities."[71]

Yet Russian cyber-attacks on military targets were limited to information compromise, such as Dev-0257 and STRONTIUM – phishing campaigns against government and military employees.[72] The Microsoft report found that there were "several attacks that appeared to show parallel cyber activity and ground activity."[73] For instance, Russia targeted government buildings in Dnipro with strikes on the same day an agency located there suffered a major malware attack.[74] This generally falls within the guidelines of current literature that suggests the destruction of military capabilities for now remains primarily within conventional weapon alternatives and cyberattacks will remain supportive.[75]

Despite the lack of current evidence of cyberattacks directed to disrupt or disable military capabilities, the technical vulnerability to and consequences of such attacks are concerning. The Department of Defense (DoD) "routinely found mission-critical cyber vulnerabilities" in developing systems.[76] Russia jammed GPS signals during the NATO exercise, Trident Juncture, in 2018. These attacks, while temporary, threatened loss of intelligence, surveillance, and reconnaissance functionality if ever later conducted on a larger scale.[77] An attack that interfered with military capabilities could lead to retaliation as a consequence of interference or out of the defending state's worry that it is a precursor for follow-on action, as seen in the Russian preemptive cyberattacks on Ukraine. Although strategic cyber operations cannot "hold ground… gain or reclaim it," when they threaten conventional capabilities to do so, they could spark conventional retaliation.[78]

Economic and Infrastructural Damage

President Biden in his June 16, 2021 meeting with President Putin listed sixteen critical infrastructure sectors that "should be off-limits to attack, period, by cyber or any other means."[79] A senior official noted that these sectors are those that fall under the auspices of CISA: chemical infrastructure, commercial facilities, communications infrastructure, critical manufacturing, dams, the defense industrial base, emergency services, the energy industry, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors (including both materials, and waste), the transportation sector, and water and wastewater.[80] During the Russia-Ukraine conflict, Biden has stated that "If Russia pursues cyberattacks against our companies, our critical infrastructure, we are prepared to respond."[81] However, he has not stated the consequences of such attacks.

Direct damage that equates to an armed attack could result from cyberattacks on critical infrastructure. Hijacking and crashing vehicles, poisoning water supplies, flooding dams, or cutting off hospital functionality, for example, are acts that would be considered terrorism and hence qualify as acts of war. In 2017, the Department of Homeland Security ran an experiment where a team succeeded in remotely hacking into a Boeing 757.[82] While there have been no such large-scale attacks on critical infrastructure, a July 2021 attack by Russian-linked REvil, a ransomware-as-a-service criminal group, on Kaseya, a Dublin- and US-based company that develops computer software for business-networking, affected 800-1500 businesses' downstream supply chains.[83]

Although the US has not experienced a direct, crippling economic or critical infrastructure attack, the past two years have seen several large incidents globally; civilian infrastructure is not 'off-limits' for cyber conflict. Colonial Pipeline and JBS, while causing international concern, both resulted in a temporary halt in supply-chain operations due to ransomware disablement, rather than destruction.[84] It is unclear whether Colonial Pipeline was operationally affected, given that the company chose to internally shut down operations while investigating the attack, and the JBS shutdown resulted in less than a day's loss of output.[85]

However, other attacks have been more deliberately focused on damaging infrastructure, rather than monetary gain. On April 23, 2020, the Israeli National Cyber Directorate alerted energy and water companies that there were "intrusion attempts at wastewater treatment plants, water pumping stations, and sewers."[86] The attack was linked to the Jerusalem Electronic Army, an affiliate of the Gaza Cybergang, an Arab-speaking group believed to be working from Palestine. Western intelligence sources allege that hackers attempted to alter water chlorine levels, and nearly succeeded.[87] Yigal Unna, head of the National Cyber Directorate, noted that if the attack had not been detected in real time, the consequences could have been "harmful and disastrous" if chemicals were mixed into the water.[88] The hack also could have triggered a fail-safe and shut down water sources during an on-going heat wave.[89]

