CYBER-ATTACK AGAINST UKRAINIAN POWER PLANTS

Prykarpattyaoblenergo and Kyivoblenergo

LESSONS LEARNED; IMPLEMENTATION CONSIDERATIONS

Gary Lehman

Professor Maras

3/20/2016

Contemporary Issues in Security Management, PMT 754

Cyber-attack On Multiple Ukrainian Power Plants: Attack Description

On December 23, 2015 wide swaths of the Ukraine in the Ivano-Frankivsk region (McGarry, 2016) experienced power outages for up to three hours impacting a large number of people, variously estimated at 225,000 (Ward, 2016) to 700,000 (Miller, 2016). This was reportedly the first time that a cyber-attack caused a power outage. (Miller, 2016). Power plants lost their automated control capabilities due to the cyber-attack; to effect restoration of service, power plant engineers switched off Supervisory Control And Data Acquisition (SCADA) systems (SCADA Systems, n.d.) and reverted to manual operation (which allowed service to be successfully restored). There were many contributory factors to why the power grid was disabled (which we will discuss later) but the trigger for the disabling of the power plants was that malicious software (malware) had been introduced into three Ukrainian power utilities via explicitly-targeted spear phishing attack (FBI, 2009) using Microsoft Office spreadsheet attachments ostensibly from the RADA (the Ukrainian Parliament). When the spreadsheets were opened, the users were prompted to "click here" to "enable macros" - which the users unwittingly did. This triggered the installation of BlackEnergy, a well-known, versatile, and pernicious malware weapon which DHS indicates (DHS, 2016) is frequently associated with Russia-based cyber-attacks.[1]

The malware thus introduced allowed the attacker to take over the internet-connected SCADA systems and use the SCADA to open circuit breakers at around thirty substations. (ESET, 2016)[2] ESET reported that stealth attributes were used in the malware to avoid detection and to complicate post-incident forensic analysis, and that there is no evidence as to the identity of the cyber-attackers. No indication of any motive was provided. The exact details of the attack are unclear, however it appears that the malware disrupted communications from SCADA device serial ports (serial port technology is obsolescent and usually associated with aging and thus more vulnerable hardware and operating systems) to the Ethernet backbone (which connects the devices in the power substations to centralized control rooms). Removing communication capabilities to/from the serial ports put the attacker into 'stealth mode', at which point the cyber-attacker(s) with impunity apparently turned off circuit breakers, thus taking portions of the power grid offline. (Klump, 2016) In addition it was reported (Miller, 2016) that the BlackEnergy malware installed and activated the 'KillDisk' plug-in, which (as the name implies) corrupted the SCADA devices disk drives. This prevented the ability to reboot the Industrial Control System (ICS) as a

[1] BlackEnergy has an insidious quality in that it can lay dormant, undetected and quiescent for long periods of time - until called into action to destroy or steal data, cause disk corruption, or receive and install damaging plug-ins, and thus possibly serving as the first stage of a systemic cyber-attack (Miller, 2016)

[2] ESET (Cyber Security Center of Excellence) reports on their website that in January 2016, a new wave of attacks were directed against the Ukrainian power grid and that, in contrast to the December attack which used the BlackEnergy malware, a new and unspecified malware software method was used

circumvention to enable a more rapid restoration of electrical service[3]. This information - combined with the post-incident joint US/Ukrainian team of technical investigators' report that extensive network topology surveillance must have been conducted in advance of the attack, indicates the possibility/likelihood of an insider attack. (DHS, 2016). This view is corroborated by iSight Partners' Senior Director Stephen Ward, a well-known beltway cyber-threat intelligence consultant, who indicated that custom logic to control the ICS was written following analysis of the power plants' internal processes. (Ward, 2016).

Only a Power Interruption in the Ukraine,

SO…Exactly Why Is This a Big Deal to Us?

