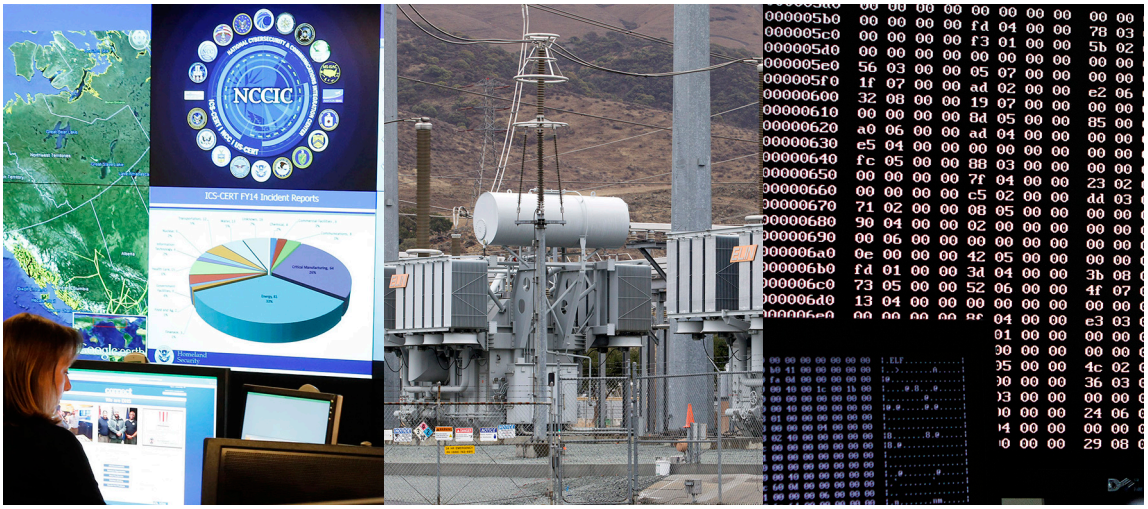
COUNCIL on FOREIGN RELATIONS

Center for Preventive Action



CONTINGENCY PLANNING MEMORANDUM NO. 31

A Cyberattack on the U.S. Power Grid

Robert K. Knake
April 2017

Author Bio

Robert K. Knake is the Whitney Shepardson senior fellow at the Council on Foreign Relations.

A Cyberattack on the U.S. Power Grid

INTRODUCTION

The U.S. power grid has long been considered a logical target for a major cyberattack. Besides the intrinsic importance of the power grid to a functioning U.S. society, all sixteen sectors of the U.S. economy deemed to make up the nation's critical infrastructure rely on electricity. Disabling or otherwise interfering with the power grid in a significant way could thus seriously harm the United States.

Carrying out a cyberattack that successfully disrupts grid operations would be extremely difficult but not impossible. Such an attack would require months of planning, significant resources, and a team with a broad range of expertise. Although cyberattacks by terrorist and criminal organizations cannot be ruled out, the capabilities necessary to mount a major operation against the U.S. power grid make potential state adversaries the principal threat.

Attacks on power grids are no longer a theoretical concern. In 2015, an attacker took down parts of a power grid in Ukraine. Although attribution was not definitive, geopolitical circumstances and forensic evidence suggest Russian involvement. A year later, Russian hackers targeted a transmission level substation, blacking out part of Kiev. In 2014, Admiral Michael Rogers, director of the National Security Agency, testified before the U.S. Congress that China and a few other countries likely had the capability to shut down the U.S. power grid. Iran, as an emergent cyber actor, could acquire such capability. Rapid digitization combined with low levels of investment in cybersecurity and a weak regulatory regime suggest that the U.S. power system is as vulnerable—if not more vulnerable—to a cyberattack as systems in other parts of the world.

An adversary with the capability to exploit vulnerabilities within the U.S. power grid might be motivated to carry out such an attack under a variety of circumstances. An attack on the power grid could be part of a coordinated military action, intended as a signaling mechanism during a crisis, or as a punitive measure in response to U.S. actions in some other arena. In each case, the United States should consider not only the potential damage and disruption caused by a cyberattack but also its broader effects on U.S. actions at the time it occurs. With respect to the former, a cyberattack could cause power losses in large portions of the United States that could last days in most places and up to several weeks in others. The economic costs would be substantial. As for the latter concern, the U.S. response or nonresponse could harm U.S. interests. Thus, the United States should take measures to prevent a cyberattack on its power grid and mitigate the potential harm should preventive efforts fail.

