193 Southdown Road
Edgewater, MD 21037

July 12, 2018

Mr. John R. Bolton
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Avenue, Washington D.C. 20500

Dear Sir,

Attached is my seventh white paper titled: "Security in the North American Grid – An Existential Threat", July 10, 2018.

Since 2011, copies of all previous papers have gone to your predecessors. Industry fragmentation, the EPA of 2005, and many other issues absolutely rule out this industry, or its overseers (DoE and DHS), from preventing, or recovering from, a cyber attack. The nation's electric system can continue its defenseless posture, or the nation's leadership can declare it "off-limits" to our adversaries. There are no other choices.

As the enclosure, and previous papers have documented, Russian military cyber forces (the GRU, supported by the SVR) have had unlimited access to conduct reconnaissance and analysis of the vulnerabilities of our electric networks since at least 2012, including last year's penetration of nuclear generation facilities. Executive Orders, Justice and Treasury sanctions, and recent indictments have not deterred them. The industry, regulators, and DoE/DhS cover-up of these incursions has only encouraged the Federation. The media is hot on the trail of this national affront.

The enclosed study fully supports the Defense Science Board recommendation of deterrence with measured retaliation, which aims to protect the nation's National Security organizations from what would be a cataclysmic loss of commercial power. The risks are beyond argument. If the White House cannot address this issue, I urge you to have the Secretary of Defense make the call.

Respectfully,

George R. Cotter

George R. Cotter

Enclosure: a/s

Distribution:

Assistant to the President for National Security Affairs
Attorney General of the United States
Secretary, Department of Defense
Undersecretary of Defense for Acquisition & Sustainment
Chief, National Guard Bureau
Secretary, Department of Energy
Secretary, Department of Homeland Security
Director, National Intelligence
Commander, Cyber Command/Director National Security Agency
Director, Central Intelligence Agency
Director, Federal Bureau of Investigation
Chairman, Federal Energy Regulatory Commission
Chairman, Nuclear Regulatory Commission
Director, National Institute of Technology and Standards
Chairman, House Committee on Homeland Security
Ranking Member, House Committee on Homeland Security
Chairman, Senate Committee on Homeland Security & Governmental Affairs
Ranking Member, Senate Committee on Homeland Security & Governmental Affairs
Chairman, Senate Select Committee on Intelligence
Ranking Member, Senate Select Committee on Intelligence
Chairman, House Permanent Select Committee on Intelligence
Ranking Member, House Permanent Select Committee on Intelligence
Chairman, Senate Energy and Natural Resources Committee
Ranking Member, Senate Energy and Natural Resources Committee
Chairman, House Energy and Commerce Committee
Ranking Member, House Energy and Commerce Committee
Chairman, Senate Armed Services Committee
Ranking Member, Senate Armed Services Committee
Chairman, House Armed Services Committee
Ranking Member, House Armed Services Committee

Security in the North American Grid

The Existential Threat

A White Paper

Abstract

Seventh in a Series of Studies of the Security Vulnerabilities of the North American Electric Grid. This White Paper Examines the Reasons for Failure to Protect the System, the Increasing Risk to the Nation, and the Need for a Strong Deterrence Polccy.

George R. Cotter

grcotter@comcast.net

July 10, 2018

Disclaimer: the information in this White Paper is all from the public domain. The judgments, conclusions and recommendations are solely mine, unless annotated. There are no endorsements by any organization and none are implied.

George R. Cotter
July 10, 2018

Security in the North American Grid – The Existential Threat, A White Paper

Outline

Security in the North American Grid – The Existential Threat

A White Paper

Motivation

Is there any infrastructure more critical that the nation's electric system? Other national infrastructures greatly dependent on commercial power include communications, transportation, health and medicine, financial, governments at all levels, and national security. Over nearly its entire existence, the nation has not had to worry about the security of its domestic institutions. But with explosions of information technologies, and the Internet, all that has changed. "Fortress America" is now "Target America", a cyberwarfare priority for the nation's adversaries.

However, It is a unique period in our national security history wherein classical policies and organizations for protection of the nation from determined cyber adversaries have been deliberately sidelined by two Administrations, with incoherent strategies and federal agencies Incapable of even a minimal defensive strategy and totally devoid of both defensive and offensive cyber forces. Powerful electric and IT industry forces exploit these weaknesses and collude with their federal counterparts in minimizing or covering up Russian reconnaissance and assaults on the North American Grid.

Given this frozen cybersecurity policy, the existential threat to the US Grid, commercial power-dependent military, cyber, and intelligence organizations challenged to defend this nation, including other power--dependent critical infrastructures, are now facing mature Russian Federation Cyber and Information Operations capabilities that have convincingly and unopposed, targeted the grid for at least 7 years. And the nation's only remaining defense is its nuclear triad.

I. Introduction

The six previous White Papers on ***Security in the North American Grid*** addressed the structural complexities of the nation's electric system, the functions and methods employed cooperatively by utilities for operating and managing it across the lower 48 states and District of Columbia, and Cybersecurity Infrastructure Protection (CIP) Standards that have evolved under laws over the last two decades. The White Papers summarized related actions by the Administration, Congress, two regulatory commissions, oversight agencies (DoE and DHS), and Presidential Executive Orders intended to invoke, clarify or augment CIP standards. Vulnerabilities of the electric grid, threat information from open sources, and actual attacks on infrastructures were described, as well. White Papers were distributed to the nation's leadership, six Congressional committees, the White House (National Security Advisor), DoD, DHS, DoE, the DNI, CIA, NSA, FBI, FERC and NERC. The objective was to inform national cybersecurity policy on critical infrastructure protection.

This White Paper largely focuses on Vulnerabilities and Threats, including a critical view of industry, regulatory and federal approaches to cybersecurity for electric systems, which this paper labels ***The Existential Threat.*** Further, the threat discussion includes details on Russian incursions in the Grid dating from 2012.

Appendices provide background on the Electric Industry, Critical Infrastructure Standards, Russian Federation Cyber Organizations and Capabilities, and Supply Chain systems being targeted.

The Bottom Line. The nation is at an impasse, a political impasse. The industry, Congress, its regulators cannot come to grips with cyberattacks on the Grid; now an existential threat from inaction and inabilities to confront foreign adversaries. National cybersecurity policy is frozen on dead center, the elephant in this boardroom is Russia's involvement in the 2016 election. But it is also Russia that is the major threat to the North American Grid. In fact, it is the same Russian Federation organizations involved in both attacks, the SVR and the MOD/GRU. Their capabilities have developed to where their Cyberwarfare tools, training, reconnaissance and testing puts Russia in control of the Grid as a battlespace, the electric industry, regulators, and overseers of cybersecurity efforts, and six White Papers on this topic notwithstanding. It is a December 6, 1941, September 10, 2001 national "moment".

It is simply outrageous that an Act of Congress, the **FAST Act**, intended to protect sensitive Critical Enterprise Infrastructure Information (CEII) should be abused since 2014 to suppress information on the coordinated testing of Russian cyberattacks on this nation's, and Ukraine's, electric systems. Misuse of this authority permits utilities to hide vulnerabilities, data breaches, weak regulatory decisions, ineffective oversight, near complete absence of protection, lack of coherent national policy. This conspiracy ensemble includes large utilities, the industry, the regulators, DoE, DHS, two administrations, several embarrassed IT firms, and, of course, Mr. Putin.

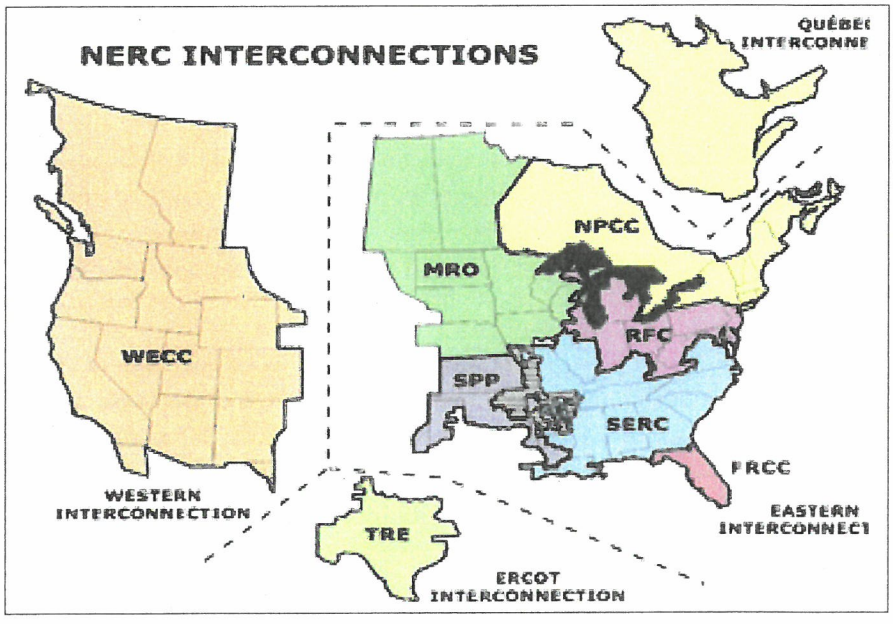
Comment. The industry and the nation are paying a huge price for cybersecurity protection, both dollars and manpower with the gap between adversaries' offense, and industry defense growing ever wider. Funding and industry intellect devoted to modernizations should take precedence. National action is way overdue, but the only choice left to the nation is the Grid-focused recommendation of the Defense Science Board ***"Task Force on Cyber Deterrence"*** February 2017 that would put Critical Infrastructure "off-limits" to the nation's adversaries with measured retaliation the consequences for crossing that red line. The current Administration's "Saving Coal Mining" initiatives blatantly uses DOE's role in supporting National Security interests, to cite Cybersecurity risks in moratoriums on early retirement of coal-fired, and nuclear generators, an absolute farce, (more later). Utility and therefore consumer costs of electricity will rise. ***The major purpose of this White Paper is to document this inescapable conclusion that the nation is past the tipping point on threats from the Russian Federation and on Critical Infrastructure Protection costs inflicted largely on itself, such as this DoE initiative.***

II. The Electric Industry – A Huge Security Challenge

Federal industry deregulation was well-underway as cybersecurity emerged as a challenge to the nation's critical infrastructures. The Energy Power Act of 2005 was created by congressional reaction to the North East blackout of 2003, but applied primarily to the Bulk Power System (**BPS** aka **BES**) limited to ***Transmission*** and related Generation resources in the lower 48

States, leaving ***Distribution*** Systems (local utilities) under the jurisdiction of the individual States including Alaska and Hawaii. Nuclear Generation sites covered by the Atomic Energy Act of 1948 were also omitted from the EPA. Congressional intent was clearly to continue the deregulation trend of the 1990's. To this end, the EPA authorized creation of an industry group to formalize Reliability and Cybersecurity Standards, an Electric Reliability Organization, ERO. The Federal Energy Regulatory Commission (FERC) role was limited to approval of such standards. Thus, the die was cast for far-from-complete coverage of only long-haul Transmission Systems and related Generation facilities supplying bulk power for interstate commerce.

Interstate power transmission tariffs are regulated by FERC involving over 3200 independent and semi-independent firms and cooperatives. This business activity has been labelled, the Bulk Power System, BPS. Consolidation of these many electric entities into multi-layered consortiums, many across state lines has required FERC to establish controls to ensure sales of electric power across these boundaries are competitive, i.e., market systems free of manipulation. There is basically a wholesale (day-ahead) market and a spot market (an oversimplification with lots of qualifiers). To ensure a continuing flow of electric power through ***Distribution*** Systems to consumers, at the lowest possible cost, the EPA produced formalized ***Reliability Districts*** to independently oversee operations and order ***"Registered Entities"*** to make necessary adjustments to critical power flows required for a functional BPS. Entities include Regional Transmission Organizations, Transmission Operators, Generator Owners, Generator Operators, etc. Most such entities are merely **"double-hatted"** industry consortiums; charged with maintaining separation of business decisions from **"Reliability"** functions. Example: PJM is the RTO for the central Atlantic region (19 major operators) and ***Reliability First Consortium (RFC)*** oversees the **"Reliability District".** The shallowness of this arrangement can be seen when PJM frequently speaks for the RFC.



The map above shows the eight Reliability Regions.. Note: SPP has petitioned FERC to cease Reliability Operations and divide their ***"Registered Entity"*** utilities between the MRO and SERC. Note also that with extensive power exchanges with Canada, Reliability Regions include separate agreements with adjacent Canadian Provinces.

Not shown on this map are subdivisions in Reliability Regions, semi-autonomous in reliability functions since they align with physical BES transmission lines owned by individual, large utilities. Also not shown on this map are Independent System Operations (ISOs such as CA ISO, NE ISO, NY ISO etc.) and Regional Transmission Organizations (RTOs), representing regional integrated operations, functional entities that almost always speak for their utilities on Reliability and/or Cybersecurity issues. Example: FERC recently tasked ISOs and RTOs for comments on reliability and cybersecurity views on energy supply tariff issues.[1]

Further discussion of industry issues follows in ***Appendix I, Reliability and Resiliency.***

III. Critical Infrastructure Protection (CIP) Standards

Following the passage of the EPA of 2005, NERC and FERC's chose to develop and apply CIP Standards to individual facilities, thus foreclosing Grid-wide protective mechanisms and processes., e.g., cross-utility linkages and their vulnerabilities. This exclusion extends to communications and networks linking physically separate facilities (e.g., a utility network between a control center and its substations are explicitly excluded from CIP Standards, i.e., CIP v5-002-1a. CIP standards end at the "Physical Security Perimeter", i.e., the fence line. This has led to extraordinary NERC/FERC struggles to address vulnerabilities arising out of, for example, Supply Chain exploitations by the Nation's principal adversary, Russia.[2]

Between 2005 and 2008, there were substantial discussions between FERC and NERC and tangentially, with congressional staffs on the intent of the EPA. Congressional staffs urged the industry and FERC to adopt NIST standards, then applicable to Federal agencies.[3] Voluntary cybersecurity standards in place were eventually grandfathered into Order No. 706 as CIP Version V3. There were obvious differences on how each of the Reliability Regions viewed coverage, with major differences on what utility organizations voluntarily included under the standards.

