Cyber War on Energy Grids and Infrastructure: Implications of the Russia-US Case

Debashish Bose

The US electrical grid is the largest interconnected machine on Earth: it is made up of more than 7,000 power plants, 55,000 sub-stations, 200,000 miles of high-voltage transmission lines and 5.5 million miles of local distribution lines, linking thousands of generating plants to factories, homes and businesses. This web of generators, sub-stations and power lines is organised into three major interconnections, operated by 66 balancing authorities and 3,000 different utilities. The National Academy of Engineering ranks it as the greatest engineering achievement of the 20th century. In addition to all this paraphernalia, the retail power distribution companies are using advanced metering systems. Advanced metering allows distribution companies to show customers how much electricity they are using at different times of the day and how much that power costs. Multiple sources of power (including wind and solar generation) will eventually lead to the coming of smart grids. The smart grid will monitor everything at a very fine level of detail and will react instantaneously so that operators will have time to fire up another plant if the wind speed drops or a big cloud formation reduces solar output. This huge technological behemoth, along with health care, finance,

Colonel **Debashish Bose** is Senior Fellow, Centre for Land Warfare Studies, New Delhi.

N.B. The views expressed in this article are those of the author in his personal capacity and do not carry any official endorsement.

transportation, water, and communications sectors, make up what is known as the US critical infrastructure. All these sectors have reported significant cyber incidents in the last decade.

Russian Attacks on US Critical Infrastructure

On March 15, 2018, the US-CERT (Alert TA18-074A) released a report describing a massive Russian hacking campaign to infiltrate America's "critical infrastructure" — things like power plants, nuclear generators, commercial facilities, water facilities,, aviation, and critical manufacturing sectors. The joint report from the Federal Bureau of Investigation (FBI) and Department of Homeland Security stated that Russian hackers gained access to computers across the targeted industries and collected sensitive data, including passwords, logins, and information about energy generation. While the report did not specify any identifiable sabotage, the intrusion could set up future attacks that do more than just record observations. The joint study resulted in the identification of distinct indicators and behaviour related to this activity. There were two distinct categories of victims: staging and intended targets. The initial victims were peripheral organisations such as trusted third-party suppliers, with less secure networks, referred to as "staging targets". The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. The threat actors in this campaign employed a variety of Tactics, Techniques and Procedures (TTPs), including

- Spear-phishing emails (from compromised legitimate accounts).
- Watering-hole domains.
- Credential gathering.
- Open-source and network reconnaissance.
- Host-based exploitation.
- Targeting Industrial Control System (ICS) infrastructure.

Phases of the model included reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and actions on the objective. Instead of disrupting power generation, the intruders watched and recorded information from computers that received the data from the energy generation systems. Essentially, if the hackers could get into computers the same way they did for this scouting mission, and were able to modify codes on the targeted computers as easily as they did, then there's no reason why they will not be able to stage another attack and take it to the next level. The report also noted that the hackers tried to mask the evidence of their intrusion on the way out, and advised the targeted companies to take precautions in case any malicious code was left behind. The US Treasury Department issued fresh sanctions against several Russian individuals and organisations on March 15, 2018—it named these cyber attacks as one of the reasons for doing so. The Treasury Department specifically sanctioned individuals involved with Russia's Internet Research Agency and the GRU, Russia's military intelligence branch, though it declined to specifically link any of the individuals named to this latest hacking campaign. In fact, just a day after the report was released, Energy Secretary Rick Perry stated that cyber attacks are "literally happening hundreds of thousands of times a day," and warned that the Department of Energy needed an "office of cyber security and emergency response" in order to be prepared for threats like this in the future. This finally got created in February 2018.

The report marked a major turning point, as it was for the first time that the US government had publicly blamed Russia's government for attacks on the energy infrastructure. Explicitly pinning the attack on the Kremlin meant that rather than targeting the hackers as individuals, the United States could now respond against Russia as a whole. Another major development was the fact that by tying the attacks to Russian intelligence agencies, the US government could now sanction high-level members of those agencies for the actions of their subordinates. This makes further hacking operations a lot riskier not just for the hackers themselves but also for their chain of command, and the government that authorised them. It's a first step toward establishing deterrence in cyber space.