THE CONTINGENCY

The U.S. power system has evolved into a highly complex enterprise: 3,300 utilities that work together to deliver power through 200,000 miles of high-voltage transmission lines; 55,000 substations; and 5.5 million miles of distribution lines that bring power to millions of homes and businesses. Any of the system's principal elements—power generation, transmission, or distribution—could be targeted for

a cyberattack. In the Ukraine case, attackers targeted substations that lower transmission voltages for distribution to consumers. Lloyd's of London, an insurance underwriter, developed a plausible scenario for an attack on the Eastern Interconnection—one of the two major electrical grids in the continental United States—which services roughly half the country. The hypothetical attack targeted power generators to cause a blackout covering fifteen states and the District of Columbia, leaving ninety-three million people without power. Other experts have concluded that an attack on the system for transmitting power from generation to end consumers would have devastating consequences. In one scenario, disruption of just nine transformers could cause widespread outages. Many experts are now also concerned that smart grid technologies, which use the internet to connect to power meters and appliances, could allow an attacker to take over thousands—if not millions—of unprotected devices, preventing power from being delivered to end users.

Regardless of which part of the power grid is targeted, attackers would need to conduct extensive research, gain initial access to utility business networks (likely through spearphishing), work to move through the business networks to gain access to control systems, and then identify targeted systems and develop the capability to disable them. Such sophisticated actions would require extensive planning by an organization able to recruit and coordinate a team that has a broad set of capabilities and is willing to devote many months, if not years, to the effort. State actors, therefore, are the more likely perpetrators, and given these long lead times, U.S. adversaries have likely already begun this process in anticipation of conflict. It is doubtful that a terrorist organization would have both the intent and means to carry out such an attack successfully. In the future, however, criminal groups could pose a real threat. They are growing in sophistication and in some cases rival, if not exceed, the capabilities of nation states. Payments for ransomware—malicious software that encrypts data and will not provide a code to unlock it unless a ransom has been paid—by some estimates have topped $300 million. This funding could allow criminal groups to purchase more sophisticated capabilities to carry out the ultimate ransomware attack.

The likelihood that an attack carried out by a determined and capable adversary would be thwarted by security measures is low. While some U.S. utilities might block attempts by an adversary to gain initial access or might be able to detect an adversary in their systems, many might not have the necessary tools in place to detect and respond. Efforts to improve data sharing that could enable detection by one company to block access across the entire industry are in their infancy. In the Lloyd's scenario, only 10 percent of targeted generators needed to be taken down to cause a widespread blackout.

Short of outright conflict with a state adversary, several plausible scenarios in which the U.S. power grid would be subject to cyberattack need to be considered:

- *Discrediting Operations.* Given the importance of electricity to the daily lives of Americans, an adversary may see advantage in disrupting service to undermine public support for a U.S. administration at a politically sensitive time.
- *Distracting Operations.* A state contemplating a diplomatic or military initiative likely to be opposed by the United States could carry out a cyberattack against the U.S. power grid that would distract the attention of the U.S. government and disrupt or delay its response.
- *Retaliatory Operations.* In response to U.S. actions considered threatening by another state, such as the imposition of economic sanctions and various forms of political warfare, a cyberattack on the power grid could be carried out to punish the United States or intimidate it from taking further action with the implied threat of further damage.

There are many plausible circumstances in which states that possess the capability to conduct cyberattacks on the U.S. power grid—principally Russia and China, and potentially Iran and North Korea—could contemplate such action for the reasons elaborated above. However, considerable potential exists to miscalculate both the impact of a cyberattack on the U.S. grid and how the U.S. government might respond. Attacks could easily inflict much greater damage than intended, in good part because the many health and safety systems that depend on electricity could fail as well, resulting in widespread injuries and fatalities. Given the fragility of many industrial control systems, even reconnaissance activity risks accidentally causing harm. An adversary could also underestimate the ability of the United States to attribute the source of a cyberattack, with important implications for what happens thereafter. Thus, an adversary's expectations that it could attack the power grid anonymously and with impunity could be unfounded.

WARNING INDICATORS

A series of warning indicators would likely foretell a cyberattack on the U.S. power grid. Potential indicators could include smaller test-run attacks outside the United States on systems that are used in the United States; intelligence collection that indicates an adversary is conducting reconnaissance or is in the planning stages; deterioration in relations leading to escalatory steps such as increased intelligence operations, hostile rhetoric, and recurring threats; and increased probing of electric sector networks and/or the implementation of malware that is detected by more sophisticated utilities.