Iran's Shahid Rajaee port terminal was knocked out on May 9, 2021, causing long line-ups of vessels stuck in and outside the harbor. The computer system was off-line "briefly," but the lasting traffic build-up caused miles-long jams around the port that took days to clear. One official called the situation "total disarray," claiming that Iranian official media understated the damage.[90] Two months later, a cyberattack on Iran's railroad systems and Iran's transport and urbanization ministry website caused delays and cancellations of hundreds of trains as false information was reported on display boards and the electronic train tracking system failed.[91] On July 22, 2021, Transnet SOC Ltd., a ports and freight-rail company responsible for over 60% of South Africa's shipments, experienced an "act of cyberattack, security intrusion, and sabotage" and declared a force majeure five days later with four harbors disrupted: Durban, Ngqura, Port Elizabeth, and Cape Town. The force majeure lasted for 11 days, with port operations systems, websites, and digital communication down, causing delays and bottlenecks.[92] Port issues ricocheted into importers and exporters of manufactured and agricultural goods, and experts predicted a high economic toll during an already unstable time for South Africa.[93] In April, Ukraine revealed that it had narrowly withstood a planned Russian attempt to shut down its power grid, with a potential blackout threatening two million citizens.[94]

Parallels in the US could have consequences reaching the threshold of cyber terrorism with secondary lethal effects. In a 2022 discussion on "Strengthening the Cybersecurity of American Water Utilities," Samantha Ravich, chair of the Center on Cyber and Technology Innovation, stated that "water may be the greatest vulnerability in our national infrastructure.... [E]ach of these [52,000 drinking water and 16,000 water waste] systems operates in a unique threat environment."[95] A mid-2021 publication confirmed three recent attempted US-based hacks of water facilities.[96] A large port shut-down in the vein of the Shahid Rajaee or Transnet SOC attacks would cost billions; a supply-chain congestion outside the Los Angeles and Long Beach ports left over twenty billion dollars' worth of goods stranded outside the docking area for days.[97] A hypothetical attack on the Northeast US power grid, affecting 15 states, would cost anywhere from 243 billion to a trillion dollars.[98] The Colonial Pipeline attack and the JBS attack cost about five and 11 million dollars, respectively, in ransom costs, with no publicly announced cost of the business disruption.[99] However, the scale of these attacks was limited to a short-term concern given the rapid recovery.

The Center for Strategic and International Studies, an American thinktank, compiles a worldwide rolling list of significant cyber incidents that focuses on "cyberattacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars."[100] They list 131 such incidents in 2020, thirteen of which had kinetic effects on critical infrastructure, over 100 in 2021, and 118 as of December 18, 2022.[101]

Without defining the threshold, the Biden administration has publicly floated the possibility of a US military response to cyberattacks, saying "we are not taking anything off the table as we think about possible repercussions, consequences, or retaliation."[102] Likewise, other countries are experiencing emerging thoughts regarding conventional responses to cyberattacks, and there is a growing global realization that cyber and/or political retaliation may not continue to suffice to counter severe cyber incidents.

CONCLUSION

Overall, the fast-evolving relationship between cyber conflict and the threshold for conventional warfare demands more attention. Libicki in 2020 correctly noted that there had not yet been a conventional response to a cyberattack, and that remains true today. But some states are realizing it is not too soon to develop norms, given the recent growth of serious incidents and the targeting of critical and civilian infrastructure. Cyberattacks increasingly are imposing significant costs on countries. Without effective deterrence mechanisms, the frequency and intensity of attacks will continue to grow. Public conservativism regarding responses cannot be expected to hold in the aftermath of a massive attack or significant loss of life. With military and infrastructure vulnerabilities, the boldness of state-sponsored cyberattacks, and more timely investigations, the US must prepare to respond to unprecedented cyber incidents or to aid allies in an invocation of Article 5.

While publicly stating thresholds of cyberattacks may be marginally useful, the NATO Secretary General has correctly observed that NATO never grants adversaries the privilege of knowing specifics on what will trigger Article 5. More consideration needs to be given regarding mutual, multi-lateral understanding of cyber conflict red lines.[103] This paper focuses on conditions that could justify conventional retaliation to cyberattacks, but future work is needed to address specifics regarding targets and responses. There may be different cost thresholds, for instance, for private sector attacks on civilian infrastructure than for state-sponsored infrastructure. A conventional retaliation can also take many forms depending on the target and impact; a retaliation for the degradation of missile launch capabilities may look different from that for civilian deaths from water shutdowns.

If cyberattacks meet the retaliation threshold - resulting in loss of life, degraded military ability, and/or strategic economic damage – and if sanctions and cyber counterattacks are deemed inadequate, a conventional retaliation may be reasonable and even necessary, especially if accurate attribution ceases to be a serious challenge.

