

Cyberwar is What States Make of It^[1]

Dr. Martin Libicki

No one there at the time could forget the vicious cyberattack on Venezuela's power systems in March 2019. Four days of chaos ensued. Stores and restaurants closed. Card payments systems were down, with customers asked to pay in dollars. Disrupted public transportation left many unable to get to work. Looting ensued. Seventeen people died in hospitals for lack of electricity.^[2]

Wait, some of you may be thinking: *what* cyberattack? There is no question that Venezuela's grid had serious problems, but the only evidence that a cyberattack caused these problems was the word of President Maduro. He certainly had political reasons to mobilize his supporters against yet another delivered insult by the US, which has made no secret of its desire to see Maduro go.^[3] More likely, the power outage reflected the same dysfunctional energy facilities that reduced the average daily oil production rate from nearly 2.5 million barrels in 2015, to a third of that in 2019.

Brazil can tell a similar tale of woe. In 2007, hackers attacked the grid of the state of Rio Grande do Sul, causing severe power outages. The CIA picked up and circulated this story within the intelligence community for two years before it was broadcast by *Sixty Minutes* in 2009.^[4] Or was it a cyberattack? Once it was reported in the press, Brazil's government denied any such cyberattack, claiming the cause to be sooty insulators, resulting in a fine assessed against the relevant utility.^[5] So, end of the story? Not necessarily, argue two of the savvier observers on the cyberwar scene (one American and one Israeli); there were known groups that had both an interest in, and a talent for cyberspace mischief, and the government of Brazil would have been embarrassed to admit their success.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



Dr. Martin C. Libicki (Ph.D., U.C. Berkeley 1978) is the MaryEllen and Richard Keyser Chair of Cybersecurity at the U.S. Naval Academy where he teaches cyberwar strategy and cyberspace economics. Prior employment includes having been a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. He wrote three commercially published books: *Cyberspace in Peace and War* (2016, second edition forthcoming), *Conquest in Cyberspace: National Security and Information Warfare* (2007), and *Information Technology Standards* (1994). He is also the author of numerous RAND monographs, notably *Defender's Dilemma*, *Brandishing Cyberattack Capabilities*, *Crisis and Escalation in Cyberspace*, *Global Demographic Change and its Implications for Military Power*, *Cyberdeterrence and Cyberwar*, *How Insurgencies End* (with Ben Connable), and *How Terrorist Groups End* (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

If attacks on the power grid can be faked or hidden, imagine what can be done with other mischief in cyberspace. Cyber-espionage can go undetected for years. Withdrawals from bank accounts can be covered by funds transfers from the embarrassed bank (albeit not legally in many countries). Induced failures in police or intelligence systems may not make the news if such systems are themselves unknown to the public. By contrast, there is no hiding when it is the lights that go out. Nevertheless, the *fact* of a power outage does not prove that a cyberattack caused it—and, while the power company might know, they may not say or be encouraged or even allowed to speak. And, even if a cyberattack is established, attribution can still be an issue.

So far, the only verified cases of electric power loss caused by hacking occurred in Ukraine: two separate incidents in late 2015 and late 2016. But just as the existence of nuclear weapons—even though none have been detonated in war since 1945—has dramatically influenced the security choices of the US, Russia, and China, an imminent threat to knockout electric power could shape future crises. Targeted countries could be coerced or alternatively, they could try to pre-empt attackers by doing likewise. The most frequently discussed way to convert the threat to the electric grid from a notional to a real possibility is to implant malware into the other side's industrial control systems (as distinct from their office and billing systems). Such implants have been likened to Soviet moves to put intermediate-range nuclear-tipped missiles in Cuba, thereby tripling their capacity to strike the US.