IMPLICATIONS FOR U.S. INTERESTS

A large-scale cyberattack on the U.S. power grid could inflict considerable damage. The 2003 Northeast Blackout left fifty million people without power for four days and caused economic losses between $4 billion and $10 billion. The Lloyd's scenario estimates economic costs of $243 billion and a small rise in death rates as health and safety systems fail. While darker scenarios envision scarcity of water and food, deterioration of sanitation, and a breakdown in security, leading to a societal collapse, it would be possible to mitigate the worst effects of the outage and have power restored to most areas within days. At this level of damage, the American public would likely demand a forceful response, which could reshape U.S. geopolitical interests for decades. Traditional military action, as opposed to a response in kind, would be likely.

In addition to the direct consequences of a cyberattack, how the United States responds also has implications for its management of the situation that may have prompted the attack in the first place, the state of relations with the apparent perpetrator, the perceived vulnerability of the United States, and the evolution of international norms on cyberwarfare.

How the U.S. government reacts, more than the actual harm done, will determine whether the cyberattack has a continuing impact on geopolitics. If the incident reveals a U.S. vulnerability in cyberspace that can be targeted to deter the United States from taking action abroad, the implications of the incident would be profound. If, on the other hand, the U.S. government shows firm resolve in the face of the attack and does not change its behavior in the interest of the attacker, the event is unlikely to have significant consequences for the role of the United States abroad.

On the domestic front, a highly disruptive attack would likely upend the model of private sector responsibility for cybersecurity. As was done with aviation security after 9/11, Congress would likely

move quickly to take over responsibility for protecting the grid from cyberattack by either creating a new agency or granting new authorities to an existing agency such as U.S. Cyber Command. Such a move would likely reduce the efficiency of grid operations and open the door to expanding government's role in protecting other sectors of the economy. A devastating attack might also prompt calls to create a national firewall, like China and other countries have, to inspect all traffic at national borders. However, the experience of other countries and the technical reality of the internet suggest that these firewalls are ineffective for cybersecurity but well suited to restricting speech online and censoring information.

PREVENTIVE OPTIONS

Preventing an attack will require improving the security of the power grid as well as creating a deterrence posture that would dissuade adversaries from attacking it. The goal of such a strategy should be to secure the power grid to make it defensible, to detect attempts to compromise the security of the grid, and to provide certainty to adversaries that the United States will be able to attribute the attack and respond accordingly.

Protective Measures. Unlike enterprise information technology, the industrial control systems that control the power grid typically perform single functions and need to communicate only with a small set of other devices in routine patterns. Thus, securing these systems and detecting malicious activity should, in theory, be relatively simple. In practice, many industrial control systems are built on general computing systems from a generation ago. They were not designed with security in mind and cannot be updated. This problem has not been corrected with the latest generation of smart grid technologies; the Government Accountability Office (GAO) has found that these devices often lack the ability to authenticate administrators and cannot maintain activity logs necessary for forensic analysis, among other deficiencies. These devices are often accessible from the public internet and use weak authentication mechanisms. Thus, improving the protection of the grid requires investing in new, more secure technology that can be protected and to implement basic cybersecurity hygiene. The challenge is, therefore, not to develop technical specifications to secure the grid but how to incentivize investment.

A regulatory approach could theoretically set a minimum standard, thereby leveling costs across all companies and addressing cost-cutting in security measures. Such a regimen—the Critical Infrastructure Protection Standards established by the North America Electric Reliability Council (NERC)—has been in place for over a decade, though GAO has found that many standards remain voluntary and the extent to which utilities have implemented these standards is unknown. Raising and enforcing standards could help prevent a catastrophic attack by encouraging utilities to proactively defend their networks. A model for such an approach could be borrowed from the nuclear sector, where the Nuclear Regulatory Council has established so-called Design Basis Threats and requires nuclear plant operators to prove that they have the controls in place to defeat such threats. Yet, given the thin margins on which utilities operate, such an unfunded mandate is not likely to meaningfully improve security. Moreover, current federal requirements do not extend to power distribution, which is regulated unevenly at the state level.

As regulated entities with fees set by control boards, utilities do not have sufficient budgets to significantly increase security funding. Risk managers at utilities will argue that they must balance the possibility of a cyberattack against the near certainty that weather events will affect their customers. A

decision to increase spending on cybersecurity could come at the expense of burying power lines, raising them above the tree line, or trimming trees along the lines. In 2016, the Department of Energy (DOE) received only three reports of cyber incidents at utilities; none of the incidents affected customers. In the same time period, forty-one weather events caused outages, affecting 5.2 million customers. Numbers for 2015 show a similar pattern. Thus, some form of rate relief is needed to encourage significant investments in cybersecurity.