NOTES

1. Nandita Bose, "Biden: If U.S. Has 'real Shooting War' It Could Be Result of Cyber Attacks," *Reuters*, July 28, 2021, sec. World, https://www.reuters.com/world/biden-warns-cyberattacks-could-lead-a-real-shooting-war-2021-07-27/.
2. Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* 5, no. 1 (2011): 85.
3. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar"; see also David Graham, "Cyber Threats and the Law of War - Journal of National Security Law & Policy," *Journal of National Security Law* 4, no. 1 (2010): 91.
4. Michael Schmitt, ed., "The Use of Force," in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Newport, Rhode Island: Cambridge University Press, 2017).
5. "International Strategy for Cyberspace" (The White House, May 2011).
6. Robert Work, "United States Cybersecurity Policy and Threats Hearing," https://www.govinfo.gov/content/pkg/CHRG-114shrg22270/html/CHRG-114shrg22270.htm.
7. "On the Application of International Law in Cyberspace" (The Federal Government of Germany, March 2021).
8. "On the Application of International Law in Cyberspace."
9. "On the Application of International Law in Cyberspace."
10. Przemyslaw Roguski, "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part II," *Opinio Juris* (blog), September 24, 2019, http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyberoperations-part-ii/; "DROIT INTERNATIONAL APPLIQUÉAUX OPÉRATIONSDANS LE CYBERESPACE" (Ministère Des Armèes, September 2019).
11. Roguski, "France's Declaration on International Law in Cyberspace"; "DROIT INTERNATIONAL APPLIQUÉAUX OPÉRATIONSDANS LE CYBERESPACE."
12. Ministry of Foreign Affairs, "Letter to the Parliament on the International Legal Order in Cyberspace," July 5, 2019.
13. Ministry of Foreign Affairs.
14. Jens Stoltenberg, "Nato Will Defend Itself," Prospect Magazine, August 27, 2019, https://www.prospectmagazine.co.uk/world/nato-will-defend-itself-summit-jens-stoltenberg-cybersecurity.
15. Stoltenberg; Oscar Williams, "The WannaCry Ransomware Attack Left the NHS with a £73m IT Bill," *NS Tech* (blog), October 12, 2018, https://tech.newstatesman.com/security/cost-wannacry-ransomware-attack-nhs.
16. NATO, "Collective Defence - Article 5," NATO, accessed May 20, 2021, http://www.nato.int/cps/en/natohq/topics_110496.htm.
17. Red Tape, "Could Cyber Skirmish Lead U.S. to War?," NBC News, June 11, 2010, http://www.nbcnews.com/business/consumer/could-cyberskirmish-lead-u-s-war-flna6C10406234.
18. Tape.
19. Heads of State and Government participating in the meeting of the North Atlantic Council, "Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021" (North Atlantic Council, June 14, 2021), http://www.nato.int/cps/en/natohq/news_185000.htm; NATO, "Press Conference by NATO Secretary General Jens Stoltenberg Following the Extraordinary Virtual Summit of NATO Heads of State and Government," NATO, February 25, 2022, https://www.nato.int/cps/en/natohq/opinions_192455.htm.
20. Heads of State and Government participating in the meeting of the North Atlantic Council, "Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021."
21. John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (February 1, 2013): 101–8, https://doi.org/10.1080/01402390.2012.730485; Thomas Rid, "Cyber Will Not Take War Place," *Journal of Strategic Studies* 35, no. 1 (February 1, 2012): 5–32, https://doi.org/10.1080/01402390.2011.608939.
22. Rid, "Cyber War Will Not Take Place."
23. Ibid.
24. Stone, "Cyber War Will Take Place!"; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 8, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.
25. Martin C. Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks" (12th International Conference on Cyber Conflict, 2020), 203–11.