So, have countries implanted malware in other countries' electric grids? In 2009, *The Wall Street Journal*, with no evidence beyond "intelligence" sources, reported that Russia and China had done precisely that to the US grid.^[6]

In late 2014, Admiral Michael Rogers, Commander, U.S. Cyber Command (USCYBERCOM), testified^[7] that,

“there are nation-states and groups out there that have the capability . . . to shut down, forestall our ability to operate our basic infrastructure, whether it’s generating power across this nation, whether it’s moving water and fuel.” Later that year evidence surfaced that Russian hackers had used tools to penetrate power stations (using Black Energy malware) and corrupted software updates of machinery that sat on electronically isolated (aka “air-gapped”) networks (using Havex malware). In mid-2018, DHS officials reported penetration by Russian hackers of the US electrical system by leveraging the phishing-acquired credentials of suppliers to electrical control systems; “They got to the point where they could have thrown switches” and disrupted power flows.^[8] Iran has been credited with similar capabilities.^[9] Some believe that “so many attackers have stowed away in the systems that run the US electric grid that experts say they likely have the capability to strike at will.”^[10]

It is difficult to know what to make of these claims. The intelligence community keeps secrets for a living. Law enforcement rarely releases sensitive information before trials. Corporations seldom concede that they are victims of hackers, especially of hacks that produced no visible effects. Finding malware is not necessarily an indication of cyberattack, either. The malware could have drifted in from elsewhere. Stuxnet, for instance, appeared in over 100,000 systems outside the Natanz centrifuge plant. A compiler corrupted to produce malware-laden software for a specific supply-chain attack can compromise other software that is unknown to the hackers. While possible, it is quite difficult for hackers who cannot communicate with the malware to time an attack.

At least, claims of extant or impending cyberattacks can be refuted if given time. Anomalous indicators on an employee’s laptop at the Burlington Electric Department . . . were initially mistaken for a deliberate Russian hacking attempt on its electrical power grid.^[11] That is reassuring to onlookers who remember the accusation, and then the retraction, but what if someone had acted irreversibly on the accusation, before it was retracted?

Matters are foggier if attackers, rather than defenders, claim that implants were installed. In mid-2019, USCYBERCOM gave notice that it was installing implants into the Russian electric grid,^[12] which the Russians denied,^[13] claiming that such attacks were thwarted.^[14] So, is the US capable of taking down the Russian electric grid (e.g., in retaliation for their doing likewise)?

Finally, even if the fact of the disruption and attribution both are indisputable, the message intended by the disruption is subject to multiple interpretations. Consider the hacks of Ukraine's power grid.^[15] The hack, according to Robert M. Lee and Mike Assante (both teach cybersecurity for SANS) was meant, “to stoke the ire of Ukrainian customers and weaken their trust in the Ukrainian power companies and government.” The article’s author, citing Ukrainian sources, then adds that “[s]peculation has been rampant that the subsequent black-outs in Ukraine were retaliation for the attack on the Crimean substations.” Robert Lee was quoted later in the article considering the possibility that, “the attack on the Ukrainian power

companies was a message to Ukrainian authorities not to pursue privatization," ultimately concluding the message to be: "We want to be seen, and we want to send you a message ... oh, you think you can take away the power [in Crimea]? Well I can take away the power from you." Finally, an attack on the electric grid that caused modest effects could easily be portrayed as one that could have caused major effects but for self-restraint or error: the late 2016 cyber-attack on Ukraine's electric grid opened circuit breakers that were closed an hour later, but analysis of the code suggested that the hackers sought to cause physical damage before power was restored but made several coding errors.^[16] Oleksii Yasinsky, a Ukrainian cybersecurity researcher, believed the hackers "could have knocked out Ukrenergo's transmission station for longer or caused permanent, physical harm to the grid, he says—a restraint that American analysts like Assante and Lee have also noted."^[17]

What can we draw from these examples? Based on the Venezuelan incident, one observer concluded, "the inability to definitively discount US or other foreign intervention, whether deliberate or accidental, demonstrates the incredible power of using cyberattacks to target utilities."^[18] But there is an alternative perspective: it demonstrates the profound impact such cyberattacks have on the public's imagination—which, when coupled with the difficulty of proving who did what and why—illustrates the power that mere *claims* of cyberattack have, either by the attacker or the attacked. There is a reason cyberspace events are mysterious. To paraphrase Ross Anderson^[19]: airline safety has improved faster than cybersecurity because airplanes crash outside and, by so doing, create facts that cannot be waved away. But computers crash inside, which allows others to understate or overstate what actually took place.

