The Electricity Journal 30 (2017) 30–35

Contents lists available at ScienceDirect

The Electricity Journal

journal homepage: www.elsevier.com/locate/electr

How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid

Julia E. Sullivan[a,*], Dmitriy Kamensky[b]

[a] Independent Attorney, Annapolis, MD, United States
[b] Professor of Law at Berdyansk State Pedagogical University, Ukraine

ARTICLE INFO

Article history:
Available online xxx

ABSTRACT

On Dec. 23, 2015, a well-planned, perfectly synchronized and brilliantly executed cyber-attack caused a six-hour blackout for hundreds of thousands of customers in and around Ukraine's capital city of Kiev. While there have been no reported cases of cyber-terrorism causing power outages in the U.S., the attack methodology, tactics, techniques and procedures that were successfully deployed in Ukraine could be deployed against infrastructure here and around the world.

1. Introduction

On Dec. 23, 2015, a well-planned, perfectly synchronized and brilliantly executed cyber-attack caused a six-hour blackout for hundreds of thousands of customers in and around Ukraine's capital city of Kiev. It was the first documented case of cyber-intruders bringing down a power grid.

While there have been no reported cases of cyber-terrorism causing power outages in the U.S.,[1] researchers acknowledge that "absolute cyber-security" is unattainable.[2] Indeed, the attack methodology, tactics, techniques, and procedures that were successfully deployed in Ukraine could be deployed against infrastructure here and around the world.[3]

Small power production resources originally designed to lower the costs of energy and eliminate harmful emissions could also improve public access to power during a cyber-attack or other emergency. The resilience and security of supply implications have become increasingly relevant in evaluating the costs and benefits of distributed energy resources and microgrids.

2. What happened in Ukraine?

Political tension in Ukraine reached a boiling point in November 2013, when its pro-Russian president, Viktor Yanukovych, decided not to sign an association agreement with the European Union, choosing instead to pursue closer ties with Russia. This led to popular protests and the occupation of Kiev's Independence Square by pro-European Union Ukrainians in a series of events dubbed the "Euromaidan." Deadly clashes in Independence Square and in other areas pushed the country to the brink of civil war. In February 2014, Yanukovych fled the capital and was delivered into exile by agents of Russian President Vladimir Putin, whom Yanukovych credited with saving his life.[4]

* Corresponding author.
E-mail address: juliasullivan@jeslaw.us (J.E. Sullivan).

[1] In December 2016, the *Washington Post* reported that Russian hackers had penetrated the U.S. electric grid, but the report was retracted days later. "Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid, security officials say" *Washington Post* (Dec. 31, 2016) (available at https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.d8cfe95647e2) (site last visited 2-9-17); "Russian government hackers do not appear to have targeted Vermont utility, say people close to investigation," *Washington Post* (Jan. 2, 2017) (available at 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?utm_term=.e2731f4a86c9) (site last visited 2-9-17).

[2] Miles Keogh, Christina Cody, Cyber-Security for State Regulators at p. 18 (NARUC June 2012) (available at https://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf) (site last visited 2-10-17) (hereinafter "NARUC Primer").

[3] SANS Industrial Control Systems & Electricity Information Sharing and Analysis Center, Analysis of the Cyber Attack on the Ukrainian Power Grid at p. 23 (3-18-16) (available at http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf) (site last visited 2-10-17) (hereinafter, "SANS/E-ISAC White Paper").

http://dx.doi.org/10.1016/j.tej.2017.02.006
1040-6190/

Days after Yanukovych fled, armed men opposed to the "Euromaidan" began taking control of Ukraine's Crimean peninsula. The local population and the press referred to the occupiers as "little green men," but they were widely believed to be unmarked Russian troops.[5] Under occupation, the Crimean leadership announced it would hold a referendum on secession from Ukraine. This heavily disputed referendum was followed by the annexation of Crimea by the Russian Federation in March 2014.

Around the same time, a Russian-backed separatist movement started seizing cities in an area of Ukraine known as the Donbass region. Government forces appeared poised to retake the separatist-held territories until Russian reinforcements rolled across the border in August 2014, knocking the Ukrainian Army back. A hasty peace deal between Ukraine, Russia, and the separatists halted the onslaught, but this agreement soon broke down. Germany's Angela Merkel and France's François Hollande have been working to broker a diplomatic solution ever since, but with little success. In early 2017, fighting intensified again.

Ukraine's security service has accused Russia of thousands of cyber-attacks against Ukrainian infrastructure and institutions, including 6,500 incidents in just the last two months of 2016. Russia has repeatedly denied the hacking accusations.[6]

What we know for certain is this: on Dec. 23, 2015, shortly after pro-Ukrainian activists physically attacked a substation feeding power to Crimea, causing power outages to the region Russia had just annexed, a brilliantly executed cyber-attack caused a six-hour blackout for hundreds of thousands of customers in and around Ukraine's capital city.

Operators at the affected companies' control centers watched helplessly as hackers took control of their computers, opening breakers to bring at least thirty substations off-line. One operator reported watching in horror as a hacker purposefully navigated through the commands necessary to cause widespread outages. The perpetrators also disabled backup power supplies, leaving operators themselves stumbling in the winter dark. The intruders sabotaged operator workstations on their way out the digital door, making it harder to restore electric service to frantic customers. Call centers were flooded with bogus calls, apparently initiated from Moscow, so that real customers could not get through, increasing the sense of chaos. Malware also wiped out essential system files, causing computers to crash.

