RAND
INAERTED ROOK
Research Report

BRIDGET R. KANE, STEPHEN WEBBER, KATHERINE H. TUCKER, SAM WALLACE, JOAN CHANG, DEVIN MCCARTHY, DENNIS MURPHY, DANIEL EGEL, TOM WINGFIELD

Defending the Homeland Against Critical Infrastructure Attacks

Exploring a Hypothetical Campaign of Cascading Impacts

In this report, we discuss threats to critical infrastructure (CI) and put forward a hypothetical case study to examine several phases of an adversarial attack on the United States. The attack is intended to constrain U.S. decisionmaking, disrupt military deployment, and impose strategically relevant costs on the civilian populace. We aggregate CIs into seven classes to demonstrate how an attack on any one of these categories can have outsized effects because of interdependencies between infrastructure assets, systems, and networks.

Because of the interconnected nature of CI systems, damage to one system can adversely affect another. This may lead to a cascading hazard, producing disruptions across geographic boundaries and CIs. We draw on reports of recent attacks on U.S. CI systems to inform our case study. These real-world events demonstrate interdependencies, probable effects, and challenges that could arise from future potential adversarial action targeting infrastructure in the homeland. Finally, we recommend actions

KEY FINDINGS AND IMPLICATIONS

- Critical infrastructure protection is a whole-of-nation challenge for which the United States is unprepared. Because of the interconnected nature of critical infrastructure systems, damage to any one system can adversely affect another; this may lead to a cascading hazard, producing disruptions across geographic boundaries and critical infrastructures.
- Attacks on critical infrastructure would rapidly stress national defense resources, creating acute tensions in resource management for which policymakers would have to prioritize, sequence, and deconflict many lines of effort.
- Attacks on critical infrastructure would challenge the resilience of U.S. society in a novel way; it is essential that policymakers not only prepare for attacks directed against critical infrastructure but anticipate the social and political effects that an adversary intends to produce and take steps to reduce or even reverse those effects.

to reduce the likelihood and severity of disruptions to U.S. CI in the event of attacks by a capable adversary.

What Is Critical Infrastructure?

The term *critical infrastructure* is defined in the Patriot Act as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[1] The Cybersecurity and Infrastructure Security Agency (CISA) further identifies 16 CI sectors, designated in Presidential Policy Directive 21 (PPD-21), that are "part of a complex, interconnected ecosystem"; "their incapacitation or destruction would have a debilitating effect on national security, national economic security, national public health or safety, or any combination thereof."[2]

Further compounding the complexity are the interdependencies that exist across sectors. Because of the interconnected nature of CI systems, it is probable that damage to one system will adversely affect another. These interdependencies are the mainspring of cascading, cross-sector (and, perhaps, cross-geographical) impacts that present challenges for response efforts in the event of a coordinated attack.

Because of the interconnected nature of CI systems, it is probable that damage to one system will adversely affect another.

Approach

We conducted an open-source literature review for each sector to understand possible threats, threat actors, impacts (both on national defense and socioeconomic well-being), and potential challenges for a coordinated U.S. response to incidents affecting CI. We also conducted interviews with experts both within and outside RAND. Our sectors were categorized based on literature related to the original 16 sectors as identified by PPD-21.[3] We downselected from those 16 on the basis of perceived criticality and opportunities for consolidation and reorganized our sector analysis into seven categories for conciseness and clarity: communications, financial services, health care, municipal services, energy, transportation, and water.[41] These categories allowed us to address larger assets, systems, and networks while retaining the ability to address smaller subsectors via interdependencies that appear only when mapping critical functions.

This approach gave us a foundational knowledge of each sector on which we could build to present a broader representation of the impacts of adversarial attacks. For example, an attack that ultimately affects the price of oil (such as the ransomware attack on the Colonial Pipeline) could have cascading effects on the transportation industry.[5] A sufficiently severe attack against CI could affect the ability of troops to deploy, potentially limiting the United States' ability to respond to an overseas crisis in a timely manner. Although this is a simplified extrapolation, our analysis of each sector allows us to identify how interdependencies may have outsized impacts on the safety and security of the country. We apply our findings (in the form of real-world case studies) to each of the designated phases of a major CI attack undertaken by an adversary. From this application, we highlight cascading effects, interdependencies, and subsequent challenges in response. Finally, we make recommendations regarding assessed vulnerabilities and potential efforts to minimize constraints and disruptions to U.S. CI in the event of an attack.

How Might an Adversary Attack Critical Infrastructure?

In the past two decades, criminals, violent extremists, and nation-states—using both physical and cyber vectors—have increasingly probed, infiltrated, and attacked U.S. CI.[6] Adversaries with increasingly sophisticated capabilities, such as China, Russia, North Korea, and Iran, have attacked and continue to test the defenses of U.S. CI using a variety of tactics, techniques, and procedures.[7]

There are many reasons why nation-state adversaries might target U.S. CI. For example, adversaries may seek to influence political decisionmaking, interfere with a U.S. military deployment, or cause large-scale societal disruption for strategic effect. China, for example, approaches military problems through the lens of *systems destruction*,[8] planning to negate the conventional strength of the U.S. military by attacking information and logistics networks. Alternatively, Russia might be more likely to take an *escalate to de-escalate* approach, seizing the initiative by quickly raising the stakes of a conflict by threatening or imposing costs that the U.S. populace and political leadership are unwilling to bear.[9] U.S. adversaries share a common desire to gain an asymmetric advantage over the United States, and our research suggests that attacking CI is one means by which they could achieve this advantage.[10]

In this report, we explore a hypothetical campaign undertaken by an adversary "designed by the aggressor to win at the lowest level of military confrontation and commitment"[11] in three phases:

- Phase 1: Constrain U.S. decisionmaking processes.
- Phase 2: Disrupt U.S. military deployments.
- Phase 3: Decisively undermine public support for initiating or continuing hostilities through widespread and severe cyberattacks against civilian CI.