Manipulating Information about Information War Itself is Information Warfare

The ease with which facts can be manipulated, given the ambiguities and obscurities of cyberspace, means that leaders will be tempted to do just that. Having examined the means of distorting the truth, it is important to understand some of the motives that would prompt such distortions. The degree of manipulation will depend on several variables, including the moral quality of a country's leaders, their ability to maintain a narrative at variance with facts, and the political context within which they operate.

In fairness, the ability to create misperceptions that vary with reality is often unequal. Transparency brings reality and perceptions closer together. So, the leeway of governments to fudge events will vary—directly or via proxies (e.g., power grid operators). Competition among private cybersecurity firms makes it more difficult to advance defensible claims. Conversely, exposure to public opinion creates a gap between perceptions and reality that may be unsupportable. Claims to expert authority are not taken as seriously as (we suppose) before. At least in the West, epistemic closure appears to be growing worse. Despite a clear consensus among the cybersecurity community that imaging servers suffices to understand a network intrusion, for instance, many who take their cues from the leaders they like believe

that shipping servers to a foreign country is a way to hide false flag attacks (e.g., Ukrainians doing what Russians are blamed for).

Adding to the discrepancy has been the tendency of some countries to separate their communications from the rest of the world. North Korea remains isolated. China's Great Firewall is a prime example of selective filtering. Iran is similar in this regard and is contemplating even more isolation.^[20] Russia recently experimented with closing its Internet off from the rest of the world.^[21] Early hopes that the Internet would bring the world together and that, in John Gilmore's words, "The Net interprets censorship as damage and routes around it," look nostalgic. As Evgeny Morozov observed in *The Net Delusion: The Dark Side of Internet Freedom*,^[22] authoritarian governments originally caught flat-footed by the Internet have learned how to control it and turn it to their purposes.

Between the facts that, for laypeople, cyberspace is opaque, and yet, the Internet can actually facilitate misperception over reality, the stage is set for states to make of events in cyberspace as they will.

To simplify the question, consider two players: the target and the attacker. The target has two basic choices: to play up the incident (even, perhaps especially, if no cyberattack were actually involved or no implant dropped), or to downplay it. The attacker has two basic choices as well, but is in a poor position vis-à-vis the target to argue about the effects of the cyberattack. Figuratively and literally, the target is there, and the attacker is not. But the attacker can either dispute or embrace attribution because the requisite evidence is something the attacker will have special knowledge of.^[23]

The target can play up the cyberattack in many ways. Assuming there is *something* to work with (e.g., a blackout), it can be mischaracterized as an accident, human error, design flaw, as well as a cyberattack. As a variant, an accidental or inadvertent cyberattack can be characterized as deliberate and malicious.^[24] A cyberattack with a weak effect could be touted as a bullet dodged, either because the hacker erred, or because the hacker was brandishing its capabilities and could have done worse if it wanted to. And, as noted, even if no cyberattack took place, some entity the target wants to malign could be accused of having planted malware "discovered" in the system. Attribution can also be played, largely because some cyberattacks are more embarrassing than others. An inside job can imply that an organization's employees are untrustworthy, or that the organization poorly vetted, and/or that its systems afforded others too many privileges. The victim of a state-backed hacker group can summon the misleading argument that a private company can no more defend its network against an army than it can defend its factory against one; falling to a criminal group is more blameworthy. Finally, if the adverse impact of the cyberattack is insufficient to meet the target's needed political narrative, the cyberattack can be cast as the beginning of a systematic campaign. With a little nerve, it can argue that it was the first shot in a kinetic war, thereby justifying the target's decision to

mobilize its society to fight. While an actual kinetic war may not happen, an action-reaction cycle could actually escalate into war. And if the war does not come, there's always the narrative that war would have come were it not for the target's raising the alarm and mobilizing (e.g., its own forces, the righteous anger of its citizenry, enraged world opinion) accordingly.