There are a number of factors which collaborate to make this a serious national security concern for the United States. The ability for an individual or group to infiltrate and disable our national electric grid either suddenly or stealthfully over time means that portions of our country could suddenly be without electricity for a sustained period. The implications of that are too broad in reach, range, and consequence to adequately contemplate. This is especially the case if the attack is conducted in a heavily-populated section of the country. Imagine no refrigeration; light; water treatment plants are down; limited (and then no) power to run pumps for fuel; airports, train stations and hospitals are unavailable; law enforcement severely degraded; the entire command / control / communications / computer infrastructure we rely on – all of it - off the air. Certainly survivalists have thought this through at some depth, and are preparing accordingly.

Degradation of our critical infrastructure (or for that matter our financial system) over a sustained period of time is a clear and present threat. We have seen in the above case *how stealthy malware code can lie dormant and undetected until activated* (potentially as part of a coordinated, time-phased attack designed to maximize service disruption in persistent waves); we have seen how in a bizarre analogy terrorist 'sleeper cells' can exist in our midst undetected (Timothy McVeigh, the San Bernardino shooters, The Tsarnaevs, including some in the most unsuspecting position and place i.e. Major Nidal Hassan to name just a few) - *only to then suddenly activate* either spontaneously or in combination with a strategic attack plan. We have learned that the attack on the power plants in the Ukraine involved studying network topology and required some scripting and knowledge of SCADA language programming and unique operating environment. This means that an attack requires considerable preparation and cannot be conducted based on a "spontaneous impulse". The "lack of spontaneity" to this kind of attack proffers a dangerously false sense of security. The alarm which ought to be raised is that we know these sleeper cells are amongst us, working (stealthily) in place - with the ability to passively, discretely and gradually collect over time all the information required by their handlers or the cyber-attack planners, such as network topology diagrams, SCADA operations manuals, automated operations scripts, hardware diagrams, and other resources. Not to mention that these items are also widely downloadable from vendor websites as PDOMs (program

[3] The KillDisk corruption was so widespread that the SCADA computers are still as of 3/16/2016 non-functional (Ward, 2016)

description/operations manuals) or other manuals as PDF's. *The worlds of intrusion and Stuxnet are not static.* New ways and means of intrusion are ubiquitous and eternal. Activity on SCADA vendors' technical support forums corroborate this (Siemens, 2016).

We are also in the midst of transformational change in our information technology design / architecture / operations infrastructure, with pervasive and increasing offshore and onshore outsourcing which represents a profound transnational IT workflow migration out of the United States and Western Europe to South America, South Asia, East Asia, Eastern Europe, Egypt, Oceana, and increasingly, Africa. "Password-protected" root access to critical files and scripts are mere keystrokes away, and can be in many cases administered locally – or from 8,000 miles away. Pervasive use of IP-enabled devices such as Point of Sale units and IP-enabled video surveillance means that those *criminal or terrorist elements committed to penetration of our IT systems and SCADA systems have orders of magnitude more unprotected penetration alternatives.* We say and may even believe that we have robust and secure 'best practices' – but do we really?

Another disturbing aspect to this discussion is that cyber-attacks used to "just" mean theft or destruction of production, customer, and/or financial data; disruption of workflow; and theft of intellectual property and industrial espionage of various kinds. *But what we are witnessing in the disruption of the Ukrainian power grid is the nascent use of cyber-attack for military advantage and achieving political objectives.* All indications are that forces loyal to Putin and Russia are using Russian cyber-attack technology and methods to cripple the Ukrainian grid. As we have learned this is a classic terrorist strategy in action - to undermine the legitimacy of the State, to ferment fear, uncertainty and doubt amongst the general population (and in extreme cases, to murder innocents). A three-hour power outage is one thing. But imagine if it were longer in duration or time-phased and the cyber-attack conducted in combination with an armed offensive? Arguably we are seeing here is a reconnaissance mission or some kind of 'proof of concept', and/or a 'shakedown cruise' for some kind of coordinated multi-dimensional strike package either in the US, or elsewhere in the world.