NOTES

26. Libicki, 211.
27. Jacquelyn Schneider, "Cyber and Crisis Escalation: Insights from Wargaming" (USASOC Futures Forum, 2017).
28. Benjamin Jensen and Brandon Valeriano, "What Do We Know about Cyber Escalation? Observations from Simulations and Surveys" (Atlantic Council, November 22, 2019), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyberescalation-observations-from-simulations-and-surveys/.
29. Jensen and Valeriano, 12.
30. Jensen and Valeriano, 6.
31. Aaron F. Brantly, "The Cyber Deterrence Problem," in *2018* 10th *International Conference on Cyber Conflict (CyCon)* (2018 10th International Conference on Cyber Conflict (CyCon), Tallinn: IEEE, 2018), 45, https://doi.org/10.23919/CYCON.2018.8405009.
32. Brantly, 45.
33. Charles Glaser, "Deterrence of Cyber attacks and US National Security" (Washington, D.C.: Cyber Security Policy and Research Institute, 2011).
34. Martin C. Libicki, "Crisis and Escalation in Cyberspace," January 3, 2013, https://www.rand.org/pubs/monographs/MG1215.html.
35. Ibid.
36. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy,*" Foreign Affairs* 89, no. 5 (n.d.): 98.
37. Jonathan William Welburn, Justin Grana, and Karen Schwindt, "Cyber Deterrence or: How We Learned to Stop Worrying and Love the Signal," September 4, 2019, 3, https://www.rand.org/pubs/working_papers/WR1294.html.
38. Welburn, Grana, and Schwindt, 3.
39. Welburn, Grana, and Schwindt, 25.
40. Nadiya Kostyuk, Scott Powell, and Matt Skach, "Determinants of the Cyber Escalation Ladder," *The Cyber Defense Review* 3, no. 1 (2018): 128.
41. Kostyuk, Powell, and Skach, 129.
42. Susan G. Straus et al., "Collective Simulation-Based Training in the U.S. Army: User Interface Fidelity, Costs, and Training Effectiveness," Product Page (RAND Corporation, 2019), 34, https://www.rand.org/pubs/research_reports/RR2250.html.
43. Straus et al., 34.
44. Timo Steffens, *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage,* 1st ed. 2020 edition (Berlin Heidelberg: Springer Vieweg, 2020), 38.
45. John S. Davis et al., "Stateless Attribution: Toward International Accountability in Cyberspace" (RAND Corporation, June 2, 2017), 23, https://www.rand.org/pubs/research_reports/RR2081.html; "Welcome to YARA's Documentation! — Yara 4.2.1 Documentation," 2021, https://yara.readthedocs.io/en/latest/.
46. Eric Horvitz, "Applications for Artificial Intelligence in Department of Defense Cyber Missions," Microsoft On the Issues, May 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/.
47. Sally Cole, "Rhamnousia: Framework for Cyberattack Attribution - Military Embedded Systems," Military Embedded Systems, February 14, 2017, http://militaryembedded.com/cyber/cybersecurity/rhamnousia-framework-cyberattack-attribution.
48. Umara Noor et al., "A Machine Learning-Based FinTech Cyber Threat Attribution Framework Using High-Level Indicators of Compromise," *Future Generation Computer Systems* 96 (July 1, 2019): 227–42, https://doi.org/10.1016/j.future.2019.02.013.
49. Maimonah Alkaabi and Sunday O. Olatunji, "Modeling Cyber-Attribution Using Machine Learning Techniques," in *2020 30th International Conference on Computer Theory and Applications (ICCTA),* 2020, 10–15, https://doi.org/10.1109/ICCTA52020.2020.9477672.
50. Davis et al., "Stateless Attribution," 23.
51. Office of the Director of National Intelligence, "Cyber Threat Framework," accessed July 11, 2022, https://www.dni.gov/index.php/cyber-threat-framework.