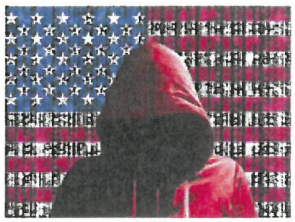
FERC was unhappy with the wide statistical variations in proposed coverage of cyber systems in **CIP v3**, the principal issue being the relationship between operational systems and their associated cyber assets. NERC proposed a substantial revised set, **CIP V4** with "brightline" criteria for CIP categorization. However, FERC continued to have difficulty with voluntary categorization. NERC and the industry proposed **CIP v5** with criteria for three categorizations of cyber assets, low, medium, and high impact that theoretically ended "voluntary" categorization. But **CIP v4** was never implemented. **CIP V5** was formally approved by FERC in Order Nr. 791 in November 2013. Twiddles with requirements and metrics over the next several years produced the **CIP v5/v6/v7** set, (see ***Appendix II***) including CiP-014-01 on physical security following the attack on the Metcalf substation in Silicon Valley.

CIP Standards are, by design, a proforma, high level set of security objectives intended to influence, not proscribe, selection of cyber protection systems by utilities. Unlike the extremely detailed standards in NIST SP

800-53, preferred by Congress in passage of the EPA of 2005, NERC CIP Standards have not served as an acquisition technical check-list for utilities. Compliance reviews are therefore hardly much more than very subjective, tabletop assessments, so general in fact, that little or no commercial support activity for CIPs has been fielded by major security technology firms. And CIP is barely mentioned by major IT suppliers. Only a major incident is likely to invoke discussion of violation severity levels (VSLs) tied to CIP requirements. Even then, under rules promulgated by RAI[4] there must be demonstrable negative effects on the BES for penalties to be assessed. Other than a mandatory but anonymized annual report to FERC, compliance with CIP Standards is non-public. Further, NERC continues pressure on FERC to make the annual RAI report, non-public.[5] Further details on CIP Standards are contained in ***Appendix II***.

> ***Comment:*** CIP Standards are hardly more than a "feel-good" placebo for regulators and other overseers. CIP Standards are simply ignored in the hundreds of media reports on Grid attacks; in the technical feedback from security firms and the NCCIC/US CERT alerts and advisories. CIP Standards have had no value in protecting the Grid from foreign adversaries; they certainly have been no impediment to the SVR or GRU since they turned to the Grid as a major malware target in 2012. The major reasons the Grid has been an easy Russian target are (1) how few cyber assets are covered under CIP Standards, (2) the exclusion of communications and network linkages despite extensive Internet connectivity by utilities, (3), the absence of hard technical requirements in standards, and (4) the extremely weak compliance system in use.

IV. Major BES and Distribution Vulnerabilities



1. Grid Fragmentation

Many issues arise out of the regulatory fragmentation in the Nation's power system, notably state and national tariff inconsistencies, oversight of nuclear facilities, accesses and rights-of-way, modernization initiatives, reliability/accessibility to energy sources, interoperability, environmental protections, and or course, operational reliability and security of the connected mass. Almost every advance and improvement invokes debate, negotiation and delays. FERC and the NRC are not responsible for this situation, it's the product of the industry and the Congress. An integrated national cybersecurity system is needed for defense of the Grid but under the current law legislating fragmentation, it is hopeless.

2. Systemic Vulnerabilities

a. Nation-wide Situational Awareness

The absence of an integrated Grid-wide capability to detect attacks aimed at controlling and/or disabling local, regional or national targets represents a vulnerability of staggering proportions. How do the Cyber Command and State National Guards respond? A structure for real-time situational awareness across both BES and Distribution facilities needs to be created and linked directly to intelligence and other alerting systems for early warning, defense, and response. The control of this structure can be vested in civil authorities in peacetime but must revert to national security authorities in cyber warfare. This is standard authority transfer in other disciplines (e.g., State National Guards).

Several additional pieces of such a structure are in place, for example Reliability Regions, the 200+ network of sites coordinating frequency stabilities, the DOE CRISP initiative, networked Synchrophasor sites. For years, the National Synchrophasor Initiative (NASPI) has been working informally in development of standards, data exchanges, application development, and networking of Distribution facilities (with much progress in the WECC); organized industry cooperation has been lacking, however, signaling the limits of "togetherness" that is critical to a reliable, resilient and secure electric system.

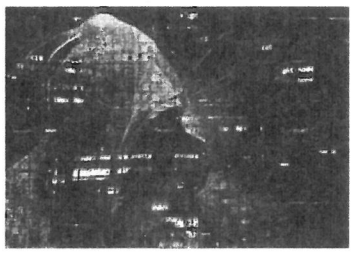
b. Communications and Networking

The exclusion (CIP 002-5.1a) of communications and networks linking so-called Electronic Security Perimeters (ESPs) represents not only a major vulnerability, but also has unintended security consequences across many other grid functional areas, e.g., supply chains that cross the Internet. NERC's argument for this exclusion was specious; utilities do not "own" commercial carriers. A plethora of conflicts has emerged; examples: Control Station to Transmission substation communications and Control Center-to-Control Station security. There cannot be a Nation-wide integrated network as described above, without eliminating this CIP 002-5,1a exclusion.

c. BES Categorization

The distribution of Cyber Assets into Low, Medium and High categories miss-labels many hundreds of cyber systems relative to threats to the BES overall, and by extension, to the entire U.S. Electric Grid. The issue is particularly acute for so-called Low Impact Cyber Assets. Permitting each utility to decide to include or exclude a Transmission Substation in coverage by CIP Standards makes it virtually impossible to operationally integrate cybersecurity for large, regional Transmission organizations such as PJM, with 19 major utilities involved. PJM operationally manages 19 utilities' Transmission systems yet must leave operational cybersecurity management in the hands of each utility. Note FERC negotiates Tariffs with PJM, not the separate 19 utilities; but NERC and FERC assiduously avoid operational cybersecurity standards which would transcend a utility's boundary. Consequently, Russia has had no difficulty in exploiting the seams in the BES. Note that FERC tasked the ISO's and RTO's for comments on cybersecurity resiliency,[6] not individual utilities, in addressing Secretary Perry's resiliency NOPR task. ***Appendix II*** contains a more detailed discussion of CIP Standards.

d. Internet Connectivity

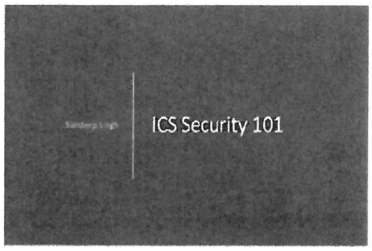


In many of their advisories and alerts, ICS CERT states, relative to Internet dependencies, ***"If you're connected, you're infected",*** and with good reason. Most of ICS CERT's incident studies reveal direct Internet connectivity and associated poor vendor and grid security practices.[7] The issue is endemic to the industry. Shodan Internet scans reveal thousands of direct vendor connections for remote service of a huge array of instrumentation and control products left to the OEMs to maintain.[8]

Note that the proposed CIP 003-7 requirement for "responsible entities" to control transient service connectivity deals with vendor technician physical access to Low Impact Cyber assets but appears to leave wide open vendor remote access across the Internet to such facilities. NERC and the industry's view that so-called low impact cyber assets are low risk to the BES is nonsense; connectivity to control systems and other substations provides pathways for malware. Internet connectivity is therefore, a major component of an adversary's attack

vectors for phishing expeditions, reconnaissance, malware insertion, intelligence collection and data extraction. See ***Appendix III Russian Federation Cyber Organizations*** for details.

e. Industrial Control Systems



Perhaps the most neglected segments of Utility cybersecurity involve Industrial Control Systems (ICS). This is due to aging of systems never secured, to the variety of vendors, to the increasing complexity of substation environments, and the absence of systems to securely manage ICS across the substation. But it is also because modernization programs are diffused and frequently lack hard requirements for security, physical or cyber. The very complexity of multiple mixes of vendor ICS product and their end-to-end importance has led the international community to develop interface standards, e,g,, IEC61850 for interoperability. And yes, for connecting low, medium and high impact cyber assets. Hence, IEC61850 is the operational component of Russia's ***Industroyer*** malware.[9]

The Synchrophasor (PMU) Map discussed in ***Appendix I*** illustrates the increasing complexity of ICS, and their importance. Precision power measurements together with use of GPS timing signals from a subset of such sites permits regionalized power management, certainly good news for reliability but quite significantly increasing the risk of cyber targeting. Security of substations and their ICS has never been more important. At least one utility understands this.[10] What the Russians undoubtedly know is how to interfere with PMU controls and data flows to achieve the purpose of the attack, e.g., Lights Out in Manhattan.

f. Data Flows

Much has changed in the automation of Grid functions, PMUs included. Data feeds to control stations to utility Energy Management Systems (EMS) originate far less often from technicians monitoring sensors feeding SCADA systems and increasingly (and often autonomously) from intelligent ICS.[11] BES Reliability Centers (e.g., Reliability First Corp/PJM) are taking advantage of such data flows for their real-time operational management functions. Some standardization is occurring, led by International standards-setting bodies, and organizations like NASPI. But data flows, repositories, applications and analytic exchanges are carefully circumscribed in the NERC standards setting process. Russia of course, knows this also.

It is therefore fair to ask, how secure are Data Flows from disruption, or worse, manipulation? Encryption is used by some utilities but is of questionable value in the absence of a universal, end-to-end secure data flow architecture.

g. Control Center Systems

The major technique used in the Russian takeover of the Ukrainian Distribution Systems in December 2015, was phishing attacks for credentials to permit capture of Control Centers. Ukrainian technicians watched their HMI cursors moving, being controlled remotely by Russian operators. The Ukrainian attack tested capabilities to take over HMI functions, to modify ICS systems including firmware, and disable emergency power systems. Actual damage was limited to takeover efforts, no intentional destruction was observed.[12] The earlier 2014 attack on the US Grid apparently involved subversion of Control Center Systems (beginning in 2012) using ***Havex*** and ***BlackEnergy*** malware, seen later in the follow-on Ukraine attack. The forensic details of that extended effort in the US Grid were bottled up by DHS, except for industry briefings. However, the ultimate objective of these Russian efforts was to test access to ICS systems through associated control systems. And reconnaissance by the

same Russian organizations has continued in the US. ***Incredibly, there has been no concerted industry or federal (NERC/NRC/FERC) action to pressure Control System vendors to secure their control system development and Grid support processes.***

h. Supply Chains

The security integrity of industry products is, today, highly suspect; vulnerable components often originate abroad. Flaws in development and production of vendor-unique systems often escape notice until they show up in a zero-day exploit. The recent disclosure of Meltdown and Spectrum, CPU architectural flaws, shows clearly that systemic vulnerabilities can exist for many years, undetected (but may have been known to nation/state cyber organizations).

Foreign adversaries have many ways to penetrate Supply Chains, down to the hardware electronic component level, and more easily in Software updates, often at vendor's plants. Testing by individual utilities would be impossibly costly. CIP Standards as drafted require utilities to develop defenses, but that guidance would specifically enjoin utilities from putting pressure on vendors. This is highly questionable guidance; how else to leverage vendors to test their products, and control access in the Supply Chain. Third party testing, Whitelisting and Blacklisting would quickly turn this situation around.

The issue is all but hopeless with vendor practice of developing utility-unique systems that operate on commercial information technologies, e.g., Windows OS, Linux OS, commercial data base systems, and networking systems with their numerous security issues. NERC has crafted meaningless standards that require utilities to address this complex vendor issue. The burden needs to be put squarely on the utility vendor, the middle man in this muddle.

A more detailed discussion of Supply Chain vulnerabilities is at **Appendix IV**.

3. Vulnerability Summary

The vulnerabilities outlined above are fundamental, indeed "systemic". By design, there is little that the Industry and NERC can, or will do to assuage real technology risks to the BES. This coalition has successfully hunkered down behind (1) the absence of damaging Grid attacks (2) general and non-specific CIP requirements, (3) use of the FAST Act authorities for deception, and controlled suppression of Russian incursions reconnaissance, over recent years, and (4) a "frozen-in-place" national leadership that has been largely in denial of the threat. There has been no serious effort to ensure compliance of admittedly, inconsequential CIP standards, with consistent attempts by NERC to water down reporting requirements and put compliance assessments under "no-public-release" wraps.[13]

V. The Existential Threat

1. Introduction

The danger to the nation in permitting Russia (or any adversary) freedom to run reconnaissance operations against the US Grid (BES and all other segments) should be obvious; understanding the "battlespace", its topology, its technologies, the way it functions, the fragmentation and all its vulnerabilities allows for adversarial development of cyber weapons, attack planning, cadre training, integrated war planning, augmented

kinetic weapon strategies, and more sophisticated information operations. Side benefits to adversaries include understanding effects of power loss on other critical infrastructures and most importantly, on national security systems. That cycle would also undoubtedly enhance the adversary's cyber defensive planning and operations. The risks of enabling the nation's adversaries across this spectrum are incalculable, but we can see from natural disasters the effects of power outages on society, health systems, governance. And these natural disasters (e.g., hurricanes) are small scale compared with what large urban, regional and national environments and populations would experience in a cyberattack.