Here, we build on prior work by Thomas Wingfield and James Bret Michael that proposed a framework for a notional strategic cyber campaign.[12] We first consider sector-specific ways in which an adversary might seek to constrain U.S. decisionmaking to lay the groundwork for adversarial action. Once U.S. leadership's decisionmaking processes are under pressure, the threat actor may strike against infrastructures that support deployment processes. The United States could well become overwhelmed (and effectively neutralized) by "interlocking domestic crises."[13] In the event that the United States still proves resistant, the adversary may then implement a series of strategic cyberattacks against CI. Such a move may be attractive to an adversary who believes that cyberattacks could control escalation in a way that nuclear or other kinetic strikes might not. Although we conceptualize the scenario as having three phases, a real-world adversary may not move cleanly between one phase and another.

In our scenario, the focus of attacks moves from one array of targets to another as the purpose of the attacks shifts. The adversary uses a variety of tactics to create an atmosphere of mistrust in government, sow tensions among the general populace, saturate the news media, and totally consume the target state's political bandwidth to reach its ultimate goal of preventing, delaying, or constraining the U.S. response to the adversary's actions abroad. Although this scenario is a hypothetical use case of a future adversarial campaign, it is based on real-world examples: The capabilities needed to execute each type of attack discussed in this report already have been tested by adversaries against U.S. CI. This case study is fictional, but the attack vectors are not.

The capabilities needed to execute each type of attack discussed in this report already have been tested by adversaries against U.S. CI.

Phase 1: Constraining U.S. Decisionmaking

Imagine that an adversary launches a military invasion of a U.S.-allied country or close partner. Initially, the adversary might seek to constrain the decision space of U.S. policymakers by shaping messages to the general public, the press, and government decisionmakers; the adversary is presenting narratives that obfuscate the nature of the military actions that are underway, those actions' characterization under international law, and the consequences of an ill-advised U.S. intervention. The U.S. government signals resolve while taking diplomatic and economic measures to impose costs on the aggressor. The President must now decide what military options they are willing to take with forward-deployed military forces and whether the United States will deploy more troops into theater. Congressional support, reflecting public opinion, is sharply divided on the issue. The situation unfolds as follows:

1. Following the President's statement of commitment and enactment of sanctions in response to the military invasion, messages—posted by a domestic extremist group known as *Nightfall*—begin to spread across social media platforms. The messages detail plans to attack major electrical substations in the National Capital Region (NCR) and call for like-minded individuals to take up arms and physically attack substations by damaging electrical equipment. The group's stated goal is to sow chaos and discord, contributing to societal collapse and a subsequent "race war" in the United States.[14] Three of these attacks occur, leaving 500,000 people without power for approximately two days while temperatures are climbing through the 90s in much of the country (see Box 1). The Federal Bureau of Investigation (FBI) suspects that this may be an attempt by an adversary to manipulate U.S. citizens with extremist views to act as useful—if unwitting—surrogates. The FBI is working to find the perpetrators and to unpack the relationship between domestic extremism and foreign influence.[15]
2. A ransomware attack against local governments in the NCR shuts down some government services. Some of these services were previously affected by the power outage while others were not. Emergency response times are now delayed for police, fire services, and emergency medical responders.[16] It is unclear whether the cyberattack was the work of a criminal group or connected to the adversary, but the threat to public safety has the public on edge.
3. Loss of power to traffic signals contributes to multiple accidents as people rush to find stores that have electricity where they can fulfill basic needs. Local hospitals rely on backup generators, which limit energy availability to critical functions. Ronald Reagan Washington National Airport shifts to its backup power system, a series of diesel-powered generators, reducing power availability to safety-of-flight operations.[17] The limited yet frustrating scope of this attack shows U.S. officials that the adversary is using this opportunity as a probe to identify particular points of weakness or cascading effects in the affected industries (see Box 2).
4. The FBI, the Department of Homeland Security (and CISA, one of its constituent agencies), the Office of the Director of Intelligence, and the National Security Agency release a joint public statement in which they note that analysts have "high confidence" that the sham

BOX 1

Real World Precedent: Electrical Substation Attacks

In 2022 and 2023, electrical substations in North Carolina, Washington, and Oregon were damaged by shootings, arson, and other forms of vandalism. These unsophisticated physical attacks led to power outages for customers across large geographic areas.

Rudlang, "Lawmakers, Energy Companies Make Moves to Protect N.C. Power Grid"; Levenson, "Attacks on Electrical Substations Raise Alarm."

extremist group was created by a foreign government. Despite this, true domestic extremist groups begin to claim ownership of the attack in hopes of gaining exposure and momentum to attract others to their causes.