Ukraine Electric Grid Attacks, 2015

No study on cyber attacks on critical infrastructure is complete without a study of the cyber attacks on the Ukraine electricity grid. It was the first known successful cyber attack on an electric grid. Ukraine has served as the laboratory where Russia has been testing its cyber attack capabilities on critical infrastructure. On December 23, 2015, electric companies in Ukraine saw the potential effect of a combined attack on an electric utility's Information Technology (IT) and Industrial Control Systems (ICS). In this instance, a Ukraine power grid was attacked, the cyber attack penetrated electricity distribution control centres in Ukraine: using software vulnerabilities, stolen credentials and sophisticated malware, the attackers were able to open dozens of circuit breakers and shut off power to more than 225,000 customers for several hours. The malicious actors then inundated the company's customer service centre with calls, which slowed the response time to the electricity outage by causing internal challenges.

In the first stage, they carried out reconnaissance to study the networks and gather operator credentials; in the next stage, they launched a well-coordinated attack on the Prykarpattyaoblenergo control centre, which distributes power to the residents of the Ivano-Frankivsk Oblast region of western Ukraine. At the same time, consumers of two other energy distribution companies, Chernivtsioblenergo, servicing the Chernivtsi Oblast, and Kyivoblenergo, servicing the Kyiv Oblast, were also affected by a cyber attack, but at a smaller scale. In total, up to 73 MWh of electricity was not supplied (or 0.015 percent of daily electricity consumption in Ukraine).

The attack had other distinct characteristics; there were clear delineations between the various phases of the operation, suggesting that different levels of actors worked on different parts of the assault. This very strongly suggests that the attack might have involved collaboration between cyber criminals and nation-state actors. It is quite possible that it started out with cyber criminals getting initial access to the network, and then handing it to nation-state attackers who did the rest. Analysis showed that the control systems in Ukraine were surprisingly more secure than some in the US. They were well-segmented from the control centre business networks, with robust firewalls. They still had weaknesses such as workers logging remotely into the Supervisory Control and Data Acquisition (SCADA) network; the network that controlled the grid, was not required to use the two-factor authentication, which allowed the attackers to hijack their credentials and gain crucial access to systems that controlled the breakers. The attackers overwrote firmware on critical devices at 16 of the sub-stations, leaving them unresponsive to any remote commands from operators. The attacks had begun months earlier with a spear-phishing campaign that targeted IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine. The phishing campaign delivered email to workers at three of the companies with a malicious Word document attached. When workers clicked on the attachment, a popup was displayed asking them to enable macros for the document. If they complied, a programme called BlackEnergy3 infected their machines and opened a backdoor to the hackers. Exploiting the macros feature is an old-school method from the decades gone by, but the attackers seem to have revived the method in the current attacks.

The initial intrusion got the attackers only as far as the corporate networks. But they still had to get to the SCADA networks that controlled the grid. The companies had wisely segregated those networks with a firewall. Over many months, they conducted extensive reconnaissance, exploring and mapping the networks and getting access to the Windows

Domain Controllers, where user accounts for networks were managed. Here, they harvested worker credentials, some of them for Virtual Private Networks (VPNs) used to remotely log in to the SCADA network. Once they got into the SCADA networks, they slowly set the stage for their attack. First, they reconfigured the Uninterrupted Power Supply (UPS), responsible for providing back-up power to two of the control centres. The aim was to ensure that when power went out for the wider region, the operators would be blind, too. Each company used a different distribution management system for its grid, and during the reconnaissance phase, the attackers studied each of them carefully and created operation specific malicious firmware updates for each of them. The aim was to prevent the operators from sending remote commands to re-close the breakers once a blackout occurred. Armed with the malicious firmware, the attackers were now ready to carry out their attack.

Some time around 3:30 p.m. on December 23, 2015, in step one of the attack, they entered the SCADA networks through the hijacked VPNs and sent commands to disable the UPS systems they had already reconfigured. Then they began to open the breakers. Prior to opening of the breakers, they did another innovation, and launched a Telephone Denial-of-Service (TDoS) attack against customer call centres to prevent customers from calling in to report the outage. In this case, the centre's phone systems were flooded with thousands of bogus calls that appeared to come from Moscow, in order to prevent legitimate callers from getting through. The TDoS also had another fallout: it unleashed the wrath of the Ukrainian customers and weakened their trust in the Ukrainian power companies and government. After the above steps had been completed, the hackers used a piece of malware called Kill Disk to wipe files from operator stations to render them inoperable as well. The purpose was to overwrite data in essential system files, causing the computers to crash. Since they also overwrote the master boot record, the infected computers could not reboot.