Comment. As a nation we have failed badly in permitting the gap to widen significantly between Grid cyber defense and our adversaries' offensive capabilities. Russia's offense is far ahead of Grid defense. And the question is "Why?". Yes, we are witnessing, for the first time, security challenges to Civil Infrastructure with terrible policy issues, misguided organization, little precedence for defenses, direct constitutional conflicts (privacy for example), a badly confused technology industry, and very uncertain priorities. There is little reason or logic for the poor security situation in the North American Grid, with many contributors to that confused state, hence the title of this white paper, "The ***Existential Threat".***

2. The Public

American citizens are overwhelmed daily with cybersecurity issues that have left then tone deaf on vulnerabilities and foreign threats. Only the victims of loss of power due to natural disasters may wonder about electric reliability and resiliency but put these concerns aside when power is restored. Weather outages are mercifully of short duration, except where long-term damage occurs (e.g., Puerto Rico). And for power loss in natural disasters, the "haves" vastly outnumber the "have nots". But the leadership in industry, the Congress, the Administration, understand that potential cyberattacks can vastly increase the "have nots" and if limited in scale and duration, may not be limited in the cascading effects on other national infrastructures. In truth, there are few cybersecurity lessons extrapolated from such events.[14]

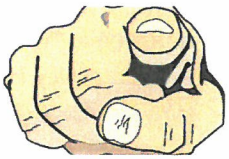
Comment: Admittedly, the EPA of 2005 attempted to extrapolate both reliability and cybersecurity lessons-learned from the infamous 2003 Northeast power outage. However, if that same blackout occurred today but for cybersecurity reasons, not a naturally-occurring cascading event, the nation would quickly conclude that the EPA was woefully insufficient.

A textbook example of potential regional effects of a cyber attack can be inferred in the Lorna Prieta, California earthquake of October 17, 1989. It was titled a "Lifelines Earthquake" because of its effects on other major regional infrastructures; one of the few natural disasters studied from a multiple infrastructure viewpoint. In this event, five major substations were affected, several destroyed. 13 miles of gas pipeline were significantly ruptured, with a spectacular fire in San Francisco. ***"The poor performance of emergency power affected several lifelines and critical facilities, including powerplants, telephone-company central offices, airports, water systems, hospitals, and emergency-operation centers."*** A cyber attack on a major urban center would be structured to cause similar service disruptions, sustained for the period of the attack. First responders to cyber attacks (e.g., state national guard units) could benefit from this study. National grid and political leadership should deeply study these natural events to understand the advantages and disadvantages of an "Islanding" strategy for Grid resilience.

3. *The Industry*

With over 3000 commercial, cooperatives, and federal corporations contributing, the North American electric system is an engineering marvel; an historic example of commercial, yet competitive, collaboration. At the same time, it is an outstanding menace to the security of the nation. Responsible cybersecurity performance falls low in priority, with costs, liabilities, energy supply, competitive forces, and of course regulatory fears taking precedence. But there is no excusing the deliberate policy of suppressing Russian incursions in mandatory incident reporting, a very welcome advantage to the nation's information warfare adversaries. See ***Appendix III***.

4. *The Congress*



In the cyber tradeoffs between security of the nation and industry deregulation, the Congress has consistently opted for the latter. For cybersecurity, the EPA of 2005 may be the worse legislation of all times, handing the industry self-regulatory authority for protection of national interests and disenfranchising both FERC and the NRC. Over a decade later, after Russian efforts to compromise our election system, major Russian incursions in the North American Grid, and excellent intelligence on the foregoing, this Congress remains institutionally impaired to address the threat. Note all six previous White Papers were sent to six congressional committees, majority and minority chairs.

5. *Regulatory System*

Given the foregoing, it might be argued that the regulatory commissions should get a free pass on the threat to the nation. But both commissions with their substantial staffs have not been blindsided on the threat to national security and have carefully sidestepped their obligation to protect the public's interest. FERC has consistently defaulted to NERC's invocation of the industry's "EPA red lines". Like the industry and the Congress, FERC remains in intentional denial as it goes about the business of supporting the electric industry's priorities. Six White Papers, numerous filings and face-to-face meetings have had little effect in getting the commissions to understand their responsibility to the nation.

6. *Department of Homeland Security*

A coherent policy for the protection of the nation's electric system has never emerged from DHS. It has direct linkages to the nation's intelligence reporting but continues to support the electric industry strategy of self-protection, articulating information sharing and "resiliency" and absolutely minimizing Russian targeting of the nation's electric system. The 2017 NCCIC annual report just issued[15] clearly illustrates this agenda; loaded with statistics but not one word about Grid attacks, the perpetrators, failure of defenses, etc.

Comment: From its inception, DHS has kept its distance from the National Security Community. Its independence has led it to policy and agenda positions at the other end of the threat spectrum. It has not directly addressed threats from obviously determined nation/state adversaries a". Throughout the 2014-2016 onslaught against the US and Ukraine Grids, DHS avoided identifying Russia, with White House polemics as cover. If that nation appears in an NCCIC Alert, it is because a DoJ or FBI action presaged it. This reticence is seized upon, and skews national policy. What a shame with so many of DHS organizations doing yeoman work on behalf of the nation, e.e., the Coast Guard. Much needs to be done with the National Guard, Military Reserve Forces, NorthCom, CyberCom for cyber defense; the DHS badly needs to be reoriented. One step is to make DHS a full member of the Intelligence Community so it begins to learn its obligations to the nation and its citizens, not just its commercial institutions. To coin a phrase, ***"What's good for the electric industry is not necessarily good for America."***

DHS has consistently underplayed the Russian threat, most recently in their NCCIC Alert TA18-074A, ***issued fully two years after the current Russian Campaign started.*** It was the first public challenge to Russian Cyber Grid aggression, evident since 2012, undoubtedly forced by a DOJ indictment of Russian MOD/GRU officials for cyberattacks. DHS was admittedly restrained by Obama's "Internationalist" views of Cyberwarfare but was under no pressure to minimize Russian activities and had many opportunities to articulate coherent policy, supporting DoD's conclusion that defense of the Grid at present is hopeless and supporting the DSB's recommendation on Deterrence. DHS lacks "active defense" assets, i.e., forces to counter cyber attacks on critical infrastructures and should learn to partner with DoD and IC organizations that have that mission.

As the federal department established to provide "Homeland Security", DHS must track other major federal actions involving attacks on the Grid; it is forced to publish notices or alerts paralleling FBI pursuit of Russian cyber law breaking, Alert TA18-074A for example, particularly after badly botching the joint release on the US election incursions titled Grizzly Steppe.[16] Triggering that Alert was the Treasury Department's March 15, 2018 designation of ***"sixteen Russian government officials, members of the Russian leadership's inner circle, including a Russian bank pursuant to Executive Order (E.O.) 13661".*** And more recently, Treasury designated five Russian entities and three Russian individuals for sanctions for violations under the same E.O.[17] It stated:

"Examples of Russia's malign and destabilizing cyber activities include the destructive NotPetya cyber-attack; cyber intrusions against the U.S. energy grid to potentially enable future offensive operations; and global compromises of network infrastructure devices, including routers and switches, also to potentially enable disruptive cyber-attacks. Today's action also targets the Russian government's underwater capabilities."

Appendix III to this White Paper summarizes both **NotPetya** and **(VPNFilter)** malware**,** the former a DDOS tool that probably got away from the GRU causing world-wide mayhem for Microsoft-7 users, including Russia; the latter was a devastating blow to a major US network firm, CISCO. Note these were embarrassingly damaging events and could not be ignored. DHS admits to working with the FBI on these "violations". Why then is there deliberate suppression of similar information on the third major justification for Treasury sanctions ***"cyber intrusions against the U.S. energy grid to potentially enable future offensive operations"?*** Could it be because those "intrusions" have no major Russian firm to sanction? Rather is it because it involves the Russian Federation military cyber organization, the GRU, not readily sanctionable, and direct confrontation of Russian leadership is a policy ***"no, no?"*** Does Treasury have hard evidence that the FSB is behind these events when all the forensic evidence points to the GRU?

Comment: There is clearly agreement within the federal establishment and the electric industry in suppressing the actual details of Russian intrusions in the US segments of the North American Grid; a practice that dates from 2014 major events to most recent 2017/2018 incidents. Obama tried and failed to convince Putin of he futility of cyberwarfare but left his portfolio to Clinton. But the current occupant of the White House has clearly put leadership issues with Putin off the table; issuing an Executive Order impossible to implement. Sanctions on a few Russian front firms and their executives are unlikely to bother Putin. Remarkedly, we have the industry treating all incidents as CEII, encouraged by regulators NERC and FERC. We have FERC giving PG&E what amounts to a free pass for 590 days of a near-total cyber asset breach and DOE suppressing incident reporting called for by their own rules,(OE-417 reports). And DHS maintaining strict anonymity rules on industry-US Cert forensic investigations. Of course, none of this is to deny Russia insights to their own adventures or access to sensitive information; it is pure pandering to special interests in the political system, the weak cybersecurity agendas of DoE and DHS. For the former, to avoid difficult questions on subsidies for the coal and nuclear industries, for the latter to avoid facing its continuing nightmare; the realization that DOD, not DHS, will somehow, have to instantly confront any disabling attack on the electric system.

7. Department of Energy

DOE has notable initiatives focused on modernization and R&D support and is the "sector specific" Department for the energy field. However, for years, its Office of Energy Reliability has shied away from serious cybersecurity oversight often supporting industry weaker positions. The situation has changed little in the new administration. Under its new Secretary, DoE tasked the Federal Energy Regulatory Commission to issue rules mandating continuing use of coal-fired and nuclear-fueled generation because of their ***criticality to national security,*** because their local fuel storage features made them essential during severe weather events. FERC disagreed with the direct task but did task the nation's ISOs and RTOs for comments on the requirements, economic issues, and cybersecurity "resiliency" factors.

DoE's impatience with this delay apparently triggered a National Security Council study to justify the national security and cybersecurity arguments. A 40-page legalistic "Addendum" to an internal policy paper leaked to the public,[18] with extensive justification for DoE's responsibilities in these matters, citing major concerns with cybersecurity risks to the nation's electric grid. Missing from this opus were any substantive discussions (as documented in this and earlier White Papers) of the far more critical vulnerabilities; also any discussion of Cyber defenses (and their limitations) and Russian incursions since 2012 (although Ukrainian events were mentioned). Of course, other risks and environmental impacts of these inefficient generation facilities (climate change, offsite power dependencies, nuclear fuel contamination a la Fukushima, etc.) were conveniently omitted.

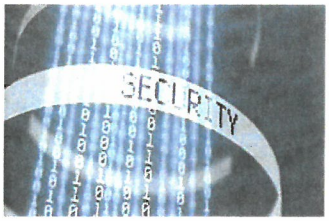
> ***Comment:*** There is considerable uncertainty over both energy supply needs for the future energy grid and on environmental policies, economic trends, scientific facts, and cybersecurity imperatives. It is certainly right for DoE to exercise responsible positions on all these issues. There are huge deficits in cybersecurity for the Grid; but fuel supply would go far down the priority list. It would be an extreme abuse of authority if cybersecurity were the number one argument for addressing the political issue of keeping uneconomical industries alive. If there were a particle of logic to this DoE initiative, its cyber adversaries would have demonstrated attacks to prevent it. Russia has not shown any interest in tampering with fueld supplies; it has far more attractive vulnerabilities in sight.

8. Laboratories, Centers of Excellence

There has been little informed comprehensive study by universities, national laboratories, and centers of excellence of the Grid, as a model for a critical national infrastructure, and of the vulnerabilities inherent in its organization, operations, and its technologies. There is even less informed examination of the threats to its survivability. Admittedly, we lack as a nation, any experience with actual domestic military threats, but here we are not talking about military-on-military, it is a case of military-on-civil infrastructure defense, a war we absolutely cannot afford to lose. What the nation is tolerating is idealistic and shallow treatises on "information sharing", and "resiliency". Many of these are funded by federal organizations in need of something, anything that appears to be learned and useful in their otherwise-weak agendas.

Further, many of the huge "dot.coms", Google, Apple, Facebook, et al, are at best apathetic (if not antagonistic) to the federal cybersecurity establishment, downplaying I/O threats to the social infrastructures they manage (and profit from), and denying the adversaries' potential for harm to national security interests. After all,

the lights are still on, power for their operations continues to flow, claims of "resiliency" permeate the literature (except in Puerto Rico of course).



"Resiliency" is, in fact, the most-often-used goal in the industry's agenda for reliability; most often applied to natural events (hurricanes, regional cold spells, winter storms). And the BES, has often proven resilient to such events, rapid recovery from severe weather. However, when "resiliency" is hyped, implying broader cyber survivability, a routine slight-of-hand practiced by senior officials or industry experts before congressional committees, or in learned publications, the public is poorly served. There is, in fact, little resiliency in the Grid to Russian cyber threats. Russia has strategically developed its cyberattacks to take down BES Transmission facilities as the surest path to disruption of power flows to urban centers.

Comment: Recent examples illustrate the continuing "resiliency" deception. A study titled ***"Terrorism and the Electric Power Delivery System",*** tasked to the National Academies and funded by DHS was completed in 2007 but the study report was immediately embargoed by DHS, ostensibly for security reasons. When finally made public in 2012 with some minor redactions, the report focused on the aging infrastructure, reliability and resilient issues for natural events, nil on cybersecurity, supposedly because the study group lacked experts in cybersecurity or terrorism threats. And indeed, no experts in cybersecurity or terrorism were listed as panel briefers. A theoretical think piece resulted with poorly connected factors. DHS's reasons for the five-year embargo have never been made public. Note, however, that Appendix E to their report titled "Summary of NERC Cyber Security Standards" stated to have been accessed in 2007 and revised in 2012- received no critical assessment.