Lessons Learned: Mitigation/Preparation/Response/Recovery

There are many lessons which can be taken from this cyber-attack in the Ukraine. Many US companies already implement many of these 'lessons learned'. The FBI, DHS and other national intelligence agencies promulgate best practices to reduce effectiveness of - or to defeat - this kind of attack. It is fair to say that the US *is less* exposed to a cyber-attack of this kind. That said, let us parse this attack for *Lessons Learned;* while not all the details of the attacks are known at this time, enough is known so that we can spotlight deficiencies [(DHS, 2016), and personal professional observations]

Mitigation Opportunities – Following Areas to be Improved/Corrected

- Unauthorized access to network diagrams
- Unauthorized access to power plant operation/procedures/documentation
- Unauthorized access to SCADA programs and manuals
- Poor user training (i.e. users not instructed to NOT open untested attachments)
- Obsolescent hardware and operating system
- Network-accessible (and thus vulnerable) SCADA computers
- Multiple-use SCADA computers (these systems should be for SCADA use only)
- Network unprotected; if SCADA must be networked then firewall and application whitelisting (single application thru firewall, all others excluded) is required
- Ineffectual software patch management (anti-virus protection)
- No network monitoring (knowing/managing who is accessing network and resources)
- Need secure consoles: badges; passwords; access logs; and locked wiring cabinets
- Need video surveillance of control rooms with monitoring and analytics
- Unused ports should be locked or disabled, and all unused OS services eliminated
-

Preparation / Response / Recovery Actions

- Disaster Recovery (DR) exercises with post-exercise management review
- Peer site security review; audits by DHS and FBI to surface vulnerabilities for correction
- Test Application Whitelisting; attempt penetration; observe results/is protection is intact?
- Secure onsite parts (e.g. preloaded disk drives) to quickly provision and reboot SCADA
- Test DR disk drives to ensure seamless recovery; test engineering levels/microcode
- *Comprehensive Defense Strategies and ICS Cyber-Security Best Practices* (Department_Homeland_Security, ICS Best Practices, n.d.) (Department_Homeland_Security, ICS Defense in Depth, 2009) (Department_Homeland_Security, Seven Strategies to Defend ICS, 2015)
- Conduct post-incident internal assessments; interlock/debrief with law enforcement and national intelligence organizations to provide technical details and logs for their analysis
- Additional security observations are examined in the Appendix under *Cyber-Attack in the Ukraine*: *Additional Security Observations and Recommendations* (based on personal professional background)

How These Lessons Should Be Implemented In the United States

Both the US energy sector and the US Department of Homeland Security and all the other federal agencies are on high alert to the dangers of cyber-attack and have invested significant resource and funding to prepare effective defense. Consequently, a recurrence of the kind of cyber-attacks targeted at the Ukrainian power industry here in the US would stand a lower chance of success. The network intrusions would be more likely to be interdicted; anomalous network activity detected; the workforce is for the most part trained to NOT open unknown attachments; better isolation of the ICS is in effect; disaster response/recovery procedures are practiced and the like.

On the other hand, the United States is more vulnerable than many other countries in the respect that our commitment to civil liberties - and an ethos of embracing diversity and commitment to fair treatment and respect for the individual - also makes us vulnerable to person(s) and organizations which do not wish us well. Current examples are the San Bernardino attack and the recent Boston Marathon bombing, and before those, the Oklahoma City bombing. These attacks were conducted against American civilians by groups and/or individuals who endeavored to and succeeded in murdering innocents in pursuit of religious and/or ideological beliefs which are at odds with the way of life we enjoy and cherish in the United States. Staff members in critical infrastructure will understand that there is necessarily a reduced 'expectation of privacy' in their line of work of national importance, and a pervasive commitment to the principle of 'need to know' is one part of the layered defense of that sector. No need to know = no access. For the jobs involving access to the most sensitive physical plant locations and data, this paper recommends intensified on-the-job surveillance (seeking to quickly identify anomalous behavior), as well as psychological profiling and correlated personal phone, travel and website surveillance to pattern-match and thus identify increased risk indicators of the kind exhibited by the perpetrators of the three terrorist attacks mentioned above.