5. Citizens remain frustrated with local and federal government processes, the length of time taken to bring power back online, the lack of physical security at key infrastructure assets, and a political climate that heightens the profile of extremist organizations. Politicians and media pundits engage in partisan finger-pointing; some emphasize domestic extremism and others emphasize the threat of war with a foreign adversary.
6. The cascading impacts of a temporary power outage in the NCR, coupled with moderate degradation in municipal services, create tangible hardships for many citizens, including some risk to lives and property. The adversary's attack vectors play on a highly partisan political climate to sow fear, anger, and hatred well beyond the scope of the attacks. With moderate disruption to the NCR and fear of more-severe cyberattacks, some voices in the President's administration question whether a U.S. military deployment to counter the invasion will be politically tenable.

BOX 2

Real World Precedent: Colonial Pipeline

In 2021, the Colonial Pipeline—through which fuel is distributed from the U.S. Gulf Coast to the U.S. east coast market—was shut down because of a ransomware attack by a criminal group operating from Eastern Europe. The attack prompted rampant panic buying of gasoline up and down the east coast, leading to localized shortages and emergency declarations in Washington, D.C., and 17 states.

Romo, "Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack,"; Sabin, "Colonial Pipeline Ransomware Attack's Unexpected Legacy."

Phase 2: Disrupting a U.S. Military Deployment

The military depends on civilian infrastructure to deploy troops abroad. By disrupting certain civilian infrastructure, an adversary can delay U.S. mobilization and deployment from the homeland and narrow options for policymakers and military commanders. The phase unfolds as follows:

1. The adversary in this scenario implements a two-pronged strike on military deployment processes. First, it releases a cyber weapon disguised as ransomware against industrial control systems (ICS) used by both rail systems and seaports.[18] Given the Department of Defense's (DoD) reliance on civilian contractors for logistical support, the adversary releases a similar, simultaneous malware attack against logistics software used by private companies who are actively carrying out shipping operations at the port of embarkation. In this attack, the adversary targets critical rail functions, such as signals, switching, and safety.[19] Until safe operations can resume, railroads are unable to move materiel from bases to ports via freight rail.[20]
2. The adversary targets companies involved in the Voluntary Intermodal Sealift Agreement, the Maritime Security Program, and the Civil Reserve Air Fleet. In a contingency, these companies could make merchant shipping and commercial airlift available to carry equipment and personnel into theater (see Box 3).[21] These attacks could slow or suspend the business operations of companies that the United States might depend on to move equipment and personnel in the event of an escalation, taking options away from the military while potentially slowing the timeline of a major deployment.[22] In particular, delayed deployment might allow the adversary to consolidate its initial gains, raising the cost of intervention with each day lost.
3. Impacts of the attacks are not felt solely by the defense industrial base. Weak and generally voluntary collaborative ties between private industry and the federal government regard-

BOX 3

Real World Precedent: Cyber Intrusions at U.S. Transportation Command

U.S. Transportation Command relies heavily on the private sector to project and sustain the U.S. military around the world. In 2014, the Senate Armed Services Committee identified cyber intrusions from Chinese entities against many of these contractors. Targets included companies involved in the Voluntary Intermodal Sealift Agreement and the Civil Reserve Air Fleet, which the United States would rely on to move materiel and troops in a conflict overseas.

United States Senate Committee on Armed Services, "SASC Investigation Finds Chinese Intrusions into Key Defense Contractors."

ing cyber incident reporting affect response effectiveness and increase the likelihood that adversaries could remain undetected and undisturbed on target systems for much longer, gathering information to enable subsequent attacks on other systems.[23] Weeks after the initial cyber intrusions, the civilian populace begins to feel the effects of attacks on additional rail control systems. Multiple companies report disruptions in freight transport, the exposure of private information, and financial losses.[24]

4. The cumulative impact of degradation to the country's rail network, port operations, and related private sector information systems impede the available options and slow the timelines required to sustain a major deployment. Should the President decide to commit U.S. troops to the defense of an overseas ally, the associated logistical support and force projection would be delayed. The President's decision space has effectively been narrowed. These attacks on civilian infrastructure produce pressure on supply chains, which, along with the risk of war, create a shock to the U.S. economy.[25]

Phase 3: Strategic Cyberattacks Against Civilian Critical Infrastructure

An adversary might target U.S. popular will directly, using strategic cyberattacks to deliver a sudden, demoralizing blow. The logic may be similar to that of other forms of military escalation, maximizing disruption to society to impose unacceptable costs.[26] This could also follow the logic of escalating to de-escalate or shock-to-pause. The adversary could rapidly raise the stakes of the conflict to gain leverage or paralyze U.S. military decisionmaking long enough to solidify its military gains and raise the cost of U.S. intervention.[27]

