Power Grids and Plumbing: The Link Between Irregular Warfare and National Critical Functions

Description

Zachary Kallenborn

On December 5, 2022, unknown shooters attacked two power substations in Moore County, North Carolina. Over 30,000 people lost power for days. Today, responding to power loss means far more than just lighting candles and winding up the hand-crank flashlight. In an increasingly cashless society, no power also means no access to the internet for payment processing. Tasks like purchasing food, paying bills, getting supplies, and refilling medications are also harder. In an increasingly remote work society, no power also means employees may lose computer, laptop, and internet access. Electrical power is a critical function of society on which numerous other critical functions depend.

The Department of Homeland Securityâ??s Cybersecurity and Infrastructure Security Agency identifies 55 such National Critical Functions, or NCFs. These are â??functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.â?• The NCF Framework is intended to focus critical infrastructure risk analysis on the functions specific infrastructure assets provide to the broader infrastructure system. This allows for more precise understanding of infrastructure vulnerabilities, interdependencies, and chokepoints that could create national-level harms. The aim is to provide more systematic and robust assessments of critical infrastructure risk, recognizing that infrastructure is interconnected.

The irregular warfare community could use the NCF framework to generate actionable insights on the complexity and interconnectivity of critical infrastructure. A better understanding of critical infrastructure could enable more targeted sabotage operations and more effective asymmetric strikes, while helping to generate more impactful civil resistances and support partner forces and governments in protecting infrastructure from such attacks. More generally, the irregular warfare community should build and expand relationships with the critical infrastructure community, because protecting American critical infrastructure is not drastically different than protecting allied infrastructure. And better understanding how critical infrastructure operates and functions can be of great value in disrupting adversary infrastructure.

Value of the National Critical Functions

If Americaâ??s goal is to protect a government against insurgency, itâ??s useful to know how best to ensure that lights stay on, water runs, and food gets to the table. If Americaâ??s goal is to support an insurgency, itâ??s useful to know how best to switch all that off. The National Critical Functions framework enables both.

Each of the 55 NCFs break into sub-functions, sub-sub-functions, and contributing assets and components. For example, the NCF â??Supply Waterâ?• could be divided into sub-functions like treat water, store water, and transport water. Specific facilities and assets enable each sub-function: a water treatment facility treats the water; a water tower stores it; and pipelines transport the water to the home. Although countries will perform each function differently, they still must perform the function. During times of drought in Mexico, for instance, water trucks called â??pipasâ?• may be the only way to get water. Water still must get to peopleâ??s homes somehow. IW practitioners could readily take the function and sub-function breakdown and map them against the specifics in their area of operation.

Critical infrastructure deep dives would also improve understanding of vulnerabilities. The critical infrastructure system is complex and dynamic. Numerous facilities, assets, processes, and personnel are linked together to provide needed services across a country. The electric grid needs not only power plants, but also substations, transmission stations, and distribution systems. Each element also requires maintenance, billing systems, control software, and personnel to operate. Personnel also need to get to work, eat, drink, and sleep. All of those operate in a larger legal and regulatory framework.

Carefully characterizing those systems and their dependencies can help identify critical chokepoints at which small disruptions can yield big bangs. For example, in 2020 a simple distributed denial of service attack on the New Zealand Exchange halted trading on the countryâ??s financial markets for four days. The attack breached no critical data. All that happened was the website went down. However, New Zealand financial regulations require public posting of market announcements. No announcements, no trading. So, no website, no stock exchange. Knowing that vulnerability requires understanding dependencies on which the countryâ??s financial sector relies.

A complete rendering of critical infrastructure also may highlight unexpected opportunities for malfeasance. As a former colleague liked to say, â??we never think about our shit.â?• Literally. Plumbing is a basic staple of modern society. Folks can just flush their waste away. If the toilets donâ??t work, life is foul smells, physical discomfort, and overall misery. If oneâ??s goal is to destabilize an adversary authoritarian regime, attacking water treatment plants, and encouraging plumber strikes certainly could encourage discontent. Conversely, if the American goal is to counter an insurgency, protecting the basics is a good idea too.

Better characterizing critical infrastructure can guide security assistance to appropriately protect partner infrastructure. The United States might observe that desalination plants are particularly critical to the Middle East, where 70% of desalination plants reside worldwide. American forces could assess current and future threats to the plants, and provide appropriate training, equipment, and other support to physical and cyber security forces protecting them.

Of course, critical infrastructure sectors are also deeply interconnected. During World War II, allied forces targeted German ball-bearing factories because tanks, airplanes, machine guns, submarines, and heavy artillery all needed them. The NCF Framework identifies interconnections, and, as a result, such critical vulnerabilities. For example, the same computer operating systems support most NCFs, so vulnerabilities in the operating system generate vulnerabilities across the entire infrastructure landscape. Likewise, treating the NCFs and their sub-functions as a directed network allows network analysis to identify, and analyze common functional dependencies that could result in cascading consequences if a risk manifests.

Furthermore, special warfare operators may not seek to sabotage or target a critical chokepoint, but simply to signal that they can. Special warfare operators might deep-dive into a countryâ??s critical functions to identify areas of geographically concentrated risk. That is, relatively small geographic areas that have numerous assets, systems, or personnel critical to one or more NCF. Special warfare operators might discover that a particular city in China has a high concentration of chemical production facilities critical to commercial and defense manufacturing in an area near a major port. Non-harmful special warfare activities in the area could signal to China that the United States is aware of this vulnerability and, if conflict breaks out, is prepared to target the area with cyberattacks on the common power grid, sabotage operations against any of the targets in the area, or, in the event of a major war, bombings and other kinetic attacks.

Next Steps

To take advantage of the opportunities the NCF framework provides, the IW community should engage with Cyberspace and Infrastructure Security Agency (CISA) and the National Risk Management Center. Engagement will help better understand the NCF Framework, and how NCF analysis can support their goals. As a starting point, researchers and analysts in the irregular warfare and special operations community should reach out to CISA to request a briefing on the NCF Framework, sharing of any NCF-based risk analysis products, or perhaps observe the process and tools that generate NCF-related risk analysis, such as the Suite of Tools for the Analysis of Risk. Researchers and analysts should look at how the NCF Framework can complement or supplement existing infrastructure analysis frameworks. For example, the NCF Framework could support CARVER-based analysis by helping identify critical systems, identify system-level vulnerabilities, and better assess and anticipate effects. Those insights could be incorporated into Naval Postgraduate School coursework on critical infrastructure protection, advanced courses at the U.S. Armyâ??s Special Warfare Center and School, and Joint Special Operations University courses on national resistance, cyberspace, or operational design.

Critical infrastructure assets do not exist on their own; they support a delicate, interconnected system of functions. Shifting to a functional approach to critical infrastructure analysis can help the irregular warfare community better characterize and understand how critical infrastructure operates, depends on one another, and how sabotage or attacks can generate cascading consequences.

Zachary Kallenborn is an adjunct fellow (Non-resident) with the Center for Strategic and International Studies (CSIS), Policy Fellow at the Schar School of Policy and Government, Fellow at the National Institute for Deterrence Studies, Research Affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), an officially proclaimed U.S. Army â??Mad Scientist,â?• and national security consultant.

(Note: the author was contract support to the NCF team at CISA from 2019 to 2023, and the views expressed here do not necessarily reflect the views of CISA)

Main image: Officials from Congress, the U.S. Army and Nolin RECC wait as the power stations begin the power-down process prior to Louisville Gas & Electric cutting off power to the Fort Knox grid Oct. 24, 2018. (US Army)

Date Created
2023/07/12