This litany of options illustrates why the target may play up a cyberattack. They help unify a country in the face of an adversary while distracting the polity from the government's mistakes. The mobilization of opinion helps governments institute repressive measures or raise taxes. Threats of cyberattacks may persuade the public to allow its government access to personal or organizational systems. Once governments are granted authority to surveil systems for malware or other evidence of intrusion, they can use such access to monitor unwanted activity by citizens. Accusations may create cover for the target's own aggressive acts, forcing concessions from the attacker, even if the incident is phony or exaggerated. It can warn third countries that war may be coming, thereby forcing alliances or other commitments. (Ironically, hyping a cyberattack could lower tensions by substituting conflict in cyberspace, which is unlikely to kill anyone, for more risky posturing in the physical world).

The most innocent explanation is that exaggerating the cyberspace threat will persuade many to take cybersecurity more seriously as they should have from the start (like Senator Arthur Vandenberg, who told President Truman public support for aid to Greece and Turkey against Communists required him to "scare the hell out of the American people"). But this rationale holds some paradox. If the point is to inspire confidence in the integrity of government processes – for instance, that voters can trust election results because they are protected – advertising their vulnerability to hacking may ultimately lead to trustworthy voting systems but, until then, will not produce trusted voting systems.

That logic is one of several reasons' leaders may be reluctant to play up cyberattacks. As a device for mobilizing popular opinion, cyberspace events may be too esoteric, incomprehensible, and removed from daily concerns to allow for galvanizing emotions. Unlike terrorism, cyberattacks more likely will engender anxiety and annoyance, on par with the prospect of a morning traffic jam. But if someone's literal viscera are not threatened, can cyberattacks induce the kind of visceral fear with the requisite political clout?

Reasons to downplay cyberattacks are not hard to find. Falling victim to cyberattacks is, as noted, embarrassing. Such catastrophes can be prevented either by diligent cybersecurity investments or through various forms of self-denial (e.g., closing systems to easy access by others, retaining less information, or prioritizing security over usability and flexibility). Because the point of government is providing security and reliability, admitting that it failed at that can be difficult.

Other reasons for reticence may arise in strategy. Just as playing up cyberattacks may help mobilize citizens for confrontation, playing them down may allow governments to avoid

confrontations they cannot win or at least can win only at great cost. Analogously, many in Europe were eager to accept Putin's assertion that Russia had no forces in Ukraine's east: "[The West] connived in Mr. Putin's pretense that he had not invaded eastern Ukraine—even though in a furtive tricky way he plainly had—because to say otherwise would have required a drastic response."^[25] Playing down attacks also signals insouciance. Thus, if its purpose is to goad the target into doing something rash (e.g., as the September 11th attacks may have been used by al-Qaeda to goad the US into Afghanistan) then downplaying that would translate as an insufficient pain threshold to merit response. Similarly, by refusing to admit to being hurt, a state conveys that it is not coerced and thus will not accede to whatever demands, be they explicit or implicit, are imposed by the attacker, and will itself be undeterred in pursuing its own ends.

Denying attribution also obviates pressures on the target to respond, and also conveys, albeit weakly, that the cyberattack fell below some pain threshold. This allows the target state the option to determine later that they have enough confidence to respond. Conversely, an argument that the pain of cyberattack is limited can be undermined by the discovery of wider and deeper effects and rarely can be assigned by the reverse (much as death tolls can only go up as catastrophes are investigated). The same holds for characterization of near-attacks or failed-attacks. Earlier interpretations that they were not deliberate or carried out by incompetents can be credibly revisited.

A last option is to cast doubt on any early facts, whether helpful or harmful. One reason may be to avoid prejudicing the investigation in the hopes of learning the real lessons for the incident. Another is to prevent the attacker (and would-be copycats) from receiving battle damage assessment so to speak, the better to perfect subsequent attacks.