NOTES

52. CISA, "Information Sharing and Awareness | CISA," February 16, 2022, https://www.cisa.gov/information-sharing-and-awareness; Richard Manfredi, "President Biden Signs into Law the Cyber Incident Reporting for Critical Infrastructure Act, Expanding Cyber Reporting Obligations for a Wide Range of Public and Private Entities," *Gibson Dunn* (blog), March 22, 2022, https://www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/.
53. Sanjay Goel, "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race," *Connections* 19, no. 1 (2020): 87–95.
54. Milton Mueller et al., "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?," *The Cyber Defense Review* 4, no. 1 (2019): 107–22.
55. "Tracking State-Sponsored Cyberattacks Around the World," Council on Foreign Relations, 2020 2005, https://www.cfr.org/cyberoperations.
56. Ibid.
57. Christopher Bing, "Exclusive: Wide-Ranging SolarWinds Probe Sparks Fear in Corporate America | Reuters," *Reuters*, September 10, 2021, https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10/.
58. Scott Jasper, "Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack," *Atlantic Council* (blog), June 1, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/.
59. The Associated Press, "REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says," NPR, June 3, 2021, sec. Business, https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says.
60. Charlie Osborne, "Updated Kaseya Ransomware Attack FAQ: What We Know Now," ZDNet, July 23, 2021, https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/; Kari Paul, "Who's behind the Kaseya Ransomware Attack – and Why Is It so Dangerous?," *The Guardian*, July 7, 2021, https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers.
61. Patrick O'Niell, "The US Is Unmasking Russian Hackers Faster than Ever," MIT Technology Review, February 21, 2022, https://www.technologyreview.com/2022/02/21/1046087/russian-hackers-ukraine/.
62. Ryan Maness, Brandon Valeriano, and Ben Jensen, "Codebook for the Dyadic Cyber Incidentand Campaign Dataset (DCID) Version 2.0," June 2022, https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.
63. Ibid.
64. Dan Goodin, "A Patient Dies After a Ransomware Attack Hits a Hospital," *Wired,* https://arstechnica.com/information-technology/2020/09/patient-dies-after-ransomware-attack-reroutes-her-to-remote-hospital/.
65. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Goodin, "A Patient Dies After a Ransomware Attack Hits a Hospital"; Williams, "The WannaCry Ransomware Attack Left the NHS with a £73m IT Bill."
66. Sarah Kreps and Debak Das, "Warring from the Virtual to the Real: Assessing the Public's Threshold for War over Cyber Security," *Research & Politics* 4, no. 2 (April 1, 2017): 2053168017715930, https://doi.org/10.1177/2053168017715930.
67. Ryan Shandler et al., "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment," *British Journal of Political Science*, undefined/ed, 1–19, https://doi.org/10.1017/S0007123420000812.
68. Kreps and Das, "Warring from the Virtual to the Real"; Shandler et al., "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment."
69. Andy Greenberg, "How 30 Lines of Code Blew Up a 27-Ton Generator," *Wired,* October 23, 2020, https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/.
70. Microsoft, "Special Report: Ukraine," Microsoft On the Issues, April 27, 2022, 3–4, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.
71. Patrick O'Niell, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion," MIT Technology Review, May 10, 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

NOTES

72. Microsoft, “Special Report: Ukraine”; Kate Conger and David E. Sanger, “Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds,” *The New York Times*, April 27, 2022, sec. U.S., https://www.nytimes.com/2022/04/27/us/politics/russia-cyberattacks-ukraine.html.
73. Microsoft, “Special Report: Ukraine”; Conger and Sanger, “Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds.”
74. Conger and Sanger, “Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds.”
75. Matthias Schulze, “Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations” (Berlin: 12th International Conference on Cyber Conflict, 2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf.
76. Government Accountability Office, “Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities | U.S. GAO” (U.S. Government Accountability Office, October 9, 2018), https://www.gao.gov/products/gao-19-128.
77. Ryan Browne, “Russia Jammed GPS during Major NATO Military Exercise with US Troops | CNN Politics,” CNN, November 14, 2018, https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html.
78. Ciaran Martin, “Cyber Realism in a Time of War,” Lawfare, March 2, 2022, https://www.lawfareblog.com/cyber-realism-time-war.
79. Sean Lyngaas, “Biden Says He Gave Putin List of 16 Sectors That Should Be Off-Limits to Hacking,” *CyberScoop*, June 16, 2021, https://www.cyberscoop.com/biden-putin-summit-russia-geneva/.
80. CISA, “Commercial Facilities Sector | CISA,” accessed September 1, 2021, https://www.cisa.gov/commercial-facilities-sector.
81. The White House, “Remarks by President Biden on Russia’s Unprovoked and Unjustified Attack on Ukraine,” The White House, February 24, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/24/remarks-by-president-biden-on-russias-unprovoked-and-unjustified-attack-on-ukraine/.
82. Kate O’Flaherty, “How To Hack An Aircraft,” Forbes, August 22, 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/08/22/how-to-hack-an-aircraft/.
83. Osborne, “Updated Kaseya Ransomware Attack FAQ.”
84. Ben Gilbert, “Colonial Pipeline Reportedly Paid Nearly $5 Million to the Hackers Who Shut off Service to the Largest Fuel Line in the US,” *Business Insider*, May 13, 2021, https://www.businessinsider.com/hackers-get-5-million-after-causing-major-gas-shortage-2021-5; The Associated Press, “REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says.”
85. Derek B. Johnson, “US Proposes $1 Million Fine for Colonial Pipeline Ransomware Attack,” SC Media, May 9, 2022, https://www.scmagazine.com/analysis/critical-infrastructure/us-proposes-1-million-fine-for-colonial-pipeline-ransomware-attack; Joe Walsh, “Meat Producer JBS Says It’s Fully Recovered From Cyberattack,” Forbes, June 3, 2021, https://www.forbes.com/sites/joewalsh/2021/06/03/meat-producer-jbs-says-its-fully-recovered-from-cyberattack/.
86. Catalin Cimpanu, “Israel Government Tells Water Treatment Companies to Change Passwords,” ZDNet, April 27, 2020, https://www.zdnet.com/article/israel-says-hackers-are-targeting-its-water-supply-and-treatment-utilities/.
87. Catalin Cimpanu, “Two More Cyberattacks Hit Israel’s Water System,” ZDNet, July 20, 2020, https://www.zdnet.com/article/two-more-cyberattacks-hit-israels-water-system/.
88. AP and TOI STAFF, “‘Cyber Winter Is Coming,’ Warns Israel Cyber Chief after Attack on Water Systems,” May 28, 2020, https://www.timesofisrael.com/israeli-cyberchief-attack-on-water-systems-a-changing-point-in-cyberwarfare/.
89. TOI Staff, “Cyber Attacks Again Hit Israel’s Water System, Shutting Agricultural Pumps,” July 17, 2020, https://www.timesofisrael.com/cyberattacks-again-hit-israels-water-system-shutting-agricultural-pumps/.
90. Joby Warrick and Ellen Nakashima, “Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility,” *Washington Post,* May 18, 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.
91. AP Staff, “‘Cyber Disruption’ Stops Websites of Iranian Ministry,” AP NEWS, July 10, 2021, https://apnews.com/article/middle-east-business-technology-iran-hacking-f03eb188712be46648886e1c80e50586.