1. In this phase, the adversary intends to impose severe costs on the United States, assuming that it would be able to control escalation. Feeling increasingly vulnerable under wartime conditions, the adversary conducts a massive malware attack on the NCR's electric power grid, believing that the effects will be controllable and reversible (see Box 4).[28] Continuing to escalate the crisis, the adversary conducts additional malware attacks against municipal services. The original attack leaves 50 percent of the NCR without power for 72 hours, rendering affected municipalities unable to access databases that support crucial local services. The ripple of service failures renders utility operators unable to monitor water utilities and stresses fire, police, and emergency medical responders.
2. Chaos once again ensues as traffic and financial systems malfunction. Hospitals, airports, and other lifesaving and life-sustaining facilities and assets begin to lose backup power generation, which, in many cases, is designed to last only up to 48 hours. For reference, household appliances, such as freezers, hold a safe temperature for approximately 48 hours; refrigerators keep food and medications safe for approximately 24 hours.[29] The public does not have access to running water or functional waste treatment processes; backup generation is limited to the restoration of key government functions and higher-priority life-saving and life-sustaining facilities.[30] While the first

BOX 4

Real World Precedent: Wolf Creek Nuclear Power Plant Hacking

A Russian government entity hacked into Kansas's Wolf Creek nuclear power plant in 2017 as part of larger efforts to maintain persistent, unauthorized access to U.S. infrastructure companies' systems and assets. The entity spent five years targeting supervisory control and data acquisition systems of energy companies and embedding malware in software updates, eventually using compromised employee accounts to spread malware throughout the Wolf Creek Nuclear Operating Corporation internal network.

Woodruff Swan, "Russian Spies Indicted in Worldwide Hacks of Energy Industry, Including Kansas Nuclear Plant"; Corera, "Cyberattack"; Goldbaum and Rashbaum, "The MTA is Breached by Hackers as Cyberattacks Surge"; Center for International and Strategic Studies, "Publicly Reported Iranian Cyber Actions in 2019."

attack happened during a heat wave, this new intrusion comes in December, and the general populace is unprepared for freezing temperatures. Hundreds of civilians die from hypothermia and exposure.

3. A hacker accesses a water treatment plant in New Jersey and changes the levels of chemicals added to treat the water, causing dozens of people to fall ill in a matter of hours (see Box 5). Multiple municipalities issue "do not drink" notices. Grocery stores around the country experience a run on bottled water.[31]
4. With the economy already in a severe downturn, Wall Street is hit with multiple cyberattacks that close stock trading for two days.[32]
5. DoD elevates the security posture at military installations nationwide, and the President declares a national emergency for which the Federal Emergency Management Agency is led under the National Response Framework, which governs how the federal government responds to emergencies in support of state, local, tribal, and territorial (SLTT) authorities.[33]

BOX 5

Iranian Dam Breach

In 2013, a group linked to Iran's Revolutionary Guard Corps accessed the ICS of the Bowman Avenue Dam in New York state. Local officials suggested that the dam may have been mistaken for a much larger dam in another state, or that this was a trial run to similarly access the industrial control systems of larger CI sites.

Ferman, "Texas Power Grid, Energy Sectors Facing Elevated Russian Cyber Threats During War in Ukraine"; Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case."

6. Several thousand U.S. citizens are killed as a direct result of the adversary's strategic cyberattack campaign, and the President must decide how to respond to this attack on the United States. The President calls the National Guard in Virginia, Maryland, and the District of Columbia into federal service.
7. The governors of the most directly affected states believe that their National Guards will be needed to support emergency responders and protect their citizens. These governors try to resist the federalization of these resources by quickly initiating in-state mobilization, creating further complexities for the disentanglement of units and reorganization under federal control. The general public is outraged by the unfolding of events; some demand a forceful military response, and others insist that the United States "mind its own business" and focus on protecting its own people.

Acknowledging the Threat

This hypothetical campaign against U.S. CI reveals significant gaps in the country's preparedness.

Critical Infrastructure Protection Is a Whole-of-Nation Challenge

This analysis demonstrates that **CI protection is a whole-of-nation challenge for which the United**

States is unprepared. The United States has never faced the aforementioned scenario or anything like it, in which a sophisticated adversary conducts a coordinated, escalating campaign of attacks on CI. The U.S. government and other CI stakeholders are not postured to successfully address multiple simultaneous attacks on U.S. CI.

CI owners and operators—which include private sector entities, SLTT governments, and federal entities—are the first line of defense, responsible for preventing, identifying, and remediating intrusions and attacks. In some cases, these organizations take preparedness very seriously and invest large sums of money in their own security. These companies sometimes lack the knowledge (including insights generated by the U.S. Intelligence Community) and the capability (including specific defensive techniques recommended by U.S. Cyber Command) to defend themselves. CI owners and operators may also lack the incentive to fully prepare to withstand a cyberattack or other attack from a state-sponsored adversary.[34]

In addition to owners and operators, CI is overseen by authorities that cut across municipal and regional boundaries and a variety of federal agencies, each of which has its own responsibilities, authorities, capabilities, and dependencies on CI. This patchwork governance creates problems in securing CI and preparing for emergencies.[35]

Amid unfolding incidents that affect multiple CI systems and assets, these stakeholders will need to share information, assess impacts, diagnose problems, and undertake mitigation and response activities. While some stakeholders may have contingency plans and may have exercised their own response capabilities, this type of broad coordination and integration of efforts has never happened at scale during a similarly complex crisis. Nor do processes or mechanisms exist to facilitate such coordination.

While some stakeholders may have contingency plans and may have exercised their own response capabilities, this type of broad coordination and integration of efforts has never happened at scale during a similarly complex crisis.