More could also be done to improve government support for securing electric utilities. The DOE has run a pilot program, known as the Cybersecurity Risk Information Sharing Program (CRISP), for several years to help companies detect advanced threats targeting their networks. DOE labs have also funded research projects on the specific cybersecurity needs of utilities. Yet critics of the program argue that it is too expensive for most utilities to participate in and that it is only focused on detecting threats at network boundaries rather than within ICS networks. Expansion of intelligence and data sharing between the government and private companies, and among private companies themselves, could greatly reduce the chances of an attacker being capable of taking down multiple targets and causing a cascading effect. The Electricity Information Sharing and Analysis Center (E-ISAC) is mostly focused on physical threats and weather events. GAO found cybersecurity information sharing weak across the sector. Sectors such as finance and the defense industrial base have developed strong information sharing practices with government support. Emulating these efforts in the electricity sector would be a valuable government contribution to help owners and operators in the industry protect themselves.

Given the large number of utilities and the vast infrastructure to protect, even with improved cybersecurity, an adversary would still be likely to find numerous unprotected systems that can be disrupted. As the Lloyd's analysis concluded, only 10 percent of targeted generators needed to be taken offline to cause widespread harm. Therefore, improving the security of individual utilities alone is unlikely to significantly deter attackers. By focusing on detecting early signs of an attack and sharing that information within the sector and with the government, even when individual utilities fail to detect attacks on themselves, they can warn the government and other companies and help prevent wider disruption.

Deterrent Measures. Adversaries may underestimate both the ability of the U.S. government to determine who carried out an attack and the seriousness with which such an attack would be addressed. Law enforcement agencies such as the Federal Bureau of Investigation (FBI) and the U.S. Secret Service have built strong forensic investigation capabilities and strong relationships with both foreign law enforcement and the intelligence community. Through cooperation, the U.S. government has been able to determine the parties behind most major attacks. The Barack Obama administration publicly named the foreign actors behind some attacks and provided supporting evidence on a case-by-case basis. Making public attribution of attacks a routine practice could be a deterrent.

Beyond simply naming the adversary behind attacks, the U.S. government could make clear how it would view an attack on the power grid and the kinds of responses it would consider. Characterizing an attack on the power grid as an armed attack would likely have the strongest deterrent effect. Doing so would reflect the developing norms against peacetime attacks on critical infrastructure as agreed to in the UN Group of Governmental Experts. In keeping with these norms, the U.S. government could outline response options that would be proportional but not necessarily in kind. These response options would clarify how the U.S. government would respond not only to a successful attack but also to a failed attempt and to the discovery of adversarial probing and exploration to prepare for an attack.

In developing its policy, the U.S. government should keep in mind that a strong policy against targeting U.S. systems could constrain U.S. military options to target foreign systems. Yet, given the long lead times for carrying out a successful cyberattack campaign, labeling reconnaissance activities as hostile actions and limiting such activities by U.S. cyber operators could mean forgoing the ability to make significant use of cyber operations during a conflict.

MITIGATING OPTIONS

If an attack on the grid cannot be prevented, steps can be taken now to mitigate the effects of the attack and plan the response.

Pre-Attack Measures. Actions taken now could significantly mitigate the effects of a large-scale blackout caused by a cyberattack. Maintaining and exercising manual operations of the grid, planning and exercising recovery operations, and continually expanding distributed power could significantly shorten the duration of any blackout and reduce economic and societal damage.

A SANS Institute report concluded that the effects of the attack on Ukraine's power grid were largely mitigated because grid operations there could be returned to manual control. Most experts believe that the current complexity of grid operations in the United States would make a switch to manual operations difficult; newer systems might not allow for the use of manual controls at all. Requiring the ability to shift to manual controls and exercising those controls on an annual basis might now be the most valuable step to take. Michael Assante, the former chief information security officer for NERC, argues that utilities should design their systems with backup tools that are either not connected to any information technology networks or are analog. For certain pieces of technology, it may make sense to replace software systems with hardware systems, "hardwiring" functions into circuit boards so that they cannot be modified remotely.

The next administrator of the Federal Emergency Management Agency (FEMA) could make response and recovery planning a priority. The all-hazards approach favored in emergency management may prove insufficient for a blackout of long duration covering large swaths of the nation. Beyond domestic emergency planning, exercising crisis response at a national level with government, allies, and private sector actors would be valuable. Doing so would identify the difficulties of operating without power systems and prompt the development of response options to prevent unneeded delay.

The continued expansion of distributed generation in the form of wind and solar installations could also significantly reduce the magnitude of an attack on the grid; however, most rooftop systems feed directly into the grid, and homes and businesses do not draw from their own systems. From a resiliency perspective, it might be worth incentivizing the purchase of systems that allow a direct draw and have on-site storage. Moving military installations in the continental United States off the grid so that they can supply their own power would eliminate one of the rationales for attacking the grid and limit the hindrance caused by such an attack on military operations.

