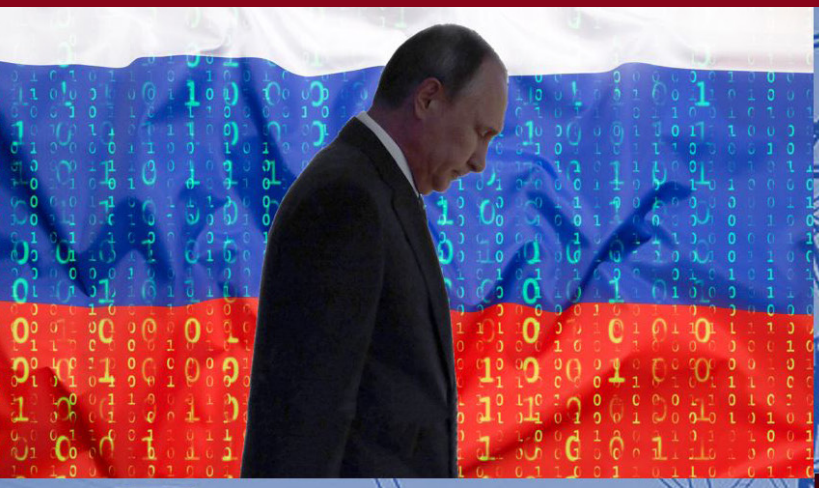
CENTER
FOR SECURITY POLICY

FEBRUARY 2022

As Russia/Ukraine Situation Raises Specter Of Cyberwar, How Can We Be Better Prepared Here At Home?

BY TOMMY WALLER



As Russia/Ukraine Situation Raises Specter Of Cyberwar, How Can We Be Better Prepared Here At Home?

BY TOMMY WALLER

President Biden told reporters this week that "every indication we have is they are prepared to go into Ukraine, attack Ukraine." Biden's words echo a narrative about "imminent invasion" that has dominated headlines, with more than 500 English-language publications discussing the matter over the last four months. Other experienced national security experts have expressed skepticism, saying the invasion narrative doesn't fit with Russian president Vladimir Putin's larger strategy, and warn the threats may be intended as an information operation seeking to divide western political leaders.

What we do know for certain is that major Russian military action is often preceded by a series of significant cyberwarfare attacks against critical infrastructure. This was the case in Georgia in 2008, and when Russia moved against Ukraine in Crimea in 2014, and again against Ukraine in 2015. While some downplay the military usefulness of such cyber "shock and awe" campaigns, they can prove extremely disruptive for civilians and unprepared national or regional governments.

In the lead up to the current crisis, major oil terminals throughout European ports were targeted for cyber-attack. The flow of oil into U.S. NATO allies, particularly Germany, is a major strategic factor related to the Russia-Ukraine conflict. Bank regulators in Europe and the U.S. also issued warnings of cyber threats against financial institutions. In January, The Department of Homeland Security (DHS) issued a bulletin to critical infrastructure operators and state and local governments warning "Russia maintains a range of offensive cyber tools that it could employ against U.S. networks" with possible targets including hospitals, dams, bridges and other major systems.

That said, whatever the Kremlin has up its sleeve for the Ukraine, it seems unlikely that the Russians would unleash a broader cyber campaign against *local* targets in the United States, absent some kind of major escalation of the conflict. Yet it remains vital that local law enforcement, emergency managers, and critical infrastructure owners realize three things: (1) that in the age of cyberwarfare, national security issues thousands of miles away can rapidly come to

affect them closer to home, (2) that the Russians have effectively targeted our *electric grid* and that it *remains critically vulnerable*, and (3) that a major escalation of conflict between Russia and the U.S. could trigger the Russians to exploit these vulnerabilities in the grid – potentially causing widespread and long term blackouts inside the United States.

Our "shields" are down

The Department of Homeland Security divides up critical infrastructure into 16 "sectors" each of which is vital to maintaining our complex modern infrastructure system and way of life. In a recent announcement by DHS, the Cybersecurity Infrastructure Agency (CISA) declared that all critical infrastructure owners should adopt a "Shields Up" policy in preparation for potential Russian cyber-intrusions. While we have seen Russian hackers successfully target infrastructures ranging from pipelines to food production, CISA referenced "power and communications" infrastructure, as specific infrastructure targets. There is a reason for this: *all other critical infrastructures rely on electric power and communications to function. And, all our adversaries, most especially the Russians, know this.*

There is ample reason to believe that this warning comes too late, as the Russians are already inside our "shields."