Attacks on Critical Infrastructure Could Stress National Defense Resources

This analysis also suggests that attacks on CI would rapidly stress national defense resources. Our scenario envisions the homeland under attack as part of a larger conflict on the far side of the world. Decisionmakers would have to weigh the imperative to respond to emergencies within the United States against the need to deploy troops overseas.

A large-scale, complex homeland emergency, coupled with the need to deploy forces abroad, would create acute tensions in resource management, and policymakers would have to prioritize, sequence, and deconflict many lines of effort. First, U.S. Northern Command may not have the necessary forces in theater to conduct both its statutory homeland defense and defense support to civil authorities (DSCA) missions, both of which would be necessary in a situation similar to the one we have outlined.[36] Second, the National Guard plays a key role in homeland defense and DSCA as a force that is responsive to state governors. These same forces house important capabilities for the U.S. Army and U.S. Air Force that are essential for contingencies, both in the United States and in other theaters, such as medical personnel. Much of the Army and Air Force's medical capability resides in the National Guard.[37] It is already uncertain whether DoD has enough medical capacity to meet

its warfighting requirements, let alone requirements resulting from a homeland emergency.[38]

Another consideration is the availability of cyber professionals. Given the scope of cyberattacks that we posit in this scenario, U.S. Cyber Command could conceivably be asked to support civil authorities with its high-demand skill set.[39] Some of its forces are reserve and National Guard, and in some cases, these same cyber professionals hold cybersecurity-related jobs in the private sector. This raises important questions for policymakers about the interconnectedness of DoD's homeland defense and DSCA missions, and whether U.S. forces are ready to meet them.[40] It also brings into question the capacity of the civilian interagency and whether the organizations charged with any response, including consequence management, are resourced and prepared to take on a national-level emergency while the military focuses on events overseas.[41]

Attacks on Critical Infrastructure Could Challenge the Resilience of American Society

Finally, attacks on CI would challenge the resilience of U.S. society in a novel way. The scenario we offer is hypothetical, but its constituent elements are based on actual compromises of U.S. CI. In these real-world attacks, bad actors demonstrated their abilities to penetrate and degrade the systems on which those living in the United States rely for their security and welfare. As we saw in 2021, one relatively minor incident—a ransomware attack on the Colonial Pipeline—caused no direct fuel shortage, but the ensuing panic buying created fuel shortages. This isolated incident consumed the airwaves and suggests that a coordinated campaign of such multiple, simultaneous attacks will have significant impacts on the public, both practically and psychologically. Attacks intended to forestall a U.S. response to aggression overseas could create fear among the general public, undermine social cohesion, and paralyze political decisionmaking structures. **It is essential that policymakers not only prepare for attacks directed against CI but anticipate the social and political effects that an adversary intends to produce and take steps to reduce or even reverse those effects.**

Preparing for the Worst

Given the demonstrated vulnerabilities in U.S. CI, policymakers should take action prior to a crisis to prepare the United States to manage the homeland consequences of a coordinated attack on CI while preparing for potential military mobilization and deployment to a contingency. Recognizing these gaps, federal and SLTT governments and private-sector CI stakeholders should work together to plan, resource, train, and exercise their detection and response capabilities, including their processes and mechanisms to achieve unity of effort in preparedness and response. The federal government should continue to prioritize its relationships with SLTT governments and private-sector owners and operators of CI. This could include expanded information-sharing, training, and combined planning prior to an emergency. Incorporating the private sector into preparedness efforts strengthens the first line of defense for attacks on CI, and developing interoperability between the federal government and the many other stakeholders could mitigate friction and increase the speed of a response during crisis.

Given the possibility that attacks on CI could stress national defense resources, the federal government should ensure that all departments and agencies are resourced and postured appropriately to

Attacks intended to forestall a U.S. response to aggression overseas could create fear among the general public, undermine social cohesion, and paralyze political decisionmaking structures.

fulfill the government's homeland defense and force projection missions—simultaneously, if needed. DoD should consider its ability to project forces abroad in relation to its homeland defense mission and the frequent tasking of DoD assets and capabilities to support civil authorities. Additionally, DoD should consider the support that it will need from the federal interagency, SLTT governments, and private-sector entities during a national emergency and work to develop those vital relationships. This could include planning for (1) redundancy in contracted logistical support, (2) assistance from state and local authorities in securing military facilities, or (3) access to civilian subject-matter experts.

Finally, the whole country must build societal resilience. A capable adversary might conduct attacks on U.S. CI to gain advantage in a potential conflict, seeking to narrow policymakers' decision space, delay or degrade military mobilization, and influence public opinion. By disrupting the systems that undergird the way of life in the United States, an adversary could create a climate of fear and possibly disorder. This could divide communities by causing economic scarcity, political polarization, and racial prejudice. The adversary's actions could create mistrust and sow a lack of confidence in the government, leading to a break in popular will to confront an adversary militarily. As demonstrated by recent emergencies, it could even result in widespread civil unrest.[42] To safeguard against these outcomes, policymakers should build societal resilience from the ground up. Similar to the unity of effort needed for effective emergency response, resilience is a whole-of-nation task. Policymakers could devote resources to improving, hardening, and creating redundancy in CI to lessen the impact of future attacks. Policymakers could work at all levels of government and with civil society to educate the public on emergency preparedness and foster dialogue within communities about the need to navigate uncertainty with attitudes of mutual respect and mutual support. Government agencies could prepare for the broad-scale messaging needed to reach the general public during a time of emergency, potentially in an environment of disrupted communications. As small, isolated emergencies arise, they could serve as tests for new techniques and procedures in which the cost of a suboptimal response would not be catastrophic. This real-world practice would serve not only to validate new approaches to resilience and recovery, but would start to build, over time, the trust between stakeholders that will be essential to respond effectively to a complex attack on U.S. CI.