As to attackers, they, like defenders, can play up or play down the consequences of the attack, its characterization, or its attribution. In practice, however, it is difficult for attackers to more credibly characterize the attack than the target, which has far greater access to information than the attacker. Indeed, the attacker often will have very little if any firsthand information. Reports, for instance, that the US successfully interfered with performance of North Korea's Musudan missile had to be left dangling because of the lack of any sure way to know whether the hack actually worked, or, even if it did work, was a decisive factor in subsequent launch failures.^[26] The best the attacker can do is to argue that while the target may know better, its leaders often lie about what they know to be otherwise. It took two months after the public learned about Stuxnet for Iran to concede it had been hurt. Yet neither the US nor Israel officially claimed that the attacks succeeded.

In theory, matters are less clear. Attackers usually know better what they tried to do than do defenders; if the damage is subtle or only appears under certain circumstances, the attacker may know to look for telltale signs that its attacks worked, often leaving the defender oblivious to the attack. Subtle attacks also do not make the news, at least not until their impacts become visible.

This leaves attribution as the attacker's primary lever. Countries generally do not acknowledge their cyberspace operations, even when so accused. This stands in contrast to acts of terrorism (at least pre-9/11), which were followed by multiple claimed terrorist *group* perpetrators. Many cyberattacks such as the 2012 attack on Saudi Aramco or the 2014 attack on Sony are claimed by *groups*: The Cutting Sword of Justice and the Guardians of the Peace, respectively. But these groups do not really exist as separate entities. The reasons to deny attribution are straightforward. Most accusations involve cyber espionage whose operators avoid—because the point is to work undetected—revealing their own capabilities and modus operandi.

As for the rarer instances of cyberattack, often the target knows the attacker's identity, while admitting as much opens the attacker to criticism and makes it hard for the attacker to, in turn, criticize incoming cyberattacks. For example, going back at least to the 1973 War, Israel's neighbors believed that Israel had nuclear weapons, thereby giving Israel the benefit of deterrence. Yet Israel strenuously denied having such weapons, to the point of even luring and then jailing Mordechai Vanunu, an Israeli who revealed as much to the British press in the 1980's.^[27] Israel may well have calculated that open admission would have led third parties to push Israel to de-nuclearize, or to pressure neighboring countries to pursue their own nuclear weapons.


Stuxnet provides an interesting case in contrast. Neither the US nor Israel denied this cyberattack,^[28] yet neither admitted it officially, at least at first. But at least some in each country wanted to take credit for it. In the US, former Vice Chairman of the JCS, General Cartwright, was accused to have been the source for David Sanger's articles on the hack. And a 2011 YouTube video captured Israel's Chief of Staff at his retirement party counting Stuxnet among his prominent achievements.^[29] In 2016, an official Israeli document baldly stated, "an example of an offensive cyber operation conducted by Israel is Stuxnet, which was jointly developed with the United States and targeted Iranian nuclear facilities."^[30] Other governments have tried to have it both ways. Russia denied hacking the DNC in 2016, but its President called the hackers "artists."^[31] North Korea denied hacking Sony in 2014 but called it a "righteous deed."^[32]

Generally, hypocrisy—a tribute vice pays to virtue—rules. Given a choice between appearing great and appearing good, countries choose good. That is, they would rather talk up their fealty to international norms than overawe others with their cyberspace prowess. But for how long? As noted, the US did not seem to mind news stories that it had penetrated Russia's grid. In the summer of 2019, the US also indicated it was penetrating systems of those intruding against the US^[33] (a.k.a. "defending forward," or "persistent engagement"), and had countered Iran's shoot-down of a US drone with a cyberattack.^[34] Might other countries follow? No country had (publicly, at least) established a cyberspace operations entity until the US formed USCYBERCOM. Many blushed at the thought of militarizing cyberspace until they—first allies, and then adversaries—followed suit. Whether other countries copy the trend

of taking credit not only for successes but also for operations more difficult to assess as successful depends on whether the aforementioned events of 2019 recur. This, in turn, depends on how much they reflected the character of the U.S. Administration at the time. But if such behavior becomes a trend, as opposed to a blip, other countries likely will follow suit in the years to come.