In 2014, Congress authorized a study of Grid "resiliency and reliability". DoE tasked, and funded, a National Academies' study, conducted during 2016/2017. This study titled ***"Enhancing the RESILIENCE of the Nation's Electricity System***" was widely considered a follow-on to the 2012 Academies' study. It was seen in the wild circulating in draft. A review revealed that, again, the report contained little about Grid vulnerabilities and astoundingly, nothing on the Russian 2014 incursions, the latter directly linked to the 2015/2016 attacks on the Ukrainian Grid. All of this was extensively reported, with much policy and technical debate at national leadership levels, though played down by NERC and the industry. The complete absence of any of this material leads to only one possible conclusion, deliberate suppression of vulnerabilities and Russian threats, a consistent practice by the industry. Previous White Papers along with numerous citations were provided to the Academies but to no avail.

As the report was not yet published, the Academies were urged to insert a simple statement that cyber vulnerabilities and threats would be covered in a future study., The Academies declined to modify the report asserting the study group had delivered what was asked for, while also stating that the study group lacked expertise in those areas. The study was subsequently referenced no less than seven times in the National Security Council's leaked **"Addendum"** for unjustified retention of uneconomical coal fired and nuclear generation sites which should prove embarrassing to the Academies for their strong position on CO2 reduction and Global Warming.

The electric industry is a major source of pollution globally. There is not much debate of the cause or the effect on the national resolve to move to green energy sources wherever possible. The nation will have to decide if coal mining jobs are worth the health and environmental costs. What is more than sad is "setting up" the National Academies to produce a "learned" study that can easily be used to justify a purely political decision. [19]

9. The Administrations

Throughout the previous administration, Obama's "internationalist" instincts circumscribed national cybersecurity policy, but with a focus on societal concerns. A succession of EOs did little for protection of national interests. For national security, Obama clearly worried about a cyberwarfare arms race. He was successful in getting China to roll back PLA espionage efforts against US Defense Industry, though not China's Ministry of State Security more-stealthy (Axion) efforts. But Obama failed the acid test of responsibility in his tepid response to Russia's aggression in the 2016 Presidential campaign while simply ignoring Russia's incursions into the National Grid. The carryover into the current administration reflects continuing "Grid-lock" as discussed throughout this White Paper.

10. Conclusion to Existential Threats

Given the importance of electric power to national security, there is no rationale for the consistent downplaying and actual suppression of evidence of Russian targeting of the North American Grid, the misbegotten motivations of many so-called stake holders in the Security of the North American Grid. The leadership of those constituencies simply fail to accept huge risks to the nation, risks that will link to Russian actions in an international crisis. It becomes virtually impossible to explain how national leadership in this industry, its regulators, DHS and DoE, the national security community, the Congress, two Administrations can put its special interests ahead of the security of our critical electric infrastructure. Hence, this ***"Existential Threat".***

The danger is in miscalculation, wherein Russian leadership decides to use its cyber capabilities to leverage its position in some dispute. Putin undoubtedly has the confidence in the Federation's ability to bring off an actual attack, confident that it will force this nation to accept Russia's will. Plausible denial, or "false flag" deception may well create hesitation in a US response. Russia does not need many more successes (Crimea, Syria, the 2016 election) to reach this point. What's clear as a bell is the extreme difficulty of a national security response with NSA and Cyber Command challenged with active defense of the Grid from a "cold start". And a Grid crisis is no time for internal debates on cyber policy, particularly with so many National Security installations and activities dependent on commercial power. The nation is overdue to adopt and articulate a deterrence strategy that Russia and other nations will respect.

VI. Russian Cyberattacks on the US Grid

1. Background

Russia's cyber activities have been continuous since at least the mid-90s. Cyber espionage was the focus for many years but has morphed into the broader cyber-based Information Operations strategy seen today. The evolution of Russian Cyber activities is contained in ***Appendix III*** to this White Paper. The two "actors" (to use the malware term in vogue) are the SVR (APT29/Cozy Bear) and MOD/GRU (APT28/Fancy Bear). The SVR is the comprehensive Foreign Intelligence Organization while the GRU is focused on of targeting for strategic i.e., National Security significance, including infrastructures critical to social and economic stability.

2. *Targeting the Grid*

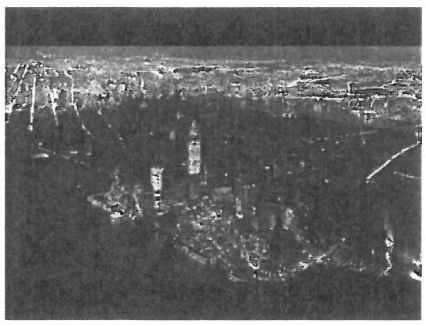
Industrial espionage involving the Grid undoubtedly goes back many years, however, the first clear indication of cyber targeting of the Grid was the exploitation of Control Center systems traced back to 2012. This marked the transition from pure espionage to the Grid becoming a target for a MOD/GRU cyberattack. A full-scale active reconnaissance commended in Spring 2014. It is likely that the period 2012-2014 involved stealthy operations by the SVR for ***"preparations of the battlespace".*** Note the SVR had earlier carried out a substantial "phishing" expedition against the Pentagon, the White House, and other US government facilities. Note also that DHS would not use the word "attack" in the dream world they occupied, it was not an attack unless physical damage occurred.

The 2014 attack was announced by US CERT, the DHS forensic staff.[20] The actors were not identified publicly.[21]Major vulnerabilities exploited were Control Systems modified at the vendors and a zero-day Microsoft vulnerability. (It was not until October 2014 that Microsoft fixed the vulnerability). Note that IT vendors' software, such as Microsoft, underpin vendors' control system products. Three Vendors subsequently confirmed that the modifications occurred in 2012.[22] ***Four years later, today, in 2018, the industry is asking for further delays, 18 months) in addressing Supply Chain vulnerabilities (e.g., access control and monitoring systems in CIP Standards).***

DHS requested the FBI investigate the attack as a suspected "insider" event, and details of that investigation were not made public. The FBI with DHS assistance, conducted non-public briefings for industry executives. Forensics on Russian malware were also embargoed, although general descriptions were promulgated by a few security firms, wanting to stay competitive with their European counterparts who are under no such constraints. Of course, the FBI will never publish details on a criminal investigation until after grand jury or prosecutor engagement. (It is likely that the same argument will surface to filings on the Incident Reporting NOPR under consideration at FERC.[23]) The public should not be deprived of cybersecurity revelations that are unclassified.

What we do know about the 2014 attack is that it was conducted by the GRU, APT 28 and that initial penetrations involved previously-bugged vendor control systems. What the GRU tested was a suite of malware involving "droppers" ***(HAVEX),*** software that evaded access control systems and implanted reconnaissance tools in "linked libraries". If ***HAVEX*** succeeded in its tasks, it communicated to GRU control systems ***(Black Energy 2),*** resident in C2 servers the GRU controlled. ***Black Energy 2*** SW had extensive features to permit takeover or modification of the targeted Grid systems. This reconnaissance operation went on for several months, until at least December 2014 in many cases. Security firms under utility contract, US Cert and industry executives know the details, the public does not. Why?

3. *Follow-on Targeting of Ukrainian Grid*



In December 2015, Russia remotely attacked Ukrainian Distribution systems, taking control of those systems and shutting down power to Kiev and about half of Ukrainian customers. In this attack, they used credentials for access obtained over the previous six months through phishing attacks. Nonetheless, both ***HAVEX*** and an upgraded version of ***Black Energy (BE3***) were found on the system. The attack was apparently conducted from Z+4 time zone, Moscow, St. Petersburg. A feature of the incident was a telephone denial of service (DOS) attack that confounded

at least one control center and customer call-in attempts. After about 6 hours, the GRU team withdrew, remotely, wiping files and residual evidence of their attack system. Note, this was a test, and a demonstration, no permanent damage to Ukrainian facilities occurred. A US team led by DHS and including FBI, DOE, US CERT, State Department personnel visited Kiev to obtain information from utility and government elements. The visit was not publicized until US Cert issued a post-visit report; one that downplayed any relationship to the US Grid 2014 incursions. A subsequent DHS "intelligence" report[24] attributed the Ukrainian attack to "criminal elements", making no reference to the 2014 events. A statement issued by NERC claimed zero impact on the US electric system, and a later NERC report made only an oblique reference to a Ukrainian initial assessment that linked the attack to Russia.

In December 2016 Russia attacked a Ukrainian Transmission facility, shutting off power for one hour. The attack was attributed to Russia by Ukraine. Most observers viewed the "demonstration" as a warning to Obama to avoid a cyber retaliation for the SVR/GRU 2016 Election events. And there was no "public" cyber retaliation by the outgoing Administration. It was only several months later that a Slovakian security firm, ESET, announced that, in fact, the Russians had tested a new malware attack in the Ukrainian Transmission utility, titled by ESET, ***Industroyer.*** (See ***Appendix Iii***). This is a malicious technology involving modification and augmentation of an international communications standard, ***(IEC61850)*** to penetrate and damage/destroy industrial control systems (ICS). Note: the destructive module was not activated in the Ukrainian test.

4. ***Russian Federation Cyber Incursions Continued into 2015 and Beyond.***

The federal suppression of incident reporting was intensified as well as almost all forensic analytic results. This obviously took coordination by DHS which included FBI and other federal analytic efforts. However, since similar cyberattacks were occurring in the Ukraine and elsewhere in Europe, insights to Federation capabilities were possible from security firms' reports including US firms doing business abroad. (The US government succeeded in shutting off reporting by Ukrainian industry and government sources but not capable security firms.) Technical details of threat developments are discussed in ***Appendix III*** to this White Paper.

Technically, what has been seen is steady improvement in both SVR and GRU capabilities, freely tested in the Ukraine and probably in the U.S. ***HAVEX*** and ***BlackEnergy*** upgrades by the GRU, and several new developments to address gaps in GRU toolsets. The continuing Federation efforts undoubtedly have economic, political and cadre training objectives as well as testing of new developments. Analytic linkages across incidents are the main way continuity on Federation organizations is maintained; however, attribution to specific organizations is carefully avoided except where the forensic results are indisputable. What is eminently clear is that the Federation is increasingly using GRU teams and capabilities against civil infrastructures, all of which testifies to steady improvements in both capabilities and GRU cyber warrior growth and the willingness of Federation leadership to use for GRU military-on-civil targeting.

SVR developments are always reported under the APT 29 ***Cozy Bear*** title since that tends to avoid the near-constant confusion over labeling such activities as SVR vs. FSB. ***Cozy Bear's*** activities are widespread, typically national strategic in goals, and prioritized accordingly; the higher the echelon, the more-stealthy and sophisticated the development or actual incident. No government wishes to credit the Federation with cyber successes but security firms' reporting shows it is clearly widespread.

5. Conclusion Russian Threats

Appendix III contains details of Russian Federation Cyber organizations and capabilities. There are many possible scenarios now available to Russia for interference in the US electric system; local, regional, national cyber incidents coupled to policy and economic initiatives Putin could attempt. They could be abroad, similar to Ukrainian Grid examples, they could be domestic coincidental with natural disasters, Harvey, Maria, Irma. They could be more adventuresome such as Syria, the Baltic states, an EU crisis, timed to coincide with a crisis involving another nation/state. Most would be elements of a broader Information Operations campaign, similar to the complex US 2016 Election example. In the absence of a US National Deterrence Policy, there is little to prevent such occurrences.

VII. Other Threats

This White Paper will not address the threats to the Grid from other potential adversaries., China, North Korea, Iran and Terrorist Organizations. China's capabilities against the Grid are largely unknown but reconnaissance for intelligence collection or cyber warfare is evident. But note that there is increasing evidence of Russian ***"false flag"*** operations, pretending to be another US adversary. When conducted by the GRU, such operations are almost always immediately compromised, usually through malware linkages to known GRU operations. Practice does make perfect, the GRU will improve, so accurate attribution must be maintained. The Federation will not hesitate to use both the SVR and GRU in single campaigns when the political challenges and manpower needs are much greater, as seen two years ago in the various US Election operations.

VIII. Conclusion

1. Existential and Russian Threats Converge

Cyber warfare is all about vulnerabilities and threats, but it has not been possible to hold to account, American institutions that contribute to the ***Existential Threat*** described in this white paper. Consequently, critical infrastructures including the National Security community, nearly totally dependent on electric power, teeter on the edge of a crisis that lies almost totally in Russian Federation control. And Russian Information Operations are shaping up to the high-risk level where temptation might tip that nation into action, to seize control or damage the electric system, with ***"false flagging"*** or denial within reach.

2. Rising Costs and Politics Converge

While this state of confusion persists, the costs to the industry for questionable protection keep rising, and absence of real defenses and industry hype will not change. Add to this uncontrollable situation the administration's efforts to shore up two energy industries, coal and nuclear on quite different national security grounds, absurd efforts given other more critical vulnerabilities being ignored. Those costs will add onto the unnecessary expenses now being borne, simply because the nation lacks a firm national deterrence policy.

3.The Better Road Ahead

The most immediate, demanding, and frankly critical step for national leadership is implementation of the DSB study's recommendation, a declared deterrence policy founded on the principle of measured retaliation. We know now what U.S. infrastructures are critical and must be put out-of-bounds. No nation/state, certainly Russia or China, will risk U.S. Cyberattacks on their far more vulnerable infrastructures, attacks that should be measurably more serious than those they initiated. Iran has already been taught that lesson. Other pariah states will not be a serious challenge to US offensive forces. To ensure deterrence, a nation-wide early warning and situational awareness system must be established, to support other dependent civil infrastructures. National Guard and Military Reserve elements should be trained as cyber first responders. The DARPA RADICS effort should be reoriented to provide "edge" (i.e., domain) protection for all Critical Infrastructures. And the end-to-end federal and infrastructure defense should have the smartest AI and Machine Learning tools applied. Legislation may be required to ensure utilities status is available. Real time linkages to intelligence capabilities will help make the warning and response system, all-source. In truth, it is ***"pay now or pay later"*** time for federal action.