So while the US is less vulnerable in some respects, the US remains highly and crucially vulnerable in other ways.

The question thus presents, in what other ways can the US improve its critical infrastructure protection against the pervasive cyber-attack threat?

One means of doing so would be to ensure there is a robust, persistent, and engaged collaboration between the federal agencies with jurisdiction over the respective critical infrastructure sectors and the operating authorities of those facilities. This need is recognized by The Department of Homeland Security (Department_Homeland_Security, Sector-Specific Agencies, 2015) and sixteen key sectors are identified with plans and programs in place for each of these sectors. DHS maintains an active posture with regard to threats, and shares available information on blogs with industry and quasi-government partners, as evidenced by the currency

of the DHS communications/alerts on the subject of managing cyber-threats (Touhill, 2016) . DHS also has an ICS "SWAT" team which engages with sectors which use ICS, and works to ensure the cyber-security of these organizations. (Department_Homeland_security, 2016) .The outreach by DHS to the energy sector and the fifteen other critical infrastructure sectors appears engaged, energetic, consistent and effective.

The active 'watchdog' function of security-industry consulting firms and think tanks is also crucial, because these organizations have the capability and expertise to provide both the 'extra-organizational' critical thinking and envisioning, as well as more tactical system/mission assurance roles. These firms benefit from worldwide visibility and extend thought leadership, and can help structure appropriate defenses to identified or potential threats for their clients. A leader in this field is IHS Janes, which has been a consistently compelling contributor to thinking about, facing and positioning positively to defend against transnational security threats in both the Cold War and post-Cold War period. The implications of the cyber-attack against the Ukraine (probably conducted by Russian attackers) was not lost on IHS Janes (Janes IHS 360, 2016).

A final comment related to implementing the '*lessons learned'* from the post-incident analysis of the Ukraine cyber-attacks is that there is always value in peer review, and that peer reviews could be put together in which one energy provider assesses the cyber-threat mitigations which have been put in place by a peer energy provider. (Potentially, if these providers are in a competitive posture with each other, then peer review participants could be 'swizzled' such that non-competitive providers are teamed up to mutually self-assess). The advantage of conducting these assessments in advance of a crisis is that the surfacing and identification of shortcomings will give the opportunity to correct them to reduce/eliminate negative impact in the event of a cyber-attack. Exercises of this kind would be consistent with the notion of a 'positive sum game', in which each participant gains incremental war fighting advances against the shared, common threat of cyber-attack; with the result that in the event of a systemic cyber-attack against the energy sector, communities affected will benefit from increased energy-sector collaboration owing to relationship building which will result from the peer-to-peer assessments conducted pre-crisis. In fact, all critical infrastructure sectors could similarly benefit.

This brief has examined the circumstances of the December 2015 cyber-attacks against the Ukrainian power grid; discussed the new and potentially dangerous geopolitical/military direction cyber-threats have taken; and has identified lessons learned from these attacks. The status of these lessons have been considered from a United States point of view to assess US preparedness and offers thoughts regarding the path forward to a more cyber-threat resilient energy sector.

References

Janes, 360, J. I. (2016, January 7). *If confirmed, cyber-attack against Ukrainian power distribution would indicate increasing threat of Russia disabling critical infrastructure abroad*. Retrieved from IHS JANES - Every Decision Matters: http://www.janes.com/article/57060/if-confirmed-cyber-attack-against-ukrainian-power-distribution-would-indicate-increasing-threat-of-russia-disabling-critical-infrastructure-abroad

CHIPS_Clearinghouse. (2016). *Clearing House Interbank Payments System*. Retrieved from CHIPS: https://www.theclearinghouse.org/payments/chips