Three of Ukraine's regional electric power distribution companies experienced power outages,[7] but similar malware was found in the networks of other Ukrainian utilities as well.[8] The attackers used a malicious software platform known as "BlackEnergy" to access utility networks, planting a related piece of malware, "KillDisk," on targeted systems.[9] There are widespread reports that a group known as "Sandworm" has used BlackEnergy for targeted attacks in the U.S., Ukraine, and NATO that appear to align with the interests of Russia's Putin regime.[10] It is unclear whether other groups also use the same malware.

Experts agree that the attackers could have done more damage than they did,[11] such as destroying power generation equipment the way the well-known Aurora Generator Test did.[12] Some people believe the attack was just a warning – a tit-for-tat after pro-Ukrainian forces temporarily cut power to Crimea.[13] According to U.S. Navy Admiral Michael S. Rogers, the probable goal was not just to knock out Ukraine's power grid, but to watch the response and learn how to slow it down in future attacks.[14]

"In many ways, the Ukrainian oblenergos [regional operating companies] and their staff, as well as the involved Ukrainian government members, deserve congratulations. This attack was a world first in many ways, and the Ukrainian response was impressive with all aspects considered."[15] Despite this, and the rapid deployment of substantial NATO resources to help harden Ukraine's grid against future attacks,[16] Nikolay Koval, a Ukrainian cyber-security expert,[17] stated in an interview that the probability of recurrence remains "very high." He attributed a Dec. 17, 2016 blackout in Ukraine's capital city to malicious software, saying the incident was similar to an attack that had been simulated at a recent conference in which participants successfully hacked into a modern electrical substation model.[18]

In an interview, Inna Migulya, a resident of Okhrimivka village in the Zaporizhzhya region, described her concern that blackouts may once again become routine, as they were in the early years of Ukraine's independence:

> I remember a couple of winters of 1997 and 1998, when every day for three winter months in a row we did not have electricity from 5:00 to 7:00 p.m. It was already dark outside by the time of electricity cut off and my children had to do homework by candlelight. I had to make dinner fast before the electric stove was off as well. We were all in a rush and there was always a feeling of small depression in the air by that time. We all felt just miserable. Thank God we had coal-based heat in the house to keep us warm. The government officials told us that the rolling blackouts were necessary to maintain the electrical supply in the country. All I hope today, in 2017, is that blackouts do not become routine again, due to hacking attacks, the war in Donbass, or whatever other reason.

[4] "Vladimir Putin saved my life, says ousted Ukrainian president Viktor Yanukovych, *The Telegraph* (6-22-15) (available at http://www.telegraph.co.uk/news/worldnews/europe/russia/11692593/Vladimir-Putin-saved-my-life-says-ousted-Ukrainian-president-Viktor-Yanukovych.html) (site last visited 2-10-17).

[5] "Putin comes clean on Crimea's little green men," *Sky News* (3-10-15) (available at http://news.sky.com/story/putin-comes-clean-on-crimeas-little-green-men-10368423) (site last visited 2-10-17).

[6] "Russia's waging a 'cyberwar' against Ukraine: Poroshenko," *Reuters* (12-29-16) (available at http://www.newsweek.com/ukraine-hacking-cyber-attacks-russia-536999) (site last visited 2-10-17).

[7] *Cyber Systems in Control Centers*, 156 FERC ¶ 61,051 at P.4 (2016).

[8] Kim Zetter, "Everything we know about Ukraine's power plant hack," *Wired* (1-20-16) (available at https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/) (site last visited 2-10-17).

[9] "Ukraine utility cyber-attack wider than reported: experts," *Reuters* (1-4-16) (available at http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104) (site last visited 2-10-17).

[10] *До вимикання електрики в Україні причетна група російських хакерів - iSight Partners (To turn off the electricity in Ukraine involved A Group of Russian Hackers is Involved in Shutting Down Electricity in Ukraine - iSight Partners)*, 09:56 am, Jan. 8, 2016 (available at http://www.unian.ua/society/1231178-do-vimikannya-elektriki-v-ukrajini-prichetna-grupa-rosiyskih-hakeriv-isight-partners.html) (site last visited 2-10-17);Jeff Stone, "Russian hacking group sandworm targeted US before knocking out power in Ukraine," *Technology* (1-8-16) (available at http://www.ibtimes.com/russian-hacking-group-sandworm-targeted-us-knocking-out-power-ukraine-2257194) (site last visited 2-10-17).

[11] *Supra* note 10.

[12] The Idaho National Laboratory ran the Aurora Generator Test in 2007 to demonstrate how a cyber-attack could destroy physical components of the electric grid. The experiment used a computer program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode.

[13] *Supra* note 10.

[14] "NSA chief warns black energy attack on U.S. power grid a 'matter of when, not if' – lights out scenario not a myth but a coming reality," *All News Pipeline* (3-8-16) (available at http://allnewspipeline.com/NSA_Chief_Warns_Black_Energy_Weapon.php) (site last visited 2-10-17).

[15] SANS / E-ISAC White Paper at p. 24.

[16] For more information on the NATO Trust Fund on Cyber Defense for Ukraine, see http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf (site last visited 2-10-17).

[17] Mr. Koval is a former officer of the Computer Emergency Response Team of Ukraine, a special division of the State Center of Cyber Security of Ukraine.

[18] For more information on "Positive Hack Days," see http://www.phdays.com/press/news/41213/?sphrase_id=28251 (site last visited 2-10-17).