To those who fear uncontrollable cyber war, do they settle for "Putin wins"? Think carefully about other deterrence efforts that have worked. Cyber weaponry will continue to be developed but held in reserve for actual kinetic warfare. Terrorist and hactivist capabilities must simply be pre-empted as the nation would do for any other major initiative they might mount. The advantage of such policies is that the energy industries can focus on modernization including environmental controls, and only such cybersecurity protections as are essential for warning and "active measures", i.e., counterattack by first responders.

In truth, this nation has no alternative, none. Fixing cybersecurity in the Grid would take monumental, virtually impossible, business and regulatory changes. Russia is getting too far ahead in cyber capabilities. Putin is adventuresome, missed the cold war games, but plenty of opportunities remain, he loves brinksmanship and needs it domestically. In another age, an evolutionary age, it may be possible to mount effective protections for critical infrastructures but at present all the nation can do is pray that no competent nation/state adversary will do serious damage in a Grid cyber adventure.

There can be interminable arguments on which is more damaging to America, disruption of the US election machine or shutting down power to the its national security Community and other critical entities.. The nation should not have to make that choice but unfortunately, the American public does not know its options.

Endnotes

[1] FERC Order - Grid Reliability and Resilience Pricing - Docket Nos. RM18-1-000, Jan 8, 2018
[2] NOPR- Supply Chain Risk Management Reliability Standards, Docket No. RM17-13-000, Jan18, 2018
[3] See p31, NERC Petition, Docket 13__, Approval of CIP v5 Standards, Jan 31,2013
[4] NERC "The Application of Risk-based Compliance Monitoring and Enforcement Program Concepts to CIP Version 5", October 22, 2014
[5] Ibid
[6] See Endnote 1.
[7] ICS CERT Monitor, May-August 2014
[8] Shodan is an open source scanning tool; widely used to find ICS devices directly addressable from the Internet.
[9] ESET "Industroyer: ICS protocols were developed decades ago with no security in mind", 19 Jun 2017 - 11:00AM
[10] National Grid Advances Digital Substations, T & D World, May 1, 2018
[11] The Eastern Interconnection Data Systems Network (EIDSN) connecting Reliability Regions in the Eastern Interconnect handles data flows from both SCADA and PMU systems.
[12] "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks" Authors:Julia Summers, Michael Walstrom, International Policy Institute, October 11, 2017. This is a comprehensive summary of Ukraine attacks, well-researched.
[13] FERC - North American Electric Reliability Corporation Docket No. RR15-2-005, ORDER ON COMPLIANCE FILING, Issued November 16, 2017
[14].U.S. GEOLOGICAL SURVEY PROFESSIONAL PAPER 1552-A The Lorna Prieta, California, Earthquake of October 17, 1989-Lifelines. See also Paul Stockton's paper on SUPERSTORM SANDY: IMPLICATIONS FOR DESIGNING A POST-CYBER ATTACK POWER RESTORATION SYSTEM, Paul Stockton, Johns Hopkins University. A Contrast of Reality vs. Speculation.
[15] 2017 NCCIC Year in Review Operation Cyber Guardian. Only malware discussion was WannaCry (non-Russian).
NCCIC AR-17-20045 February 10, 2017 Enhanced Analysis of GRIZZLY STEPPE Activity
[17]Treasury Sanctions Russian Federal Security Service Enablers, Treasury Department News Release June 11, 2018
[18]Addendum", labelled DRAFT-5/29/18, Prieleged & Confidential, Attorney-Client Privilege, NOT FOR FURTHER DISTRIBUTION. A 40 Page NSC document, detailed legalistic justification for impending DoE action on a moratorium on further closures of Coal firing and Nuclear electric generation sites
[19] The author of this White Paper is a member of the National Academy of Engineering and strongly felt the obligation to point out to the Academies, a clear case of abuse. The extensive citation of the study in the NSC initiative has but one purpose, to help justify an initiative to retain inefficient coal and nuclear generation facilities. The Academies risk compromising their science-based positions on Global Warming and Health.
[20]ICS-ALERT-14-281-01 Ongoing Sophisticated Malware Campaign Compromising ICS, October 28, 2014
[21] Adm. Rogers after a closed hearing In DEC 2014 stated publicly that China and "perhaps others" were involved in hacking the US. He was obviously constrained from mentioning Russia although it was well-established by Dec 2014 ICS-ALERT-14-281-01 Ongoing Sophisticated Malware Campaign Compromising ICS, October 28, 2014
[22]ICS CERT Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
[23]Docket No. RM16-15-000, Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information (Issued June 16, 2016)
[24] DHS INTELLIGENCE ASSESSMENT "Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector" 27 January 2016

Appendix I - The Electric Industry, Reliability and Resiliency

There is much about the Electric Industry of concern, the unusual disaggregated operational structure described earlier, aging facilities, green energy modernization, recurring policy debates on energy supply, and a relatively flat revenue picture for the last decade. The industry must contend with mixed economic and policy pressures while utilities rapidly convert from coal-to-oil-to-natural gas for economic reasons. Meanwhile the Secretary of Energy pressured FERC to selectively modify tariffs to ensure retention of nuclear and coal-fired generation facilities, ostensibly for assured fuel supply reasons.[1] The muddled future of Nuclear Generation has site construction cancelled in several cases while owners petition states for "Green Energy" subsidies or federal underwriting of construction risks. States are subsidizing Solar, Wind and other non-polluting electric generation systems while the President leverages federal regulations to keep coal mines in business. Natural disasters, undoubtedly heightened by Global Warming, are causing havoc in coastal areas with recent extended outages in Texas, South Florida, and Puerto Rico impacting millions with serious questions being raised about Grid reliability, and resiliency.

Modernization

It has been over ten years since a DoE program launched with 2008 economic recovery funds initiated a shared 50/50 initiative to implement Synchrophasor (PMU) technologies in Transmission and Distribution systems, largely at the sub=station level. These systems sample power streams for significant consistencies in phase, frequency, amplitude and current. in reacting to anomalies with a wide area perspective, data can be correlated from multiple PMUs for situational awareness. The technologies when used correctly by utilities, provide excellent status data permitting much more precise management of assets than SCADA (Supervisory Control and Data Access) but also pointers to anomalous system behavior, often in neighboring facilities. Synchrophasors are already proving their worth in detecting and helping to resolve maintenance issues with transformers, generators and other Grid instrumentation. Their value during "islanding" was established nearly a decade ago, in a White House study of Grid Resiliency:

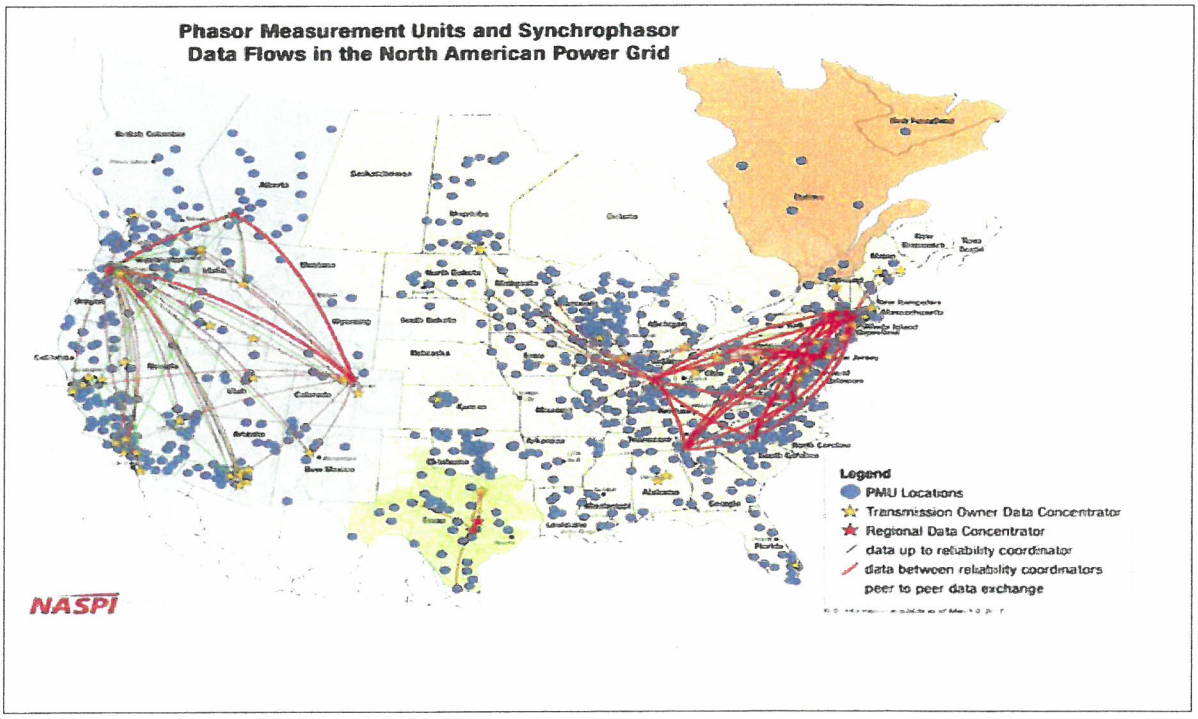
"During Hurricane Gustav in 2008, Entergy, an energy company responsible for delivering power to customers in Arkansas, Louisiana, Mississippi and Texas, had 14 transmission (substations) trip out-of-service in the Baton Rouge to New Orleans area which created a Baton Rouge-New Orleans electrical island for 33 hours, meaning interconnection to the grid was lost. During this period, Entergy was able to control the island's frequency, balance three large generating units, and maintain electric service to customers because of the 21 PMUs the company had installed across a four-state area. PMUs identified and warned of islanding conditions during emergencies and provided Entergy with insight into how to manage islands and where else in the territory additional PMUs were needed. Entergy's success with PMUs during Gustav demonstrated that these devices had moved from being optional equipment to vital components of a modern electric grid (Galvan et al. 2008)."

---

[1] Secretary of Energy Letter to FERC Chairman and Commissioners, September 28, 2017 Subject: Enclosed NOPR to address Tariffs for Energy Supply subsidies for Coal Generation and Nuclear Generation facilities. The proposed rule was rejected unanimously by FERC. This led to draft DOE memo defying FERC decision, supported by NSC 40 page justification, and Trump statement supporting DOE, 1 June 2018. A DoE implementation order has not yet surfaced.

Strangely, overseers (NERC, FERC) have been largely inactive on this technology. However, a Grid-wide issue has come to light with the advent of these systems; they have revealed the existence of "forced oscillations" that can propagate across large segments of the Grid, are a hazard to safety instrumentation, and could provoke cascading outages.[2] And the oscillations can have higher amplitude than the original frequency excursions that created them. Under its Reliability mantra, DoE recently issued a draft guidance document[3] that describes the phenomena and suggests mitigation procedures.

Comment: PMU's and associated data sets in Processing Data Centers (PDCs) offer an excellent opportunity for supporting regional or Grid-wide cybersecurity situational awareness. However, the industry, NERC and FERC have kept their distance from Synchrophasors; they complicate the separation of Transmission (BES) and Distribution sectors and call attention to their exclusion from CIP Standards. Their advancement has been left to individual utilities, regional ISOs (and a few Reliability Coordinators) that have seen their value; i.e., investment in Synchrophasors pays real dividends in asset management. On exploiting their potential for wide area surveillance, leadership has totally avoided such a commitment. The Reliability Coordination structure would easily accommodate such a program, at little additional cost of manpower since it would significantly add to Reliability capabilities. Thousands of Synchrophasor systems are now deployed (see map that follows) The industry-wide interest group (North American Synchrophasor Program Initiative, NASPI) has been active for the past decade in further[ng the technology (initially with DoE funding), loosely coordinating data standards, application development and "sharing", and recently, began to address cybersecurity potentials. NERC and FERC have both been absent in national-level coordination efforts, undoubtedly because the technology transcends Distribution and BES domains. This serves as another example of industry and



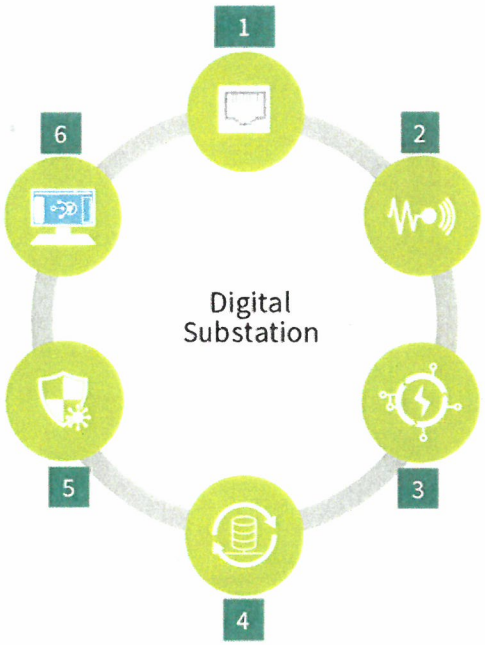
[2] Roadmap for Addressing Power Oscillation Risks in Power Systems:, BPA August 2015

[3]Recommended Guidelines for NERC CIP Compliance for Synchrophasor Systems, DoE, Nov 2017

There are literally hundreds of modernization efforts underway in the electric system; most do not depend directly on regulatory approval to meet reliability or cybersecurity standards. However, utilities must be sensitive to these overarching regulations if only to ensure that modernization initiatives do not adversely affect reliability or security.