NOTES

92. Suren Naidoo, “Transnet’s Ports Force Majeure Is over, but Most Websites Are Still Offline,” *Moneyweb,* August 2, 2021, sec. Industry, https://www.moneyweb.co.za/news/industry/transnets-ports-force-majeure-is-over-but-most-websites-are-still-offline/.
93. Felix Njini and Prinesha Naidoo, “South Africa Port Operator Declares Force Majeure Over Cyber Attack,” *Bloomberg*, July 27, 2021, https://www.bloomberg.com/news/articles/2021-07-27/s-africa-port-operator-declares-force-majeure-over-cyber-attack-krln4ku6; Denys Reva, “Cyber Attacks Expose the Vulnerability of South Africa’s Ports,” *ISS Africa*, July 29, 2021, https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.
94. e Tidy, “Ukrainian Power Grid ‘lucky’ to Withstand Russian Cyber-Attack,” *BBC News*, April 12, 2022, sec. Technology, https://www.bbc.com/news/technology-61085480.
95. Nate Nelson, “U.S. Water Utilities Prime Cyberattack Target, Experts,” Threatpost, June 10, 2022, https://threatpost.com/water-cyberattack-target/179935/.
96. Kevin Collier, “A Hacker Tried to Poison a Calif. Water Supply. It Was as Easy as Entering a Password.,” NBC News, June 17, 2021, https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206.
97. Matt Egan, “$24 Billion in Goods Is Floating Outside California’s Biggest Ports | CNN Business,” CNN, October 25, 2021, https://www.cnn.com/2021/10/25/business/supply-chain-ports-inflation/index.html.
98. Will Daugherty, “Lloyd’s Report Highlights Risk of Cyberattacks on National Power Grid,” JD Supra, July 24, 2015, https://www.jdsupra.com/legalnews/lloyd-s-report-highlights-risk-of-83905/.
99. Vanessa Romo, “How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline’s Ransom Back,” NPR, June 8, 2021, https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac; Jacob Bunge, “JBS Paid $11 Million to Resolve Ransomware Attack,” *Wall Street Journal*, June 10, 2021, sec. Business, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.
100. CSIS, “Significant Cyber Incidents | Center for Strategic and International Studies,” updated monthly, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
101. CSIS, “Significant Cyber Incidents | Center for Strategic and International Studies,” March 2022, https://www.csis.org/programs/strategic-technologies-program/significant-cyberincidents.
102. “US Mulling Military Response to Ransomware Attacks, Biden Officials Say,” accessed June 26, 2021, https://www.theguardian.com/technology/2021/jun/06/us-military-response-ransomware-attacks-biden-russia-putin.
103. NATO, “Press Conference by NATO Secretary General Jens Stoltenberg Following the Extraordinary Virtual Summit of NATO Heads of State and Government.”