Ukraine Electric Grid Attacks, 2016

A year later, in 2016, a week before Christmas, hackers again struck a Ukrainian electric utility, Ukrenergo, north of the city of Kiev, blacking out a portion of the Ukrainian capital equivalent to a fifth of its total power capacity. The attack lasted for about an hour. What is disturbing is the fact that investigators feel that the blackout may have only been a dry run. The hackers appear to have tested a highly evolved specimen of grid-sabotaging malware, not ever observed in the wild. The researchers describe that malware, which they've alternately named "Industroyer" or "Crash Override," as only the second-ever known case of malicious code purpose-built to disrupt physical systems. The first, the Stuxnet, was used by the US and Israel to destroy centrifuges in an Iranian nuclear enrichment facility in 2009. The unique feature of this malware is the fact that it can lead to automation of mass power outages, like the one in the Ukrainian capital, and includes swappable, plug-in components that could allow it to be adapted to different electric utilities, easily reused, or even launched simultaneously across multiple targets. The implication of the adaptability of the malware is the fact that the tool poses a threat not just to the critical infrastructure of Ukraine, but to other power grids around the world, including America's. This is extremely alarming for the fact that nothing about it is unique to Ukraine. This is in effect a platform to carry out future attacks. Thus, it is clear that the second attack was not a rerun of the first attack.

Instead of gaining access to the Ukrainian utilities' networks and manually switching off power to electrical sub-stations, as hackers did in 2015, the 2016 attack was fully automated. It had specific functionalities which allowed it to speak directly to grid equipment, sending commands in the specific protocols those controls used to switch the flow of power on and off. That means Crash Override could perform blackout attacks more quickly, with far less preparation, and with far fewer humans managing it, all indicating its capability for automation.

The malware had "logic bomb" functionality, which allowed it to automatically detonate at a preset time. Step one appears to be the same where targeted phishing emails enabled the necessary access to the network. Once Crash Override had infected the Windows machines on Ukrenergo's network, according to researchers, it automatically mapped out control systems and locate target equipment. The programme also recorded network logs that it could send back to its operators, to let them learn how those control systems function over time. From this stage onwards, Crash Override could launch any of four "payload" modules, each of which could communicate with grid equipment via a different protocol. Apart from its modular adaptability, the malware could also comprehensively destroy all files on systems it had infected, to cover up its tracks after the completion of an attack.

Another disturbing capability of the malware was that it could potentially be used to cause physical damage to power equipment. The malware exploits a known vulnerability in the Siemens ICS equipment known as a Siprotec digital relay. The Siprotec device gauges the charge of grid components, sends that information back to its operators, and automatically opens circuit breakers if it detects dangerous power levels. However, by sending the relay a carefully crafted chunk of data, the malware could disable it, leaving it offline until it was manually rebooted. If the attackers use this capability in conjunction with overloading the charge on grid components, it could prevent the kill-switch feature that keeps those components from overheating, damaging transformers or other equipment. If one could disable the digital relay, it could lead to thermal overload to lines, which, in turn, can cause the lines to sag or melt, and can damage transformers or equipment that is in line and energised. The malware can be further innovatively exploited to cause physical destruction by carrying out a well-crafted attack on multiple points in a power grid. Damaging elements of a grid en masse could cause a "cascading" outage, in which a power overload spills over from one region to another and to another. The December 2016 attack has been widely linked to a hacker group known as Sandworm, believed to have originated in Russia. Malware analysis has shown that it was more sophisticated, adaptable, and dangerous than the cyber security community had imagined. The nature and features of the malware, as well as the way it was run seem to indicate that it was made to be used multiple times and not just in Ukraine.

Demonstrated American Capabilities

Though there are no recorded incidents of American attacks on the Russian electric grid, however, there have been demonstrations of American capabilities. The Idaho National Laboratory ran the Aurora Generator Test in 2007 to demonstrate how a cyber attack could actually be used to physically destroy components of the electric grid. In the demonstration, a computer programme/malware was used to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid, as a result of which it finally exploded. This vulnerability is referred to as the *Aurora Vulnerability*. This vulnerability is a cause for worry because most of the grid equipment supports legacy equipment and communications protocols that were designed without security in mind. As a result of which they do not support authentication, confidentiality, or replay protection, which are all standard current generation cyber security practices now. The implication is that any attacker that can communicate with the device, can control it, and use the Aurora Vulnerability to destroy it. This is a serious concern, as the failure of even a single generator could cause widespread outages and possibly cascading failure of the entire power grid. Additionally, even if there are no outages from the removal of a single component, there is a large window for a second attack or failure, as it could take more than a year to replace it, because many generators and transformers are custom-built for the sub-station.