The federal government should ensure that all departments and agencies are resourced and postured appropriately to fulfill the government's homeland defense and force projection missions—simultaneously, if needed.

By taking immediate action, the United States can position itself to prevent or effectively respond to attacks on its CI. While our scenario is hypothetical, probing attacks against CI are a regular occurrence. As discussed in this report, a variety of actors (including nation-states) have attacked the systems on which people in the United States depend for their way of life. The U.S. government can heed these warnings to build unity of effort among stakeholders, prepare for national defense during a homeland emergency, and foster societal resilience. Our adversaries' statements and actions suggest that they believe that the United States's greatest vulnerability is its own people. The United States can prove them wrong and provide for the national defense by taking measures to ensure that the country's people remain its greatest strength.

Notes

1 Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

2 CISA, "Critical Infrastructure Sectors." The 16 CI sectors as recognized by PPD-21 are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater (PPD-21, *Critical Infrastructure Security and Resilience*).

3 CISA, "Critical Infrastructure Sectors."

4 CISA, "Critical Infrastructure Sectors."

5 Romo, "Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack"; Sabin, "Colonial Pipeline Ransomware Attack's Unexpected Legacy."

6 Center for Strategic and International Studies, "Significant Cyber Incidents."

7 Woodruff Swan and Miller, "Russian Spies Indicted in Worldwide Hacks of Energy Industry, Including Kansas Nuclear Plant"; Corera, "Cyberattack"; Goldbaum and Rashbaum, "The MTA Is Breached by Hackers as Cyberattacks Surge"; Center for Strategic and International Studies, "Publicly Reported Iranian Cyber Actions in 2019."

8 Engstrom, *Systems Confrontation and System Destruction Warfare*.

9 Ball, "Escalate to De-Escalate."

10 Neville, "Orchestrating U.S. Cyber Operations to Defend the Homeland."

11 Wingfield and Michael, "Waterfall," p. 143.

12 Our hypothetical scenario is modeled after Winfield and Michael's notional campaign, which envisions a conflict in the cyber domain to frame issues related to cascading effects and escalation.

13 Wingfield and Michael, "Waterfall," p. 144.

14 Criminals have recently targeted electricity substations, resulting in power outages (Rudlang, "Lawmakers, Energy Companies Make Moves to Protect N.C. Power Grid"; Levenson, "Attacks on Electrical Substations Raise Alarm"). Competitors often use information in ways that amplify existing political divisions. For examples, see Paul and Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, and Martinez, "Facebook Ad Believed to Have Been Bought by Russians Targeted Baltimore, Ferguson."

15 China is a strategic competitor that conducts extensive activities designed to influence the United States and other countries around the world, including using news media and social media on a large scale. See Zhang, Hoja, and Latimore, *Gaming Public Opinion*.

16 Criminals have affected municipal services and first responders with these types of attacks. See "Baltimore's 911 Emergency System Hit by Cyberattack," NBC News; and City of Oakland, "City of Oakland Targeted by Ransomware Attack, Work Continues to Secure and Restore Services Safely."

17 Aratani, "Here's What Happens When the Lights Go Out at National Airport."

18 Lieto, "Cyber at Sea"; Kramek, *The Critical Infrastructure Gap*.

19 Swain, "The Emerging Cyber Threat to the American Rail Industry"; Figueroa Diaz, "An Analysis of Railway Industrial Control Systems Vulnerabilities."

20 Capra, *Protecting Critical Rail Infrastructure*; Grohoski, *The Vulnerabilities of U.S. Strategic Ports to Acts of Sabotage*.

21 U.S. Senate Committee on Armed Services, "SASC Investigation Finds Chinese Intrusions into Key Defense Contractors."

22 Wolff, "The Department of Defense's Digital Logistics Are Under Attack."

23 Lostri, Lewis, and Wood, "A Shared Responsibility."

24 Patil, "How Railroads Can Harden Their Defenses and Get Ahead of Cyber Threats in 2023."

25 Kshetri, "Economics of Supply Chain Cyberattacks."

26 Wingfield and Michael, "Waterfall," p. 147.

27 Schneider, "Escalate to De-Escalate."

28 Ferman, "Texas Power Grid, Energy Sectors Facing Elevated Russian Cyber Threats During War in Ukraine"; Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case."

[29] FoodSafety.gov, "Food Safety During Power Outage."

[30] Environmental Protection Agency, *Power Resilience*.

[31] Vera, Lynch, and Carrega, "Someone Tried to Poison a Florida City by Hacking into the Water Treatment System, Sheriff Says."

[32] Pagliery, "Russian Hackers Placed 'Digital Bomb' in Nasdaq—Report."

[33] U.S. Department of Homeland Security, *National Response Framework*.

[34] Orszag, "Critical Infrastructure Protection and the Private Sector"; Daniel, "Reporting Cyberattacks Will Soon Be Mandatory."