Post-Attack Measures. Following an attack, eliminating malware and regaining control of the power grid would likely be carried out by the owners and the operators of affected systems with support from private incident response teams. Specialized support from the Department of Homeland Security's Industrial Control System Computer Emergency Response Team (ICS-CERT) and the DOE national labs would also be provided.

The government's main role would be attributing the attack and responding to it. The FBI would take lead responsibility for investigating the attack domestically and for conducting computer forensics. The intelligence community would look at its existing intelligence collection for indications of what might have been missed and would begin targeted collection efforts to trace the attack. Within weeks, the U.S. government would have confidence in its attribution.

The White House would set the public posture for the response. Based on precedents from both cyber- and non-cyberattacks over multiple administrations, government agencies would likely advocate for a show of firm resolve but recommend avoiding a rush to judgment or an immediate counterattack. Agencies would present a range of options to respond. These options would include a show of military force, such as moving U.S. ships into disputed waters or staging exercises in contested regions; response in kind, through cyberspace; traditional military options; public and private diplomacy; use of economic sanctions targeting the state and the private entities or individuals involved; use of international law enforcement to arrest any parties involved; and targeting of known intelligence assets. The president should choose a strategy that combines these options in such a way as to deter the adversary from escalating further—the adversary should recognize that the consequences of continued escalation will be severe and choose to cease hostile activity, allowing a reset of the relationship.

RECOMMENDATIONS

The Donald J. Trump administration should focus its efforts on preventing an attack on the grid both through a deterrence policy and by strengthening security. The deterrence policy should articulate how the administration would view an attack on the power grid and should outline possible response options. As a starting point, the administration should be clear that an action against the grid would be treated as an armed attack and signal that a military response in or out of cyberspace would likely be required. The policy should also address how the administration would view the discovery that an adversary had taken initial steps toward a takedown of the grid, particularly the discovery that foreign actors had infiltrated utility networks. Together with continually demonstrating law enforcement and intelligence capabilities to attribute the sources of cyberattacks, a strong statement on deterrence could do more than anything else to prevent an attack on the grid. To ensure that the United States will be able to maintain military operations even in the face of a large blackout, the Trump administration should plan to end the reliance of military installations on the grid. Doing so would also reduce the likelihood of the grid becoming a military target.

To protect the grid from cyberattack, the Trump administration should initially focus on creating an information-sharing system that can bring together early signals that an attack against the grid is under way and share information that can be used to stop it. A stronger E-ISAC and a strong DOE counterpart to support it are necessary. The DOE should model its efforts on the Department of Defense's Cyber Crime Center, which provides intelligence feeds and forensic support to companies within the defense industrial base. The newly created Cyber Threat Intelligence Integration Center within the Office of the Director of National Intelligence should ensure that collection and analysis of threats to the grid are an intelligence priority and that intelligence on threats to the grid are downgraded and shared with targeted utilities.

In the event that an attack on the grid succeeds in causing blackout to some extent, the Trump administration should ensure that both the government and the industry are prepared to respond. FEMA

should develop a response plan for a prolonged regional blackout that addresses the logistical difficulties of responding at scale in an environment degraded by the loss of power. NERC standards should require companies to maintain capabilities for manual operations. Those operations need to be exercised on a regional and coordinated basis.

Finally, the Trump administration should ensure that utilities can invest sufficiently in cybersecurity and do not need to make tradeoffs between traditional risk management activities and addressing national security threats. Increased funding could be achieved through a user fee similar to the universal service fee on phone lines, though a new tax on consumers may not be politically feasible. Alternatively, a tax deduction for utility spending on cybersecurity may be a less direct—but more politically palatable—way to increase funding. The Trump administration should also set security requirements for infrastructure investments made for the grid as part of its proposed stimulus package.

Collectively, these recommendations, if implemented, would greatly reduce the likelihood of an adversary deciding to conduct a cyberattack on the U.S. power grid while also improving the chances that the United States would manage any such attack without significant disruption of service.

The Center for Preventive Action (CPA) seeks to help prevent, defuse, or resolve deadly conflicts around the world and to expand the body of knowledge on conflict prevention. The CPA Contingency Roundtable and Memoranda series seek to organize focused discussions on plausible short- to medium-term contingencies that could seriously threaten U.S. interests. Contingency meeting topics range from specific states or regions of concern to more thematic issues and draw on the expertise of government and nongovernment experts.

The Council on Foreign Relations acknowledges the Rockefeller Brothers Fund for its generous support of the Contingency Planning Roundtables and Memoranda.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.