The Way Forward

The cyber defence model used by many electricity distribution companies involves monitoring separate physical, operational, and information technology "silos". This architecture lacks efficiency and can negatively impact the response time to an incident. At the same time, there is a number of useful products in the commercial domain for monitoring enterprise networks to dynamically keep track of security events as they occur. A converged network monitoring solution that is tailored to the cyber security nuances of ICS would give a holistic picture and, as a result, reduce blind spots for electric utilities. This, in turn, would give comprehensive situational awareness across both enterprise business system and operational ICS environments. This would enable real-time or near real-time situational awareness which is a key element in ensuring visibility across all silos/resources/operations. The National Cybersecurity Centre of Excellence (NCCoE) of the US has developed situational awareness for electric companies to augment existing and disparate physical, operational, and information technology situational awareness efforts by using commercial and open-source products to collect and converge monitoring information across these silos. The converged information is centrally analysed in the holistic environment, which leads to better understanding of security events, many of which would have gone unnoticed in their individual silos, and thereafter, relevant alerts are provided to each domain's monitoring capabilities, improving the situational awareness of security analysts in each silo. The converged data can facilitate a more efficient and appropriate response to an incident compared to an incident response that relies on isolated data from within a single silo.

The combined ecosystem provides the following capabilities:

- Security Incident and Event Management (SIEM) platform.
- ICS equipment (e.g., remote terminal units, programmable logic controllers and relays), along with associated software and communications equipment with encryption facilities.

- "Bump-in-the-wire" devices for augmenting operational technology with encrypted communication and logging capabilities.
- Software for collecting, analysing, visualising, and storing operational control data.
- Products that ensure the integrity and accuracy of data collected from remote facilities.

Other commonly recommended measures include:

- Establish a password policy which requires complex passwords for all users, involving letters, numbers, and symbols which are to be changed every month.
- Organisations/individuals should adopt multifactor authentication to mitigate the harm from stolen logins and passwords. This ensures that instead of just using a password to get into a system, a user also has to type in an additional code that he receives via a text message on a different channel or provides an ID dongle.
- Setting limits on the functions, a regular user can access on a computer, leaving other functions to secure the administrator accounts. That would minimise the damage an intruder could do by compromising a normal user.

Conclusion

The United States is supposedly stronger in terms of abilities. However, all real world examples in the public domain are of Russian attacks on US infrastructure. The Western media is much more active and stronger, thus, the Russian attacks get covered/reported extensively. Another force multiplier for the Western world is the capability of ATTRIBUTION. There is no doubt that if cyber attack capabilities are of a higher order, then the capability for attribution will also be proportionately better. If the Russian capability for attribution is less, then they will not be able to detect the attacks in the first place and even if they are able to detect the same, they may not be able to correctly attribute it to the source nation-state. Another major advantage for the Western world is what is called open source attribution. The moment a cyber attack is reported, the whole cyber security community on the internet gets after the analysis of the incident. Literally, the cyber power of a hundred nation-states gets unleashed on it. The Russian system is not so open, and they do not openly report their attacks. At the same time, the media is also not so strong to report and carry out in-depth analysis by itself. The Western world also has the availability of a large number of top class cyber security companies to aid the attribution effort.

The biggest collateral damage of these attacks is the fact that countries the world over are rapidly learning just how much vital or even lucrative information they can obtain from hacking. These countries are investing heavily in their own research or purchase from online sites available on the dark net so as to figure out new ways to circumvent security measures they encounter. After detailed deliberations, one realises that these cyber attacks fall in the grey area between network security, espionage, and crime, making it harder to figure out how to respond to them in the first place; secondly, and more important, is how to make the response count, so that the threat actor thinks twice the next time. Intrusions like these still fall short of sabotage or war, but that doesn't mean that no action can be taken against them. The attacks were relatively short-lived and harmless, but somebody somewhere has tested its cyber attack capabilities. The cyber weapon has now been quietly added to its armoury, waiting for the right time to bring down a critical infrastructure in any part of the world.