[35] Popovich and Plumer, "Why the U.S. Electric Grid Isn't Ready for the Energy Transition."

[36] Knight, *Homeland Security*.

[37] Sheets, *Army Medical Capacity*.

[38] Farrell, *Defense Health Care*.

[39] Kirschbaum, "Is DOD Ready to Support a Response to a Cyberattack?"

[40] Spirtas and Webber, "The Future and Past of War and Disease."

[41] Cortez Masto, "Cortez Masto Requests That FEMA Factor COVID-19 into Disaster Preparedness Planning."

[42] Vergun, "DoD Official"; Tang, "More Than 9,000 Anti-Asian Incidents Have Been Reported Since the Pandemic Began"; MacFarlane and McDonald, "Jan. 6 Timeline"; Zurcher, "George Floyd Death."

References

Aratani, Lori, "Here's What Happens When the Lights Go Out at National Airport," *Washington Post*, August 16, 2018.

Ball, Joshua, "Escalate to De-Escalate: Russia's Nuclear Deterrence Strategy," Global Security Review, August 20, 2018.

"Baltimore's 911 Emergency System Hit by Cyberattack," NBC News, March 28, 2018.

Berger, Joseph, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, March 25, 2016.

Capra, Gregory S., *Protecting Critical Rail Infrastructure*, U.S. Air Force Counterproliferation Center Future Warfare Series, No. 38, December 2006.

Center for Strategic and International Studies, "Significant Cyber Incidents," webpage, undated. As of February 26, 2024: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Center for Strategic and International Studies, "Publicly Reported Iranian Cyber Actions in 2019," webpage, undated. As of February 26, 2024: https://csis.org/programs/strategic-technologies-program/resources/publicly-reported-iranian-cyber-actions-2019

CISA—*See* Cybersecurity and Infrastructure Security Agency.

City of Oakland, "City of Oakland Targeted by Ransomware Attacks, Work Continues to Secure and Restore Services Safely," news release, April 4, 2023.

Corera, Gordon, "Cyber-Attack: US and UK Blame North Korea for WannaCry," BBC News, December 19, 2017.

Cortez Masto, Catherine, "Cortez Masto Requests That FEMA Factor COVID-19 into Disaster Preparedness Planning," press release, U.S. Senate, April 21, 2020.

Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," webpage, undated. As of February 26, 2024: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Daniel, Michael, "Reporting Cyberattacks Will Soon Be Mandatory. Is Your Company Ready?" *Harvard Business Review*, April 19, 2023.

Engstrom, Jeffrey, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, RAND Corporation, RR-1708-OSD, 2018. As of February 26, 2024: https://www.rand.org/pubs/research_reports/RR1708.html

Environmental Protection Agency, *Power Resilience: Guide for Water and Wastewater Utilities*, Office of Water, EPA 800–R–19–001, June 2019.

Farrell, Brenda S., *Defense Health Care: Actions Needed to Determine the Required Size and Readiness of Operational Medical and Dental Forces*, Government Accountability Office, GAO-19-206, February 2019.

Ferman, Mitchell, "Texas Power Grid, Energy Sectors Facing Elevated Russian Cyber Threats During War in Ukraine," *Texas Tribune*, March 31, 2022.

Figueroa Diaz, Victor M., *An Analysis of Railway Industrial Control Systems Vulnerabilities*, dissertation, Utica College, May 2018.

FoodSafety.gov, "Food Safety During Power Outage," webpage, last reviewed September 20, 2023. As of February 26, 2024: https://www.foodsafety.gov/food-safety-charts/food-safety-during-power-outage

Goldbaum, Christina, and William K. Rashbaum, "The M.T.A. Is Breached by Hackers as Cyberattacks Surge," *New York Times*, July 20, 2021.

Grohoski, David C., *The Vulnerabilities of U.S. Strategic Ports to Acts of Sabotage*, dissertation, Naval War College, February 12, 1996.

Ileto, Jason, "Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition," Modern War Institute, May 10, 2022.

Kirschbaum, Joe, "Is DOD Ready to Support a Response to a Cyber Attack," blog post, Government Accountability Agency, August 1, 2017. As of February 26, 2024: https://www.gao.gov/blog/2017/08/01/is-dod-ready-to-support-a-response-to-a-cyber-attack

Knight, William, *Homeland Security: Roles and Missions for United States Northern Command*, Congressional Research Service, RL34342, June 3, 2008.

Kramek, Joseph, *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*, Brookings Institution, July 2013.

Kshetri, Nir, "Economics of Supply Chain Cyberattacks," *IT Professional*, Vol. 24, No. 3, May–June 2022.

Levenson, Michael, "Attacks on Electrical Substations Raise Alarm," *New York Times*, February 4, 2023.

Lostri, Eugenia, James Andrew Lewis, and Georgia Wood, "A Shared Responsibility: Public-Private Cooperation for Cybersecurity," Center for Strategic and International Studies, March 22, 2022.

MacFarlane, Scott, and Cassidy McDonald, "Jan. 6 Timeline: Key Moments from the Attack on the Capitol," CBS News, January 6, 2023.

Martinez, Peter, "Facebook Ad Believed to Have Been Bought by Russians Targeted Baltimore, Ferguson," CBS News, September 17, 2017.