CONCLUSION

It has been said that the first casualty in war is truth. Today advances in technology and transparency as well as the professionalization of inquiry make it easier to determine the truth sooner rather than later. In this regard, cyberspace lags. Perhaps this should not be so—a fully imaged computer hard drive after a cyberattack leaves nowhere for anything to hide. But, in practice, there is often no third-party confirmation of a successful cyberattack, much less a failed cyberattack, or one partially completed (e.g., an implant). There is no easy equivalent in overhead imagery. And besides, matters once considered settled because of elite scientific consensus are increasingly open to question for a variety of causes (e.g., populism, the Internet's ability to support echo chambers, less influence of traditional media, epistemic closure).

True facts of cyberwar are becoming secondary to misperceptions that governments either shape or influence. Increasingly, cyberwar is becoming what states make of it, and how they package it. That leaves, as open questions, what states *will* make of it. As argued, their options range in efficacy and persistence (in the face of subsequent revelations). The strategies states will employ will, of course, adapt to the circumstances. No hard projections can be made about what the games will look like, but games there will be.^[35] 

NOTES

1. Titled in homage to an otherwise unrelated article: Alexander Wendt, "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organization* 46(02):391-425, March 1992.
2. Description from Tom McKay, "Maduro Says 'Multiple Cyberattacks' Backed by U.S. to Blame for Four Days of Widespread Blackouts," March 10, 2019; <https://gizmodo.com/maduro-says-multiple-cyberattacks-backed-by-u-s-to-b-1833190542>.
3. When China's offer to help bolster the security of Venezuela's grid was rejected, even the Chinese were convinced that no such cyberattack had taken place.
4. This claim (without details) was made by the CIA's Tom Donahue (Thomas Claburn, "CIA Admits Cyberattacks Blacked Out Cities," January 18, 2008; <http://www.informationweek.com/cia-admits-cyberattacks-blacked-out-citi/205901631>) and broadcast (with more details) by the CBS news show, "Sixty Minutes" on June 11, 2009 (<http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/>).
5. Marcelo Soares, "Brazilian Blackout Traced to Sooty Insulators, Not Hackers" November 9, 2009; http://www.wired.com/threatlevel/2009/11/brazil_blackout/.
6. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009, 1, <http://www.wsj.com/articles/SB123914805204099085>.
7. Ellen Nakashima, "Foreign powers steal data on critical U.S. infrastructure, NSA chief says," November 20, 2014; http://www.washingtonpost.com/world/national-security/nsa-chief-foreign-powers-steal-data-on-critical-us-infrast-structure/2014/11/20/ddd4392e-70cb-11e4-893f-86bd390a3340_story.html.
8. Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," July 23, 2018; <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110> and Colleen Long, "Russian hackers used phishing tools in 2017 attack on grid, July 26, 2018; <https://www.apnews.com/2c17bda4ac704df6be66018197f29912>.
9. Courtney Kube, Carol E. Lee, Dan De Luce and Ken Dilanian, "Iran has laid groundwork for extensive cyberattacks on U.S., say officials," July 20, 2018; <https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081>. See also Andy Greenberg, "The Highly Dangerous 'Triton' Hackers have Probed the US Grid," June 14, 2019; <https://www.wired.com/story/triton-hackers-scan-us-power-grid/>.
10. Garance Burke and Jonathan Fahey, "Iranian hackers breached US power grid to engineer blackouts," December 22, 2015; <https://apnews.com/79f0c976364b4c9dad12c44bba4ccc88>. See also Sue Halpern, "Should the U.S. Expect an Iranian Cyberattack," January 6, 2010; <https://www.newyorker.com/tech/annals-of-technology/should-the-us-expect-an-iranian-cyberattack>.
11. Ellen Nakashima and Juliet Eilperin, "Russian government hackers do not appear to have targeted Vermont utility, say people close to investigation," January 2, 2017; https://www.washingtonpost.com/world/national-security/russian-government-hackers-do-not-appear-to-have-targeted-vermont-utility-say-people-close-to-investigation/2017/01/02/70c25956-d12c-11e6-945a-76f69a399dd5_story.html.
12. David Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," June 15, 2019; <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.
13. Ivan Nechepurenko, "Kremlin Warns of Cyberwar After Report of U.S. Hacking Into Russian Power Grid," June 17, 2019; <https://www.nytimes.com/2019/06/17/world/europe/russia-us-cyberwar-grid.html>.
14. Reuters, "Russia thwarts U.S. cyber attacks on its infrastructure: news agencies," June 17, 2019; <https://www.reuters.com/article/us-usa-russia-cyber-russia/russia-thwarts-u-s-cyber-attacks-on-its-infrastructure-news-agencies-idUSKCNITIU0>.
15. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," March 3, 2016; <http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
16. Joe Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack," August 15, 2019; <https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>.
17. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," June 20, 2017; <https://www.wired.com/story/russian-hackers-attack-ukraine/>.
18. From Kalev Leetaru, "Could Venezuela's Power Outage Really Be A Cyber Attack?," March 9, 2019; <https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/#34e80b4e607c>.