An excellent example is the caution that a northeastern Transmission Operator, National Grid that "digitized" a transmission substation using the international standard communications interface, IEC 61850 in the all-encompassing facility bus.[4] ***"The decision was made to digitalize the entire IEC 61850 substation using the process bus, which includes all the equipment at a substation, such as instrument transformers and circuit breakers. Utilities must invest in and create the grid that will enable the decarbonized, distributed energy future — safely, reliably and affordably. IEC 61850 is acknowledged as the global communications standard that enables increased control, monitoring and automation within electrical power systems." —National Grid, a northeastern TO***. This raises the fundamental question of how the DOE, the regulators and operators should institutionalize the work that has gone into this.

Core Aspects of a Digital Substation



1. **Ethernet-based communication on IEC 61850**
   Digitalization of station level
2. **Digitalization of process level**
   Introduction of process bus and NCITs
3. **Asset management support**
   Use of data from the digital substation for asset management
4. **Intrgrated engineering**
   Consistent, effiecient engineering
5. **Cybersecurity**
   Prerequisite and integral part or any digital substation
6. **Power system control support**
   Use of data from the digital substation supports control of electrical power grid

Cybersecurity is a prominent requirement of National Grid's IEC 61850 digitization architecture, as shown above. And it will be an integration security challenge since Russia has IEC 61850 in its crosshairs as seen in the 2016 Ukraine cyber attack where they tested a customizable IEC 61850 attack, titled by its discover, ***INDUSTROYER.***[5] So "institutionalizing" National Grid's investment in total substation cybersecurity would

---

[4] See ***Appendix III*** for cyber targeting of this international communications standard.

[5] Industroyer: ICS protocols were developed decades ago with no security in mind, ESET By Editor posted 19 Jun 2017

obviously have tremendous advantages in securing the electric transmission and distribution substation deployments, even though there will be many different configurations to address.

Resiliency

Almost all discussions of grid resiliencyl note that reliability and resiliency (the ability to recover from an outage) are different challenges. But there are also significant differences and therefore challenges between resiliency related to outages from natural events, and resiliency to a cyber attack on the grid. Most cyber "incidents" observed in the wild demonstrate sufficient potential for destruction or design for continuing control by the attacker.[6] This has been aptly demonstrated in the Ukrainian events, and probably the US Grid. And there are few, if any, CIP standards requirements that address the technical difficulty of combatting attackers. Cyber offense is still far ahead of cyber defense, the gap is widening, and DoD and IC organizations capable of "active defense" are sidelined. Note that the design objective of the DARPA RADICS program, a $100M effort, is recovery and reconstitution of the electric network, following an actual attack but still to be demonstrated.

Unfortunately, the articulation of cyber "resiliency" as a major feature of Grid security occurs repeatedly among the hopefuls embodied in what is described as the **"Existential Threat"** in the body of this White Paper. Can the National Grid architecture produce an ***IEC 61850*** security architecture that provides a good measure of cyber "resiliency"? Not without a thorough understanding of the end-to-end vulnerabilities of the connected electric system, a deep understanding of the emerging Russian ***IEC 61850*** threat, a willingness to take vendors to the mat on security improvements in their products and services, and address steady FERC resistance to the NERC/industry broadside opposition to CIP Supply Chain Standards.[7]

Obviously, much can and should be done to improve the overall cybersecurity resiliency of the national electric system. If made an engineering imperative, most modernization efforts would contribute a measure of improvement. And resiliency must improve to support a national objective and actual mechanisms for defense of critical infrastructure. The structural impediments, the substantial distractions suffered by the industry, and a coherent national policy on deterrence must be dealt with, to achieve such a goal.

Resilience is truly a desirable attribute and a goal that should remain high in the sizeable list of complexities the electric industry must confront. It is often described as the ***"Holy Grail"*** but it is at best, only a ***"Holy Goal".*** Most in the industry and the government would not claim defensive superiority or even parity with the nation's cyber adversaries in this critical infrastructure domain but the difficulty is the implication, nay the industry strategy, to argue that cybersecurity "resiliency" is readily achievable if just a few impediments were relieved; eg., better "Information sharing" with improved flow of classified intelligence to utilities, and of course, reduced regulatory controls. Resiliency strategy may apply to Grid reliability standards in some cases but does not stand up to inspection for cybersecurity standards.

One of the few bright spots for cybersecurity resiliency is a microSynchrophasor development project now funded by DoE involving UC Berkeley, Pacific Systems Ltd. (PSL) and other collaborators to incorporate CyberSecurity functions with safety and operational power sensor technologies at the Distribution Level, using machine learning algorithms to detect, at about twice the sampling rate of conventional PMUs, cyberphysical

---

[6] IBID

[7] See for example: Supply Chain Risk Management, Docket No. RM17-13-000 Reliability Standards, COMMENTS OF THE ISO/RTO COUNCIL

attacks. [8] The project system, a 3-year program, is installed in a subset of local Distribution substations linked into Berkeley's Power Standards Lab. The program is structured to transition to operations; this would involve cooperation of the Bay area segment of the PG&E system. It is, in fact, a great example of a grass roots effort to bring academic, industry and vendor interests together on an integrated substation-level sensor effort, with cybersecurity "built in". However, this is an effort that could have been initiated ten years ago. The question to ponder is will it be languishing ten years from now?

The Distribution asset community should also be doing careful planning for "islanding" during a cyberattack. What critical user communities occupy a survivable segment of generation, transmission and distribution resources? How large or how small can they be created? How should they be protected; i.e., automatically? With skilled cyberwarriors? Are linkages possible between "islands"? Are there wide-area, defensible "islands" hidden in the Grid or can such be created?

Conclusion

There is no question that many industry factors work to the disadvantage of security in the nation's electric system. Chief among these is industry fragmentation, over 3000 independent and semi-independent utilities is an impossible base for institutionalizing nationwide security. It begins with the absurdity of separation of 50 States abandoned to their cyber fate by Congressional Law. And as the States go, so will all urban areas, cities, users. Further, the determination of the industry, with a compliant Congress and regulatory commission, to confine its CIP standards to individual Electronic Security Perimeters (ESPs, to oppose Reliability Regions exercising cybersecurity enforcement, despite their role in Reliability Standards), speaks volumes on the risks being taken by the United States. And for the past several years the exclusion of communications networks and Internet dependencies from CIP has bedeviled regulators and NERC standards teams on how to paper over connection and supply chain vulnerabilities being exploited by Russia.

So after nearly five years of uncontested Russian penetrations of the North American Grid, we are asked to believe, to accept, a cybersecurity system based on the survivability of the Bulk Electric Transmission System providing power to the mass of unprotected nationwide Distribution systems, with less than 10% of the BES Transmission substations covered by CIP Standards, weak as they are. This is absurd on the face of it. It is no wonder that the Defense Science Board, in a two-year study, concluded that the industry was totally incapable of protecting itself and our national security interests, and recommended a hard policy position of deterrence.

Almost as sad is the certainty that fragmentation is now significantly a barrier to modernization; one only must examine the anarchy in adoption of PMU technologies for technical management of power transmission. No standardization, no efficient development of applications and processing systems, no effective use beyond the substation of correlated data, no extension into wide area surveillance and security, no wide-area use of PMUs for attack response. And this industry will be late to the party that is exploding in newer technologies, massively emerging in IT, Networking, Internet and Processing fields[9]. The Internet of Things (IoT), devices that must be spoken to by their OEMs, that must speak to their OEMs, include many that will blanket the electric system, from smart meters to critical sensors at the substation level. Vulnerability seams will blossom.

---

[8] "Combination of Old and New Yields Novel Power Grid Cybersecurity Tool", March 7, 2018, kkincade@lbl.gov

[9] See Intel white paper titled: "Embedded Computing on the Edge", Intel FPGA, June 6 2018

No other industry has a more uncertain future, technologically, and the limits on CIP have clearly been reached if a major CEO, Tom Fanning of Southern Co. warns of retaliation, in comments at a conference at the Aspen Institute on June 26, 2018. He characterized today's affairs as ***"the most underreported war in our history",*** suggesting that DoD should hold hackers accountable for crossing red lines. He pointed to a series of attempted cyber incursions at nuclear power plants and other critical infrastructure sites last year, dubbed ***Nuclear 17***, a focus on some of America's most sensitive facilities, warning that if they hit the US Power Grid,***"I can tell you the capability exists today, if somebody tries to take us down, they will have a bad day."***[10]

This should clearly be the current national policy, but it has not been declared. Further, there needs to be some structured Grid-wide Situational Awareness, warning and alerting system, an attack detection capability linked to the intelligence community, and the US Cyber Command.

[10] "Grid Hackers can expect retaliation, CEO warns" E&E News, June 27, 2018

Appendix II - Critical Infrastructure Protection (CIP) Standards

Limitations

In addition to structural weaknesses,[1] CIP Standards contain exclusions and specific metrics that further limit their coverage:

1. CIP Standards apply only to individual BES utilities and selected other "Registered Entities", e.g., "balancing authorities". Some supernumerary functionaries have "reliability authorities" but do not bring cyber assets exclusive to the function.

2. Cyber assets covered by CIP must satisfy a 15 minute "BES" impact rule to be categorized as BES Cyber Assets.

3. Metrics and other rules exclude an extensive set of generation and transmission facilities. The degree of coverage is a critical CIP issue; yet other than a slip-up during CIP v4 negotiations, NERC and FERC carefully hide these numbers from the public.[2]

4. Categorization of Cyber Assets excludes all communications systems and networks, one of four major exclusions from CIP 002-5. Internet connectivity is a major Grid vulnerability; it is also a significant factor in Supply Chain vulnerabilities.

5. With end-to-end modernization, operational technologies (OT) and information technologies (IT) in both Transmission and Distribution Systems are exploding, most with neither security protection nor overriding CIP Standards to ensure protection.

6. CIP Standards prevent utilities from holding their vendors responsible for penetration of the vendors' product Supply Chain, the major attack vector for sophisticated cyber adversaries.

7. CIP Standards do not specifically address "data flows", "data formats", "communications protocols", "encryption", "data aggregations", "analytic processes", "control algorithms" and a myriad of other generic application areas critical to protection of the BES. (NERC will always claim that interpretive decomposition of CIP Standards suffices, making obscurity the major challenge for compliance reviewers.)

8. CIP Standards do not, as yet, require utilities to remove ***known malware*** from their systems.

CIP Coverage.

In negotiations on CIP v4, FERC asked for information on assets coverage for Reliability Regions. Data sent

---

[1] For any in-depth examination of the limitations of CIP Standards, a good starting point is the NERC report on "Remote Access required by FERC Order No. 822: Remote Access Study Report, Docket No. RM15-14-___ " June 30, 2017. While NERC concludes that CIP Standards are effective in Risk Management, a good "RED TEAM" examination of this study would conclude just the opposite, flaws and huge omissions by boundary conditions put on the study would demonstrate the futility of extremely weak BES Standards protecting just the BES, let alone Distribution Utilities and Nuclear sites totally dependent on the BES for power.

[2] See table and comments in CIP Coverage. FERC has been challenged in several filings to task NERC for current statistics on assets within or outside CIP Standards but to no avail. Nonetheless, the display from CIP v4 development is believed to reflect current coverage in CIP v5/v6/v7.

publicly by NERC is summarized in the following table. CIP v4 was never implemented; however, nothing in follow-on CIP v5 developments would substantially change these facts; viz, substantial inconsistencies across utilities, extremely high percentage of assets exempt from coverage.

Transmission Substations Under CIP v4

Region	# Transmission Substations	# Transmission Substations ≥ 300 KV	Substations Under CIP-002-4-1.7	
			#	%
FRCC	537	16	6	37.5
MRO	1593	151	60	39.7
NPCC	809	119	39	32.8
RFC	3005	374	160	42.8
SERC	4467	283	110	38.9
SPP	1523	86	34	39.5
TRE	1182	100	50	50
WECC	3296	245	91	37.1
Totals	16412	1374	550	40.00%

We can see that only 1374 of a total of 16,412 BES Transmission Substations qualified for CIP Standards based on Kv power minimums (over 90% excluded) and of the qualifiers, only 550 (40%) were estimated by their utilities to be critical to BES Reliability. These judgments were validated by their Reliability Region, i.e., the Compliance Authority and by NERC. NERC will protest that this display does not reflect CIP v5 coverage, but rest assured, they will not voluntarily provide the current coverage statistics.

Critical Infrastructure Protection Standards

CIP	*Title*	*Definition*
002-5.1a	BES Cyber System Categorization	Low, Medium, High
003-5	Security Management Controls	Cybersecurity policies
004-5	Personnel and Training	Security awareness, risk assessment, access management
005-5	Electronic Security Perimeter(s)	Discrete Electronic Access Points
006-5	Physical Security BES Cyber Sys.	Physical security plan
007-5	Systems Security Management	Technical, operational and procedural steps
008-5	Incident Reporting, Response	Incident reporting -1 hour of recognition
009-5	Recovery Plans BES Cyber System	Response for stability, operability, reliability
010-1	Configuration Change Management	Monitoring, vulnerability assessment
011–1	Information Protection	Consolidation of information protection
014-1	Physical Protection	Security of Enterprise Security Perimeters

CIP Standards as they exist today are summarized in the above table. They are a subset of Reliability Standards, a much larger and more technical aggregation that were developed by the industry over the last 40 years and are kept current with the major changes in the field. [3] Further, CIP Standards invoke a number of metrics from Reliability Standards and are often linked to the latter in the referenced publication. NERC Standards Development Teams (SDTs) are responsible for development. A typical CIP Standard construct consists of a purpose, applicable "Responsible Entities", requirements that must be satisfied for CIP Cyber Systems to be covered, Violation Risk Factors, Violation Severity Levels (VSLs) to be evaluated for non-compliance, and frequently amplifying narrative. The key CIP Standard is CIP-002.5.1a since it governs categorization of BES Cyber Systems and therefore the applicability of all follow-on CIP Standards to systems so categorized.