Neville, Jamel, "Orchestrating U.S. Cyber Operations to Defend the Homeland," War Room Online Journal, June 30, 2022.

Orszag, Peter R., "Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives," Brookings Institution, September 4, 2003.

Pagliery, Jose, "Russian Hackers Placed 'Digital Bomb' in Nasdaq—Report," CNN Business, July 17, 2014.

Patil, Krupa, "How Railroads Can Harden Their Defenses and Get Ahead of Cyber Threats in 2023," AppviewX, February 8, 2023.

Paul, Christopher, and Miriam Matthews, *The Russian "Firehouse of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, RAND Corporation, PE-198-OSD, 2016. As of February 26, 2024: https://www.rand.org/pubs/perspectives/PE198.html

Popovich, Nadja, and Brad Plumer, "Why the U.S. Electric Grid Isn't Ready for the Energy Transition," *New York Times*, June 12, 2023.

PPD-21—*See* Presidential Policy Directive 21.

Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, Executive Office of the President, February 12, 2013.

Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, October 26, 2001.

Romo, Vanessa, "Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack," NPR, May 11, 2021.

Rudlang, Sarah, "Lawmakers, Energy Companies Make Moves to Protect N.C. Power Grid," Spectrum News 1, May 1, 2023.

Sabin, Sam, "Colonial Pipeline Ransomware Attack's Unexpected Legacy," *Axios*, May 8, 2023.

Schneider, Mark B., "Escalate to De-Escalate," *Proceedings of the U.S. Naval Institute*, Vol. 143, No. 2, February 2017.

Sheets, Jessica J., *Army Medical Capacity: Ready to Meet the LSCO Challenge?* U.S. Army Heritage and Education Center, Analysis and Research Team, August 2021.

Spirtas, Michael, and Stephen Webber, "The Future and Past of War and Disease," *RAND Blog*, January 27, 2022. As of February 26, 2024: https://www.rand.org/pubs/commentary/2022/01/the-future-and-past-of-war-and-disease.html

Swain, Claudia, "The Emerging Cyber Threat to the American Rail Industry," *Lawfare* blog, October 20, 2022. As of February 26, 2024: https://www.lawfaremedia.org/article/emerging-cyber-threat-american-rail-industry

Tang, Terry, "More Than 9,000 Anti-Asian Incidents Since Pandemic Began," Associated Press, August 12, 2021.

U.S. Department of Homeland Security, *National Response Framework*, 4th ed., October 28, 2019.

U.S. Senate Committee on Armed Services, "SASC Investigation Finds Chinese Intrusions into Key Defense Contractors," press release, September 17, 2014.

Vera, Amir, Jamiel Lynch, and Christina Carrega, "Someone Tried to Poison a Florida City by Hacking into the Water Treatment System, Sheriff Says," CNN, February 8, 2021.

Vergun, David, "DOD Official: National Guard Is First Choice in Response to Civil Unrest," DoD News, June 3, 2020.

Wingfield, Thomas C., and James Bret Michael, "Waterfall: Cascading Effects of a Strategic Cyber Campaign," *Computer*, Vol. 56, No. 4, April 2023.

Wolff, Jason, "The Department of Defense's Digital Logistics Are Under Attack," Brookings Institution, July 2023.

Woodruff Swan, Betsy, and Maggie Miller, "Russian Spies Indicted in Worldwide Hacks of Energy Industry, Including Kansas Nuclear Plant," *Politico*, March 24, 2022.

Zhang, Albert, Tilla Hoja, and Jasmine Latimore, "Gaming Public Opinion: The CCP's Increasingly Sophisticated Cyber-Enabled Influence Operations," Australian Strategic Policy Institute, April 26, 2023.

Zurcher, Anthony, "George Floyd Death: Violence Erupts on Sixth Day of Protests," BBC News, June 1, 2020.

Acknowledgments

We wish to recognize the contributions of the reviewers, support staff, publishing staff, and especially the participants in the INVERTED ROOK game, who provided thoughtful, timely, and operationally relevant input at each stage of the game.

Abbreviations

CI	critical infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
DoD	U.S. Department of Defense
DSCA	defense support to civil authorities
FBI	Federal Bureau of Investigation
ICS	industrial control systems
NCR	National Capital Region
PPD	Presidential Policy Directive
SLTT	state, local, tribal, and territorial

About This Report

In this report, we discuss threats to critical infrastructure and put forward a hypothetical case study to examine several phases of an adversarial attack on the United States. The attack is intended to constrain U.S. decisionmaking, disrupt military deployment, and impose strategically relevant costs on the civilian populace. We aggregate critical infrastructures into seven classes to demonstrate how an attack on any one of these categories can have outsized effects because of interdependencies between infrastructure assets, systems, and networks.

This report is based on unclassified insights gained before, during, and after the INVERTED ROOK game, which involved numerous interagency sponsors and participants. While all players provided invaluable input, the research, analysis, and final product are solely the responsibility of RAND, and do not reflect the policy or positions of any U.S. government department or agency.

The research reported here was completed February 2024 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Department of Defense, the Intelligence Community, and other interagency partners, and conducted within the International Security Defense Policy Program of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND International Security Defense Policy Program, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

For more information on this publication, visit www.rand.org/t/RRA2397-3.

www.rand.org

RR-A2397-3