NOTES

19. My interpretation of an argument on the first page of Ross Anderson, "Why Cryptosystems Fail," 1993, <https://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf>.
20. See, for example, Behrang Tajdin, "Iran letter raises prospect of 'white list' internet clampdown," November 26, 2019; <https://www.bbc.com/news/technology-50563917>.
21. Catalin Cimpanu, "Russia successfully disconnected from the internet," December 23, 2019; <https://www.zdnet.com/article/russia-successfully-disconnected-from-the-internet/>.
22. New York, USA: Public Affairs, 2011.
23. Notionally, if the attacker supports multiple, albeit uncooperative, threat actor groups, or when multiple states attack, the target's knowledge may be incomplete. Practically, this is rare to nonexistent.
24. Some consider this plausible. In 2008, a National Journal story quoted unnamed intelligence sources to argue that a hacker trying to map Florida Power & light, "got carried away and had a 'what happens if I pull on this' moment ... [and]triggered a cascade effect, shutting down large portions of the Florida power grid". The outage was later ascribed to human error. See Shane Harris, "China's Cyber Militia," National Journal Magazine, May 31, 2008, <http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531>.
25. From *Economist*, "The Siege," July 12, 2014, <http://www.economist.com/news/leaders/21606831-believing-vladimir-putin-has-surrendered-ukraine-would-be-naive-west-must-keep-up>.
26. David Sanger and William Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," March 4, 2017; <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html>.
27. But see Conrad Duncan, "Netanyahu calls Israel a 'nuclear power' before correcting himself in apparent slip of the tongue," January 6, 2020; <https://www.independent.co.uk/news/world/middle-east/netanyahu-israel-nuclear-power-weapons-iran-crisis-trump-a9272086.html>.
28. See, for instance, Deputy Secretary of Defense Lynn's non-answer in Kim Zetter, "Senior Defense Official Caught Hedging on U.S. Involvement in Stuxnet," *Wired*, May 26, 2011, <http://www.wired.com/threatlevel/2011/05/defense-department-stuxnet/>.
29. Christopher Williams, "Israeli security chief celebrates Stuxnet cyber attack" February 16, 2011; <http://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyberattack.html> and William Jacobson, "Did Israel Just Admit to Creating Stuxnet?," February 15, 2011; <http://legalinsurrection.com/2011/02/did-israel-just-admit-to-creating-stuxnet/>.
30. "Deterring Terror: English Translation of the Official Strategy of the Israel Defense Forces," Belfer Center Special Report of August 2016; <http://www.belfercenter.org/publication/israeli-defense-forces-defense-doctrine-english-translation>, 48.
31. See Andrew Higgins, "Maybe Private Russian Hackers Meddled in Election, Putin Says," June 1, 2017; <https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html>.
32. Choe Sang-Hun, "North Korea Denies Role in Sony Pictures Hacking," *New York Times*, December 7, 2014, <http://www.nytimes.com/2014/12/08/business/north-korea-denies-hacking-sony-but-calls-attack-a-righteous-deed.html>.
33. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," February 27, 2019; <https://www.whitehouse.gov/presidential-actions/presidentexecutive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
34. AFP, "US launched cyber attacks on Iran after drone shootdown: reports," June 22, 2019; <https://news.yahoo.com/us-launched-cyber-attacks-iran-drone-shootdown-reports-232123877.html>.