Department_Homeland_Security. (2009, October). *ICS Defense in Depth*. Retrieved from ICS Cyber-Security: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

Department_Homeland_Security. (2015, October 27). *Sector-Specific Agencies*. (DHS, Editor) Retrieved from Critical Infrastructure Sectors: https://www.dhs.gov/sector-specific-agencies

Department_Homeland_Security. (2015). *Seven Strategies to Defend ICS*. Retrieved from NCCIC - National Cybersecurity and Communications Integration Center: https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Department_Homeland_security. (2016, February 25). *The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*. Retrieved from DHS ICS-SERT: https://ics-cert.us-cert.gov/

Department_Homeland_Security. (n.d.). *ICS Best Practices*. Retrieved from ICS-DHS: https://ics-cert.us-cert.gov/Recommended-Practices

DHS. (2016, February 25). *Cyber-Attack Against Ukrainian Critical Infrastructure*. Retrieved from Industrial Control System Cyber Emergency Response Team: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

ESET. (2016, January 21). *New Wave of Cyber Attacks Hits Ukrainian Power Industry*. Retrieved from ESET: https://www.eset.com/us/resources/detail/new-wave-of-cyber-attacks-hits-ukrainian-power-industry/

FBI. (2009, 04 01). *Spear Phishers, Federal Bureau of Investigation*. Retrieved from FBI Stories: https://www.fbi.gov/news/stories/2009/april/spearphishing_040109

FEMA. (1991, June). *Chicken Processing Plant Fires , USFA-TR-05*. Retrieved from U.S. Fire Administration/Technical Report Series: https://www.usfa.fema.gov/downloads/pdf/publications/tr-057.pdf

Klump, D. R. (2016, January 5). *Faculty Forum*. Retrieved from Lewis University: http://www.lewisu.edu/experts/wordpress/index.php/first-malware-induced-power-outage-confirmed/

McGarry, B. (2016, January 5). *Hack of Ukrainian Power Grid Marks 'New Territory,' Analyst Says*. Retrieved from DoD Buzz Online Defense and Acquistion Journal: http://www.dodbuzz.com/2016/01/05/hack-of-ukrainian-power-grid-marks-new-territory-analyst-says/

Miller, G. W. (2016, January). *Cyber-Attack Causes Brief Service Interruption in Western Ukraine*. Retrieved from Northwest Public Power Association : https://www.nwppa.org/wp-content/uploads/tech_advisory__ukraine_cyber_attack__jan_8_2016-1.pdf

SCADA Systems. (n.d.). Retrieved from SCADASystems: http://www.scadasystems.net/

Siemens. (2016, March 9). *Malware Affecting Siemens WinCC and PCS7 Products (Stuxnet)*. Retrieved from Siemens Industry Online Support: https://support.industry.siemens.com/tf/ww/en/posts/malware-affecting-siemens-wincc-and-pcs7-products-stuxnet/46366/?page=0&pageSize=10

SWIFT. (2016). *Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. Retrieved from Society for Worldwide Interbank Financial Telecommunication (SWIFT): https://www.swift.com/

Touhill, A. S. (2016, March 16). *DHS Works with Critical Infrastructure Owners and Operators to Raise Awareness of Cyber Threats*. Retrieved from DHS Blog on Cyber-Security / Critical Infrastructure: https://www.dhs.gov/blog/2016/03/07/dhs-works-critical-infrastructure-owners-and-operators-raise-awareness-cyber-threats

Ward, M. (2016, March 16). *Could Hackers Turn The Lights Out?* Retrieved from BBC News: http://www.bbc.com/news/technology-35204921

Weldon, H. C. (1997, July 16). *THREAT POSED BY ELECTROMAGNETIC PULSE (EMP) TO U.S. MILITARY SYSTEMS AND CIVIL INFRASTRUCTURE*. Retrieved from House of Representatives,Committee on National Security, Military Research and Development Subcommittee: http://commdocs.house.gov/committees/security/has197010.000/has197010_1.HTM

Appendix

Cyber-Attack in the Ukraine: Additional Security Observations and Recommendations

A number of observations and recommendations came to mind reading about this cyber-attack and although it is beyond the scope of this assignment it seems appropriate to explore some of those observations and recommendations. All of the observations listed below would mitigate a recurrence.