An experienced cyber analyst recently warned that "the 2015 Ukrainian Grid event was a test of malware intended for use in the US." The 2015 event, in which 230,000 Ukrainians lost power for the better part of a week, could have been even more severe. Had the Russians successfully created the "aurora condition" in the over 30 electric Ukrainian substations they attacked – major utility assets could have been permanently damaged, blacking out the country for months or even years.

Unfortunately, the Russians have infected the U.S. electric grid with the same malware used to take down the Ukrainian grid. Despite years' worth of warnings and even official complaints levied with the grid's federal regulators, there is still *no requirement* to detect, mitigate, or remove that malware. And, despite consistent prompting from national security experts, engineers, and even powerful lawmakers, the utility industry has done almost everything possible to avoid taking steps to protect against the potentially catastrophic aurora threat.

In fact, to this day, there are no mandatory cybersecurity standards for real-time Grid operations, despite years-worth of warnings by some of the most experienced and credible cybersecurity experts in the world. One such expert, former National Security Agency (NSA) Chief Information Officer (CIO) George Cotter revealed the following in a letter to federal regulators on September 6, 2019:

> "The electric grid, generation, distribution and nuclear utilities, have been subject to deep technical reconnaissance since at least 2008 by the Russian Federation, including direct unexplained coupling of those incursions since at least 2004, to attacks on the US Election System… Massive systemic flaws in Grid security have been deliberately hidden, a security industry that surely knows better has been effectively gagged, oversight federal departments (DoE, DHS) have all but disgraced themselves in shying away from this existential threat to the nation."

Cotter makes clear in his letter that the government and industry's claim that the bulk power system "hasn't suffered any outage" due to cyberattack is "totally due to Russian restraint" not industry action. The current Secretary of Energy, Jennifer Granholm seemed to reinforce this realization in a June 6, 2021 interview on CNN where she admitted that adversaries do indeed have capability of shutting down the US power grid.

Finally, it is important to remember that electric utilities share many forms of infrastructure with the telecommunications sector and that communications are required for utilities to both operate the grid and to restore power after a blackout. Given this interdependency, telecommunications are also a target for our adversaries and downed communications would exacerbate an attack on the grid (even if the adversary didn't originally target telecom infrastructure). (Hence DHS's priority on these infrastructures adopting the "shields up" approach to cybersecurity.)

What can we do?

Our grid is vulnerable to Russian cyberattacks and neither the federal government nor the utility industry is moving fast enough to defend it. What, then, can be done at the local level by those who have a duty to serve and protect the people? At a minimum, we can immediately focus on preparedness in three areas: professional networking, back-up power, and communications.

Given the vulnerabilities of the electric grid and its interdependency with the telecommunications sector, local planners should immediately focus efforts to protect both infrastructures and have back-ups to use if they fail.

Fortunately, the Department of Homeland Security's Cyber Infrastructure Security Agency (CISA) formed a working group to assist in this effort. This Resilient Power Working Group (RPWG) consists of members from across numerous federal agencies (including DoD, DHS, FEMA, DOE and numerous DOE labs), state and local governments, non-profits, and private industry and the group been working on a comprehensive "Resilient Power Best Practices for Critical Communications Infrastructure." While the full document is not yet ready for public release, there *are* steps that local planners can do to begin incorporating some of those best practices:

Professional Networking:

First, local planners should find and join appropriate sector/geographically based information sharing organizations such as InfraGard, the National Council of ISACs and preparedness networks, including local Community Emergency Response Teams (CERTs). Local planners should also network with nearby National Guard units, especially cybersecurity personnel, and leverage the CISA Protective Security Advisor (PSA) Program, which can help conduct voluntary security surveys and assessments on critical infrastructure assets and facilities. These groups and programs are often full of professionals from many different areas that have a passion for security and resilience, possess experience in both areas, and often have a sworn duty to serve and protect the community.

Images: Screenshots from infragard.org, nationalisacs.org, and cisa.gov

---

Similarly, planners should form a tight working relationship with both the executives and the "on-the-ground" operators of their local electric utilities and telecommunications providers both for information sharing and for the intangible benefit this brings during a disaster. This "intangible benefit" may be hard to define in words, but it won't be hard to recognize when it's needed.

When law enforcement, emergency planners, CERT members, and utility operators know each other and can recognize the challenges and the interdependencies of each profession, they can coordinate better than with those they've never met. Conducting joint preparedness exercises is also a great way to "stress test" these relationships and establish the necessary camaraderie.

Two examples of these types of partnerships have been established in the state of Louisiana and they both serve as great examples for the rest of the nation:

- The first is the InfraGard Louisiana Member's Alliance which has been nationally recognized among 77 chapters, is home to one of the largest U.S. Coast Guard Facility Security Officer (FSO) / Port Security Working groups in the country, and hosts some of the largest security exercises in the State of Louisiana.