CIP-002-5.1a

This "gateway" standard's purpose is to identify and categorize BES Cyber Systems and their associated BES Cyber Assets. Responsible functional entities include Balancing Authorities, certain Distribution Authorities based on BES linkages, Generation Operators, Generation Owners, Interchange Authorities, Reliability Coordinator, Transmission Operator, Transmission Owner. Also defined are Facilities (types) under these authorities and BES Cyber Systems, Cyber Assets covered by Cyber Systems and Control and Monitoring and methodology permitting the flexibility the Utility has in its groupings of Cyber Assets (individually or within a Cyber System).

Attachment 1 to this CIP provides the criteria for judging whether a Cyber System (and its associated Cyber Assets) is categorized as Low, Medium or High Impact. Highlighted assets covered by that criteria are Electronic Access Control and Monitoring Systems (EACMS), Physical Access Control Systems (PACs), and Protected Cyber Assets (PCAs). (***These Assets are the subject of a major disagreement between the Industry, NERC, and FERC over FERC's insistence that they be included in CIP modifications for Supply Chain vulnerabilities[4].)***

Requirement R1 details the assets to be reviewed by the "Responsible Entity" and identified as a medium or high impact asset IAW the criterial in Attachment 1. It further states: "***Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).***"

Requirement R2 calls for a critical review of the set identifications of R1, at least every 15 months and approval of a CIP Senior manager of such decisions.

Note: The following are exclusions from CIP Cyber System Categorization:

"4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

---

[3] NERC Reliability Standards for the Bulk Electric Systems of North America, Updated January 3, 2018

[4] Docket No. RM17-13-000 COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.[5]"

Violation Severity Levels (VSLs)

This standard includes VSLs for each of the Requirements, specified as Lower, Moderate, High or Severe. Each details the omissions or flaws revealed by the compliance audit. Penalties is any, are not shown; left to the judgment of the CEA presumably. Note that these CIP Standards all relate to the Impact on the BES and over time, FERC has agreed to local determination by the compliance auditor, overseen by Regional Entities and ultimately by NERC. The Reliability Assessment Initiative[6] has significantly altered the CIP Standards effectiveness in the process.

Compliance

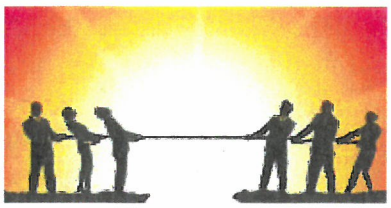
The Regional Entity serves as the Compliance Enforcement Authority (CEA) nominally the Regional Reliability authority or his agent. Compliance evidence is retained by the CEA a minimum of 3 years unless a longer period is specified by the CEA. The Compliance Monitoring and Assessment Processes can involve any or all of the following: Compliance Audit, Self-Certification, Spot Checking, Compliance Investigation, Self-Reporting or Complaint.

Other CIP Standards

The remaining CIP standards follow the same structure as outlined above for CIP 002-5.1a, over 300 pages in the latest Reliability Standards update.[7] With rare exceptions, the standards eschew technical content in favor of process-oriented guidance. The need for "plans" is dominant, plans take utilities to later decisions on details of the protective mechanisms that ultimately must be acquired, installed, maintained.

Grid-wide Security vs. Individual Utility's Endpoint Security

Introduction



Since total protection for the Grid depends on the sum of protection for all the facilities labeled "Electronic Secure Perimeter", it is fair to assess each such facility as an ***"end point".*** The security industry frequently characterizes their guidance in terms of either the enterprise, or the users ***"endpoint",*** the latter a physical or virtual location with boundary conditions that allow for specific protection advice. For "Grid"

---

[5] Section 4.2.1 identifies one or more facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

[6] The Reliability Assessment Initiative (RAI), a cornerstone of the Compliance process, keys the latter totally to BES Risk Management; permitting self-analysis, and non-public reporting, ostensibly to encourage utilities to open collaboration with CEAs. The RAI has made compliance non-threatening but FERC continues to question NERC efforts to make Compliance totally non-public.

[7] NERC Reliability Standards for the Bulk Electric Systems of North America, Updated January 3, 2018

security, we must understand that the Grid involves three major, semi-independent segments overseen by independent authorities, the Bulk Electric System (BES), the NRC nuclear generation facilities, and state-controlled distribution facilities. Neither FERC nor NERC (the Industry Reliability Organization) deny this fundamental segregation and can focus cybersecurity oversight only on the BES and its reliability in supporting the entire national electric system.

However, cybersecurity standards or processes do not apply to the Grid as a whole; instead apply to individual utilities engaged primarily in operation of the Bulk Electric System. Grid-wide situational awareness depends almost totally on the interaction of eight BES "Reliability" regions that monitor system operational technologies (OT) to keep the transmission backbone of the Grid functioning, including supporting power generation system. CIP v5/v6/v7 cybersecurity standards apply separately (and not interactively) to over 1400 "Responsible Entities",i.e., it's accumulated facilities. Each such physical facility is defined as an ***"electronic security perimeter*** or **ESP**, an "***Endpoint***". Thus Grid-wide operational cybersecurity rests on the premise that the sum of the Endpoint parts secures the overall BES and that a secured BES protects nuclear sites and massive distribution facilities.

Comment: Would any other major nation-wide enterprise, for example a national security organization, a financial conglomerate, a national healthcare provider, trust its enterprise-wide security totally to individual endpoints? Enterprise-wide security is the major reason why public cloud firms are creating national (and global) VPNs, ***coupling*** secured virtualized data centers, i.e., securing individual endpoints is simply insufficient to protect the entire, networked enterprise.

Discussion

As directed in Federal law, mainly the 2005 amendment to the Federal Power Act, and subsequent embodiment of Critical Infrastructure Protection standards developed by NERC and implemented by FERC, survivability of the entire national electric system therefore depends on the resiliency of the BES to attack, which in turn depends on the security of most of its core 1400 CIP-protected Endpoints. And those endpoints must survive without benefit of an enterprise-wide operational cybersecurity program; i.e., a 24/7 attack detection/warning/alerting system linking them together.

So the critical question for survival of the nation's electric system is "Does EndPoint Security for perimeterized utilities protect the BES and therefore assure reliable electrical supply to nuclear sites, and the mass of Distribution Systems serving fifty states and their urban centers?" Forrester, a major Research firm, rates assessments of the performance of 14 top-rated EndPoint Security Companies on three fundamental product/services capabilities - Prevention, Detection, and Remediation. How well are these functions embodied in CIP v5/v6 standards, becomes the major issue:

- **Prevention.** Do CIP standards require endpoint systems that prevent malware and exploits from executing; does the suite create an environment where malware cannot, for example, load into memory or stop an exploit from taking advantage of a running process? Do endpoint systems implemented under CIP standards reduce the attack surface through system hardening and applications control?

- **Detection**. Do CIP standards ensure that endpoint systems detect malicious activity, post-execution, (knowing attackers will inevitably bypass prevention controls)? For example, do endpoint suites monitor running memory, internal networks, and applications to prevent malware from achieving its goals? Do endpoint systems monitor both process behavior and user behavior to create a context for

complete analysis? Do CIP Standards require a SIEM (Security Incident and Event Monitoring) capability that links all facility security protections to feed comprehensive security management?

•**Remediation.** Do CIP standards result in endpoint security suites that identify and contain malicious endpoint activity or a potential vulnerability? Are endpoint suites capable of launching automated remediation (without significant admin involvement) such as: execution/file quarantining, configuration roll-back? Do they implement blocking actions for process and user behavior?

Assessment

The concept for CIP v5/v6/v7 Standards is one of "Risk/Management", with Cyber Assets grouped into Cyber Systems in estimating low, medium or high impact loss on the functioning of the Bulk Electric System as a whole. This concept must assume homogeneity of Cyber Assets with strong mutual exclusion features that eliminate major dependencies among Cyber Systems. Otherwise, significant uncontrollable linkages across low, medium and high impact Cyber Systems would make a nonsense of these categories and therefore "Risk Management".

However, CIP standards as promulgated, seldom specify, or even generalize, on modern interlocking endpoint technical controls such as outlined by Forrester above. CIP standards seldom extend beyond elementary cybersecurity hygienics; e.g., port blocking, password characteristics, personnel accesses, logs, etc., with a complete absence of Endpoint-wide SIEM. Further, there are major exceptions to CIP standards that result, almost always for a given utility, in fuzzy and porous security boundaries and vulnerabilities (for example, data flows) that violate the very concept of endpoint security, such as:

- Mass exclusion from CIP standards of most cyber assets in generation facilities and substations rated below a floor of 300 mw/kva; many with direct internet connectivity and with connectivity to medium and high cyber assets. Also excluded is any facility whose loss would not affect the BES within 15 minutes.

- Complete exclusion from categorization as Cyber assets of all communications and networks linking facility "security perimeters" as defined in CIP v5/v6/v7 standards. (Note that FERC has introduced a contradiction with an Order No. 822 task for development of a standard governing communications security of links between "Control Centers").

- Near complete absence of CIP standards for acquisition, remote maintenance and operation of modern cyber-vulnerable substation instrumentation systems; programmable logic controllers (PLCs) and other industrial control systems (ICS), synchrophasor control units and related data consolidation centers, and SCADA systems. And more importantly, the cyber infrastructures that link these operational technologies together and generate massive data sets for analysis in facility Energy Management Systems (EMS).

Conclusion

CIP Standards do not link even indirectly to vulnerabilities, and they fail to offset cyber threats that are being experienced. CIP Standards perpetuate a fallacy that "Electronic Secure Perimeters" for individual utilities collectively but imperfectly functioning as cybersecurity endpoints, secure the BES. This is eerily reminiscent of Hadrian's Wall during the Roman era in England. Hundreds of forts did not contain the Scots. Communications and networking and "Supply Chains" lacked defenses. It took the Romans 400 years to realize they were on an

island and the natives had no place to go. And 1400+ individual utility "ESPs" created from current CIP standards cannot obscure the major vulnerabilities in the North American Grid and their exploitation by Russia's cyber combat forces.

Appendix III - Russian Federation Cyber Organizations and Capabilities

Background

With the fall of the Berlin Wall, and major political changes in the former Soviet Union, there was a fairly rapid reorganization of intelligence services by Boris Yeltsin. The dominance of the KGB that evolved since Stalin's days changed and in the early 90's the KGB First Directorate was separated and designated the SVR-KR[1], an organization responsible for external intelligence services. The KGB proper was designated the FSB, responsible mainly for internal security affairs.

Much closer collaboration was called for between the SVR and the Ministry of Defense GRU (military intelligence). Interestingly, this period also saw the rapid growth of the Internet and its enormous effect on world political, economic, social and international security affairs. The SVR functioned as it had as the First Directorate of the KGB, including ***"active intelligence measures".***

In the Putin era, the Russian Federation emerged as the dominant actor in cyber-based Information Operations, linked to Putin's agenda involving militaristic and economic goals. With the Internet as a major highway, the SVR and GRU were challenged to adjust collection efforts and related "active measures" (i.e., cyber offensive capabilities) to match Putin's priorities, and then some. Stealth was a historic legacy but not to the detriment of mission success, since uncertainty of attribution and use of front companies has permitted the Federation and Putin, ***"plausible denial".*** The success of major Russian military adventures coupled to substantial GRU use of cyber warfare and information operations (Estonia, Georgia, Crimea, Eastern Ukraine, Syria, and more) frames the emerging story of "asymmetrical warfare", now well-developed for the Federation.

Introduction

US and European Cybersecurity firms striving to protect their clients, gather insights from cyber forensics on "incidents" studied by IT-competent analysts. Competition aside, it is a dangerous game since the major firms must be careful to avoid attribution, and not become targets themselves. And it becomes even trickier when firms are heavily engaged in international markets. At the same time, such firms must assure prospective clients that they are expert in defensive threat analysis, particularly with government and industrial organizations that have much to protect. Reporting by commercial firms permits some speculation in this paper on cyber activities -- targets, capabilities and complex information operations. Note that these are moving events, with much remaining hidden or not divulged. It is also very likely that specialization has occurred; teams that focus on certain targets. Where forensics (code extracts, malware examples) are reported, continuity is often possible, security firms will in fact, often identify the clues. A continuing complication, however, is the practice of most security analysts to assign different names to the hacking group when variations in forensics are encountered. US government organizations complicate the issue by using the security organization title in threat advisories (e.g., Dragonfly[2]) rather than the more generic title (e.g., APT 28).

---

[1] Wikipedia. Note that DHS and other Federal organizations continue to attribute Russian Global Cyber activities as FSB efforts, not SVR and GRU.

[2] Symantec uses the term Dragonfly for Apt28, GRU, ***FancyBear.***

SVR-KR

The mission of the SVR-KR[3] was stated by the Russian Federation to be:

1. Conduct intelligence;
2. Implement active measures to ensure Russia's security;
3. Conduct military, strategic, economic, scientific and technological espionage;
4. Protect employees of Russian institutions overseas and their families;
5. Provide personal security for Russian government officials and their families;
6. Conduct joint operations with foreign security services;
7. Conduct electronic surveillance in foreign countries

Major cyber offensive functions are highlighted. Based on these mission statements, incidents and campaigns can occasionally be linked to the SVR. Collectively, the open source community has labelled a linked set of activities and malware as APT 29 ***Cozy Bear.*** Occasionally, APT 29 events are mistakenly attributed to the FSB, probably because of cold war KGB ties. ***(But see the article on TURLA below.)***

The SVR maintains a low, often hidden profile in Russian initiatives abroad, using surrogates, front companies, and even the MOD/GRU APT 28 ***Fancy Bear*** as cover. For example, in the 2016 US election, the SVR APT 29 preceded APT 28, the GRU, in penetration of the DNC and may have kept involvement from the GRU since both teams were found to be active simultaneously.[4] The SVR APT 29 was identified conducting aggressive Phishing efforts.