It is appropriate to create a culture of cyber-security. This can be done is a couple of ways. One method would be to mandate taking a custom-developed computer-based cyber-security education module. This can include either animated scenes and/or with video scenarios, and serve to instruct the staff as to best and safe computing practices. Graded or non-graded quizzes at the end of the modules can be helpful to drive attention to the best practices recommendations and cyber-security instructions. (And a departmental pizza party perhaps, in honor of those with the 'best' scores). An excellent example of building a culture of awareness (which actually relates to fire science,) is the Tyson Farms 'incipient fire force'. This is basically an internal fire awareness SWAT team; a team of more highly trained employees who are particularly alert to hazards which can turn dangerous. These get corrected immediately upon identification. This is a terrific concept, expertly implemented at Tyson Farms' chicken processing plants. This has contributed to an exemplary fire response record with no casualties. Chicken processing is inherently dangerous with many risk factors. The 'incipient fire force' SWAT team however has really held the line by identifying potentially hazardous situations in situ and contemporaneously. (FEMA, 1991)

Analytics should be applied to security incidents. In the case of the Ukrainian cyber-attacks, we saw that multiple intrusions to multiple sites were executed. There were a number of anomalous behaviors. These went unnoticed because they were not logged; and if they had been logged, there was apparently no automated or even manual mechanism to correlate these intrusions or behaviors. For example, accesses to procedure manuals and access to program directories by individuals at the different sites – all without any explicit need to view these files -- should have raised alarms. This is a challenging problem to solve, but the ability to have some kind of resource access logging and automation working in background to spot and correlate possible security threats trends is a goal well worth pursuing. Even a manual weekly review of security-related events could have served to alert that "something was brewing".

Social, mobile and IP-enabled computing did not appear to play any role in the Ukrainian power plant intrusion an attack, however it may well have; the circumstances are fully understood at the time of this writing. The ever-present danger of social/mobile contributory factors mandate that attention be applied to this consideration. For example, if an infected smartphone has the password to access a power plant intranet, that's a problem (and similarly for an onsite located ATM or IP-enabled video surveillance capability).

Password discipline may well have played a role in this case. Passwords must be auto-invalidated and employees must either choose new ones or (better yet) have strong new passwords assigned periodically. If this is not done, then an old password can provide access to sensitive resources and over time, the general experience is that 'old' passwords get divulged. In addition, passwords assigned to employees who have been terminated or moved on are too often never deactivated.

UPS and Power Interruptions for Critical Infrastructure

One of the important points to be made about critical infrastructure has to do with uninterruptible power supplies (UPS), and how that technology factors into continuity of service and production in a critical infrastructure environment. After all, if the power goes out and critical infrastructure has UPS installed, and if it works as advertised -- then what is the issue? To answer this, we need to look under the hood a bit and identify the main issues and problems. UPS systems work (at a simplistic high level, at the outer limits of my knowledge) as follows: the equipment in question receives power from the public power grid. That equipment is also connected to a UPS unit which contains a battery capable of providing power to run the unit for a period of time. (In some scenarios, the equipment runs not off the power grid directly but off the battery in the UPS unit which not only protects the operations of the attached equipment but also conditions the power continuously, feeding the attached equipment pre-smoothed out power for optimal power feed). In any event, the battery continuously recharges from the public power grid (when the power grid is available, up and running and all is well). If the public power supply suddenly has problems and is "bursty" or fluctuating, or actually dips downs and disappears, the UPS *senses* that power fluctuation (or detects the total loss of power) and automatically (almost instantly) switches the protected device from public power to battery power (which is at full power due to having been continuously charged). The protected equipment usually survives the transition with zero impact; even in sophisticated mainframe computer installations, the most recent CHIPS[4] (CHIPS_Clearinghouse, 2016) or SWIFT[5] (SWIFT, 2016) financial "transactions-in-flight" or multiple, simultaneous datacenter distributed database "commits" will survive the power "glitch" with no loss of data. (One certainly does not want a loss of data during a billion-dollar money transfer after all!).