- The second is the New Orleans Regional Planning Commission's Emergency Preparedness Public-Private Partnership (EPP) which is comprised of 250 organizations, agencies, and individual businesses that support Emergency Preparedness in Southeast Louisiana and South Mississippi. It focuses on building resilience and continuity of operations in its members, by adapting lessons learned and best practices from local and nationally-recognized experts.

Do your employees know how to manually start your source of backup power? Do they have what they need to run and maintain it for a long-term power outage?

Image: Adobe Stock

Basic Back Up Power Preparedness:

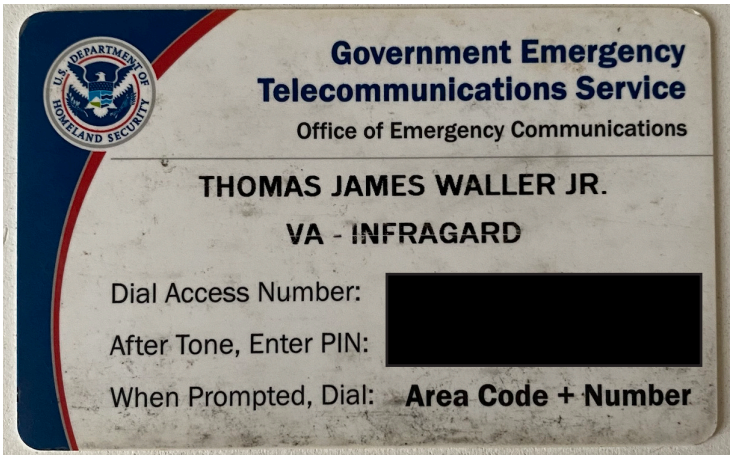
As described in the recently published "fact sheet" from DHS CISA about the forthcoming "Resilient Power Best Practices," local planners should first identify the criticality of their role as an infrastructure owner/operator or public service and then subsequently determine the "level of resilience" needed – with a level 1 being the lowest and level 4 being the highest. Regardless of level, there are some basic principles planners should immediately embrace to plan for back-up power.

First, they should identify the critical electric loads they need for basic operations and during a disaster and maintain a minimum of one backup source electric power generation (two if possible) for those critical loads. Some examples of these critical loads are power to communications infrastructure, critical refrigeration, water/wastewater, and safety/security systems. These backup generators should be regularly maintained, and load tested, and sufficient spare parts and maintenance parts (such as oil/air/fuel filters, hose clamps, spark plugs, etc.) should be stored on site. Regardless of the fuel source, a sufficient amount of fuel should be stored onsite if possible and if the fuel is gasoline or diesel, it should be maintained and rotated properly. Regardless of fuel type, planners should regularly assess fuel delivery contracts and explore/document/test emergency delivery alternatives.

Because employment and maintenance procedures of backup power systems often falls on only one or two individuals (such as facility maintenance or engineer personnel), planners should incorporate training of other employees. Additionally, many back-up power systems rely on an "automatic transfer switch" (ATS) to turn on the generator system – which can be a real convenience during an unpredicted blackout. However, if an ATS fails, employees may not know how to manually turn on the generator. Therefore, planners should publish step by step instructions (ideally with photos) for power shut down and startup and ATS bypass procedures and have employees rehearse these routinely.

FIRSTNET®
Built with AT&T

Source: FirstNet.gov



The author's well-worn and used GETS Card, designating his membership in InfraGard

---

Additionally, if generator-power is necessary 24/7 during an emergency, planners should ensure that engineers/operators create and test a means to bypass and isolate any component for repair or replacement without deenergizing critical loads (another reason why more than one source of backup power is often needed) and publish these instructions for other team members to execute in their absence.

Basic Communications Preparedness:

Depending on the mission of a local public service or critical infrastructure owner/operator, there will be a wide range of communications requirements. The internet and cellular data capabilities associated with modern telecommunications have created immense capabilities for both rapid and highly detailed (ie. photographic and video) communications. Unfortunately, these systems can be easily overwhelmed by high call volumes and low bandwidths in a disaster.

Thankfully, DHS CISA has an entire team devoted to emergency communications and, in collaboration with the Federal Communications Commission (FCC), have developed a series of priority services to "support national security and emergency preparedness communications for government officials, emergency responders, critical infrastructure personnel, and industry members." These services include the following:

- The First Responder Network Authority (FirstNet) cellular service managed by AT&T is "the first nationwide network dedicated to public to help law enforcement, fire service, and EMS do their jobs safely and effectively." [FirstNet is only available to "Primary Users" and "Extended Primary Users" that respond to emergencies/incidents so not all local planners/infrastructure owners will qualify for access.]