After the power loss event, the equipment and/or computers are then running off the batteries in the UPS unit. Naturally, batteries have a limited amount of power, so many installations, notably those running critical instrumentation or medical equipment or banks of computers and disk drives – will also have diesel-fuel generators. These generators will be turned on and will continuously recharge the batteries which are running the equipment or computers. This all works well, of course provided the generators don't sustain some kind of equipment failure and/or run out of diesel fuel. During Superstorm Sandy, running out of fuel was a distinct

[4] Clearing House Interbank Payments System (CHIPS)

[5] Society for Worldwide Interbank Financial Telecommunication (SWIFT)

possibility, and a clear and present danger to many critical infrastructure installations including hospitals.

(On the point of hospitals, during Hurricane Sandy several NYC hospitals had a serious crisis on their hands because *their basements – where the batteries are stored – were flooded*! This meant that when the power grid failed, the onboard batteries (inside the equipment) to run the life support equipment quickly became dangerously depleted and those critically ill patients had to be transported 'stat' to uptown hospitals to prevent their deaths. So we can that exogenous variables and black swan events can notoriously intervene between the best plans of mice and humans….)

So the important point here simply is that switching to UPS will preserve the computer data transactions and production capability of the equipment thus protected – but only for short while, and only if the attached diesel-fuel generators function effectively and there is an adequate supply of diesel fuel! If either of those factors fail, and if the power grid does not return before the batteries become depleted running the equipment, the installation's computers or equipment will ultimately fail – a *delayed* fail, but 'down hard' eventually.

SCADA Attack Characteristics

Malware targeting SCADA systems can attack in various ways. One approach is to flood the SCADA network making communications between the SCADA system and monitored/controlled Industrial Control Systems impossible or very slow, tripping thresholds and aborting connection attempts. Some malware attempts to shut down the SCADA supervisory computers. Other attacks create spurious network traffic prohibiting human supervisors from seeing the underlying attack occurring. This last scenario was implemented in the December attacks and perhaps also the January attacks. (Klump, 2016)

International Collaboration

"An interagency team comprised of representatives from the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation traveled to Ukraine to collaborate and gain more insight. The Ukrainian government worked closely and openly with the U.S. team and shared information to help prevent future cyber-attacks" (DHS, 2016)

…Other Risks to the Power Grid…

There are however other emerging (and grave) concerns for the energy sector which do not involve cyber-crime and therefore appear to not have attracted much attention. One of these growing concerns is the potential of a low-yield atomic device being detonated over a high population area, potentially delivered from an innocuous fishing trawler off our shores firing a crude cruise missile (or seaborne Scud). Such a device could create an electromagnetic pulse which could disable large swaths of our electrical grid with disastrous and widespread disruption of our way of life. These grave circumstances have received occasional attention in Congress viz (Weldon, 1997, p. 1). An implacable, ruthless and creative enemy capable of conceptualizing an attack by passenger aircraft against population center buildings crowded with work-a-day office workers going about their daily lives seems more than capable of creating and implementing such an attack plan. Every indication of the advance and dissemination of nuclear technology and rogue state behavior directs us to the conclusion that such an attack is increasingly possible with each passing year. So while 'garden variety' cyber-attack remains a threat against our critical infrastructure - against which the US has robust defenses- the US should never underestimate the capabilities of potential (or especially avowed) enemies to the US's way of life. DHS should take the lead in engaging in 'outside the box' attack conceptualizations, and draw up technical plans and financial assessment framework to effect the hardening of the currently vulnerable energy grid.