- The Government Emergency Telecommunications Service (GETS), which does not require special phone equipment but instead gives users a "GETS card" and Personal Identification Number (PIN) that can enable them to get prioritization over "old school" wireline telephone networks.

- The Wireless Priority Service (WPS) program is an "ad-on" feature for mobile devices that gives users priority access over cellular communications networks. They merely dial *272 on a WPS enabled device to receive calling queue priority (without preempting other calls already in progress).

Top Image: Hurricane/Tropical Storm - Biloxi, Miss. , July 23, 2009 --Darrin Ivey, emergency management team lead for Biloxi Regional Hospital, demonstrates how to use a HAM radio. The hospital acquired the radios after Hurricane Katrina to improve communications for future storms. Jennifer Smits/FEMA.

Bottom Image: [Hurricane Katrina] New Orleans, LA, September 16, 2005 -- FEMA Urban Search and Rescue workers set up a repeater to be used for communications in areas impacted by Hurricane Katrina. Jocelyn Augustino/FEMA

- The Telecommunications Service Priority (TSP) program that gives "preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause."

Unfortunately, because the above services still rely on commercial telecommunications infrastructure they are completely dependent upon electricity, and thus vulnerable. As such, planners should assume that a cyber-induced blackout will take down internet and cell networks and thus they should deploy diversity in their communications plan (i.e., cellular, satellite, landline, high frequency [HF] radio), following the PACE model (Primary, Alternate, Contingency, and Emergency).

DHS CISA has a program for those seeking back-up communications using HF Radio: the "SHAred RESources (SHARES) High Frequency (HF) Radio program." SHARES members "use existing HF radio resources to coordinate and transmit messages needed to perform critical functions, including those areas related to leadership, safety, maintenance of law and order, finance, and public health."

This means that a local agency needs to procure its own radio equipment but that it can then plug into "more than 2,400 HF radio stations, representing over 400 Federal, State, County, and Industry organizations located in all 50 states, the District of Columbia, and several locations overseas" that are resource contributors to the SHARES HF Radio Program.

To augment SHARES, and especially at the very local level, planners can and should also coordinate with local amateur radio emergency communications users (also known as "HAM" radio operators and radio clubs). Planners should identify certain of their own personnel to license as radio operators and train them how to operate this equipment without the convenience of everyday electric power and cellular communications.

In one example, a Sheriff's department in Texas ordered all deputies to be trained and licensed as HAM radio operators prior to Hurricane Harvey. That decision paid off when the law enforcement communications networks went down in the wake of that natural disaster.

Conclusion: Prepare *Prior* To The Disaster

Given the growing threats to our critical infrastructures, the unfortunately persistent vulnerabilities of these infrastructures, and the ever-increasing dependence of our society on them, it is critically important that local officials develop personal relationships, conduct information sharing and conduct preparedness planning and training *prior* to a power and/or communications outage, regardless of the cause. It is also worth noting that cyber-attacks can have major downstream consequences. As we saw in the case of the Colonial Pipeline hack, multiple states were affected and forced to declare a state of emergency as cascading effects impacted even areas where the critical infrastructure itself was not based. That was but a small example of what the Russians can do in cyberspace.

While we can't know for sure how the latest Russia-Ukraine tensions will play out this time, emergency planners can't assume they will have advanced warning to "raise their shields." Instead, prepare now for the reality that America's adversaries abroad can use cyber capabilities to bring conflicts to the Homeland. We mustn't rely solely on our opponent's "restraint" to keep the lights on.

Author's Note:

I acknowledge that a prolonged and widespread blackout will present many more challenges for planners, and for society, than just those associated with backup power and communications. Considerations must be made in many other areas ranging from security to water, to sewage/ wastewater, to food, etc. depending on the duration of the outage and these considerations should also include the families and dependents of the local first responders and utility operators who will be busy managing the disaster. Those considerations are beyond the scope of this short report but are no less important. This all underscores the need for America to SECURE THE GRID against all hazards. To learn more about what the Center for Security Policy is doing in that area, visit www.SecureTheGrid.com and consider joining our Secure The Grid Coalition.

CENTER
FOR SECURITY POLICY

Cover image credit: Arseniy Shemyakin Photo / Shutterstock.com (modified)

This report was produced by the Center for Security Policy, a nonprofit, nonpartisan 501(c)(3) institution focusing on national security policy issues.

It was made possible by generous contributions from the Center for Security Policy's supporters. All views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).