COZY BEAR (CozyDuke or APT 29) is the SVR adversary group that in 2015, according to Crowdstrike, ***"successfully infiltrated the unclassified networks of the White House, State Department, and US Joint Chiefs of Staff. In addition to the US government, they have targeted organizations across the Defense, Energy, Extractive, Financial, Insurance, Legal, Manufacturing Media, Think Tanks, Pharmaceutical, Research and Technology industries, along with Universities. Victims have also been observed in Western Europe, Brazil, China, Japan, Mexico, New Zealand, South Korea, Turkey and Central Asian countries."***

For one of its many Trojan-based operations, Symantec reports ***"Seaduke has been used in attacks against a number of major, government-level targets. The malware hides behind numerous layers of encryption and obfuscation and is capable of quietly stealing and exfiltrating sensitive information such as email from the victim's computer. Seaduke has a highly configurable framework and Symantec has already found hundreds of different configurations on compromised networks. Its creators are likely to have spent a considerable amount of time and resources in preparing these attacks and the malware has been deployed against a number of high-level government targets."*** Chasing the SVR across the internet, through the dedicated networks of government, civil and industrial organizations is a major undertaking for any security organization and we are indeed fortunate that the SVR cannot escape detection totally, despite its low profile and competency.

---

[3] Wikipedia.

[4] CrowdStrike, "Bears in the Midst: Intrusion into the Democratic National Committee", June 15, 2016

The SVR is extremely well-equipped for its mission, it clearly has the versatility and maturity to use a myriad of techniques to penetrate its victims and exfiltrate intelligence, it is obviously a cautious and patient adversary, but persistent. Cooperation with Military Intelligence was written into the 1996 law; since ***"active measures"*** frequently involve both political and military actions. Even superficial study of Russian adventures in Georgia, the Crimea, Syria, etc. imply collaboration; with SVR efforts well-hidden, and GRU efforts more open. Another factor is, of course, requirements for GRU manpower, training and tool modifications that might be needed quickly based on escalation decisions at the Russian leadership level. The Federation very likely assesses its 2016 SVR/GRU information operations campaign across the US election fabric as a considerable success, happy with its effect on the US political impasse, polarization of its citizenry, stagnation-cum-weak retaliation, and importantly, lessons learned. One of its most important by-products was the relative freedom provided Federation cyber forces in penetration and reconnaissance of the North American Grid, preceding and concurrent with the 2016 election affairs.

SVR Cyber Capabilities

Crowdstrike, the firm that was chartered to assess the attack on the DNC servers, describes the SVR (APT 29) capability as follows: ***"COZY BEAR's preferred intrusion method is a broadly targeted spearphish campaign that typically includes web links to a malicious dropper. Once executed on the machine, the code will deliver one of a number of sophisticated Remote Access Tools (RATs), including AdobeARM, ATI-Agent, and MiniDionis. On many occasions, both the dropper and the payload will contain a range of techniques to ensure the sample is not being analyzed on a virtual machine, using a debugger, or located within a sandbox. They have extensive checks for the various security software that is installed on the system and their specific configurations. When specific versions are discovered that may cause issues for the RAT, it promptly exits."***

There are many twists and turns to the SVP's repertoire. It will try to avoid detection by using layers of obfuscation, by aping legitimate users, visiting sites such as Twitter and GitHub to send commands to penetrated servers to extract data, it will change Twitter names frequently and automatically, sending precise commands timed to the victims schedule, use methods to obscure commands in images or encrypted text, and use cloud storage systems to hide exfiltrated information.

The SVR's flexibility and agility are incomparable, according to a number of security research groups that attempt to follow them in efforts to protect their clients. They have been seen using clever social engineering and voice mails to distract users while their computers are being infiltrated. They will use Adobe Reader 9-11 reader malware enticing victims to open malware-infected PDF's, the latter often with intriguing topics. The organization's versatility and scope comes with excellent techniques to avoid the victims defenses and mitigate those that would signal their presence. And the SVR slides easily from intelligence collection to information operations, as was seen hours after the 2016 presidential vote was known. That I/O campaign was focused on a continuing exploitation of election divides among the US electorate.

Of the many takeaways from SVR hacking efforts, the most prominent is that this group appears to understand its targets better than the targets understand themselves.

MOD/GRU

Fancy Bear, APT 28 is the label most often applied to the Russian Ministry of Defense, General Intelligence Directorate cyber operations. In the 20+ years since it was re-chartered for its modern missions, it has grown, developed an extensive suite of malware, sophisticated attacks, and collaborations (with the SVR). The GRU shows up in a huge set of Russian adventures, its cold war restraints that appeared to limit their geographical spread, have been completely thrown off. It appears to be the funding (and likely the logistic) source for several front companies, the Internet Research Agency (IRA) of social network fame during the 2016 US elections, and Wagner, a Russian mercenary combat group supporting Assad forces in Syria. The GRU is believed to have trained the Syrian Electronic Army in its successful information operations in the battle for Aleppo). And it has demonstrated a tactical cyber warfare capability in the Eastern Ukraine.

Fancy Bear APT 28 has been relatively easy to track as a major Information Warfare asset for the Russian Federation. Russian leadership has not hesitated to employ the GRU, ***Fancy Bear***, in a wide variety of non-military tasks, hacking Olympic data bases, hacking computers during the 2018 Winter Olympics, and of course the infamous hack of the Democratic National Committee computers and its senior users prior to the 2016 elections. The GRU also was also used in cyber attacks against State elections systems in at least 21 of the US States. There is a growing awareness that the GRU is prepared to risk detection (at least after the fact); counting on use of ***"plausible denial"*** by Russian leadership. It has become a major force in almost every major Russian aggression; in those cases where substantial cyber manpower is needed. And there should be no doubt that a major imperative for much of what we observe is the wartime, cyber combat role of the GRU, including its use to disable critical civil infrastructures.

GRU HAVEX/BlackEnergy Malware

Classic military intelligence cyber espionage was demonstrated in the penetration of US Defense Department systems[5] in 2008, using tools apparently adopted from earlier European Russian cyber operations, tools labeled **HAVEX** and **BlackEnergy**. **HAVEX** is a "dropper", malware that is inserted in a victim's system, usually through a vulnerability in Microsoft system SW. The dropper assesses the configuration, its network connections, takes possession of files and resources, and creates a back door used for secure communication of such system information to an external Russian-controlled C2 system. This channel can then be used by attackers to download ***BlackEnergy*** malware that could seize control of the victim's system, but more often is used for collection of files transferred to Russian control, and reconnaissance across controlling networks for vulnerable industrial control systems at operational sites. **HAVEX** and **BE** malware can be removed remotely if persistence is not required.

These techniques were apparently employed in 2012 after a strategic decision was made to target foreign electricity systems, including the US Grid. The GRU succeeded in penetrating major vendors supplying control systems to electric utilities, modifying such systems, apparently without detection.[6] In early 2014, the GRU successfully penetrated dispersed US electric utilities employing Control Systems, and their SCADA

---

[5] Hacking Trail Leads to Russia, Experts Say Malware Found at U.S. Firm Where Military Secrets Were Kept Wall Street Journal, Oct. 28, Pg. B1

[6] ICS CERT: <https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01>

software/firmware containing **HAVEX** and **BlackEneregy2** components. Access was via a Microsoft OS zero-day flaw; a vulnerability that was not patched until October 2014. While US CERT published an alert[7] advising the industry of the campaign, the scope of the Grid intrusions was bottled up in an FBI investigation, with the report briefed selectively to utilities but not made public. (DHS has never justified withholding these major incidents from the public.)

In December 2015, the GRU attacked the Ukrainian Grid at the Distribution level, after reportedly using phishing attacks on these utilities to collect network access credentials. Those penetrations allowed the GRU to remotely take control of electric power flows from substations, through Human Machine Interfaces (HMI). After a six-hour blackout for 225,000 customers, the GRU withdrew. **HAVEX** and **BlackEnergy3** was found in follow-on forensics.

It appears that a US investigative team, sent to the Ukraine, succeeded in convincing Ukraine government authorities to embargo any further information on the attack, but not before several foreign and domestic security firms revealed most details. Subsequent reports by US CERT and NERC's E-ISAC played down connections to the 2014 US GRU incursions. GRU Ukraine efforts were, however, forensically linked to the US intrusions/attacks.[8]

In December 2016, the GRU returned to Kiev, Capital of the Ukraine, to take down a Transmission utility, for a 1 hour demonstration (for Obama's benefit, apparently) but also to test a new, potentially destructive malware titled by its discover, ESET, ***"Industroyer"***[9] This new technique embodied malware modifications/additions to international electric standards, including ***IEC 61850*** that is used extensively as a communications interface standard to accommodate many different electric vendor products. (The destructive modules fitted to ***IEC 61850*** protocols were not used in the Kiev attack).

GRU persistence in the US Grid has continued since 2015, including nuclear site reconnaissance. These incidents cannot be totally suppressed under policies apparently in place at US departmental and White House levels. US security firms occasionally report generically on these events[10] and the FBI, DOJ and Treasury are public with law enforcement actions, including sanctions or indictments. Industry policy is to downplay incidents, public knowledge is not considered helpful in many other issues utilities must deal with. The FAST Act has apparently given the industry and its overseers license to suppress such incidents as ***"Critical Energy Infrastructure Information, (CEII)",*** which is somewhat helpful to a non-stealthy GRU.

GRU Petya/Not Petya Campaign

A new attack patterned after WannaCry, a hacking ransomware lookalike, has been developed and tested extensively by Russia's GRU. It has been firmly attributed to the GRU by the UK government[11] and it fills a void in the GRU cyber offensive tool kit; a DDOS method easily propagated through Bots available in the wild. Unlike Wannacry, it is not ransomware, but is a malicious denial-of-service, and potentially destructive hacking tool.

---

[7]Alert (ICS-ALERT-14-281-01E)

[8] DHS refuses to use the term "attack" unless physical damage occurs. This paper will follow convention; reconnaissance is a feature of attacks. Note that HAVEX and BlackEnergy are consistently linked by US and European security firms to APT 28, Fancy Bear, the GRU.

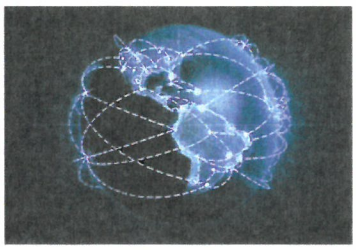
[9] ESET: WIN32/INDUSTROYER A new threat for industrial control systems, Anton Cherepanov, Version 2017-06-12

[10]See, for example, Symantec "Dragonfly: Western energy sector targeted by sophisticated attack group" 20 Oct 2017

[11]'The Guardian: Petya' ransomware attack: what is it and how can it be stopped? Oct 20, 2017

At present, ***Petya/NotPetya***[12] is a trojanized version of a Ukrainian accounting application, ***M.E. Doc***, involving a backdoor, permitting attackers to take control of any computer system and network running the malware-modified ***M.E. Doc*** application. A feature of the exploit permits infecting other systems on the same network. Selectively infiltrating just a few ***M.E.Doc*** upgrades permits testing without having to clean up after a major leakage of the malware. The GRU appears to have miscalculated on the widespread population of unpatched Windows 7 systems, leading to the June 2016 outbreak of ***Petya*** involving hundreds of thousand computers, world-wide, including Russia itself. Nevertheless, this apparent error led to the Treasury sanctions announced June 11, 2018.[13]

GRU Network Attack Development (VPNFilter)



Yet another void in the GRU cyberattack ensemble appears to be plugged, in the widespread network/router set of malware developments, named by CISCO, "**VPNFilter**".[14] CISCO and its affiliates estimate that over 500,000 network devices in at least 54 countries, world-wide, have been infected since 2016, with the major recent campaign involving the Ukraine.[15] The attack is capable of theft of website credentials and monitoring of ModBus SCADA protocols. The malware has a destructive capability that can be exercised individually or across an array of systems with the potential to cut off Internet access for hundreds of thousands of its victims, world-wide. The victim's network devices function on their IT "edge", therefore seldom have protection from such viruses, and are extremely difficult to defend. CISCO should know, they have scurried for years trying to provide defenses for their network products that often have uncertain Supply Chain origins or depend on vulnerable IT industry products, much like the electric utility vendors cited in **Appendix IV** to this White Paper.

CISCO states that ***"VPNFilter malware is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyberattack operations".*** As seen in the ***Talos*** display that follows, Stage 1 has multiple components to help it discover the IP address for the second stage server. ***Stage 1*** persists through a reboot, Stage 2 does not. However, ***Stage 2*** often has a destruct device that can render the system unusable. Additionally, ***"there are multiple stage 3 modules that serve as plugins for the Stage 2 malware. These plugins provide stage 2 with additional functionality"***. Seen so far are a packet sniffer for collecting traffic that passes through the device, including theft of website credentials and monitoring of **Modbus SCADA** protocols, and a communications module that allows stage 2 to communicate over **Tor. Tor** is an anonymity network often used by hackers.

VPNFilter has been backdated at least to 2016 by CISCO, the only other citation[16]available at present is of a ***VPNFilter*** code sample submitted to ***Virus Total*** from Taiwan in December 2017.

---

[12] The dual name seems to be the result of early confusion on whether ***Petya*** was ransomware.

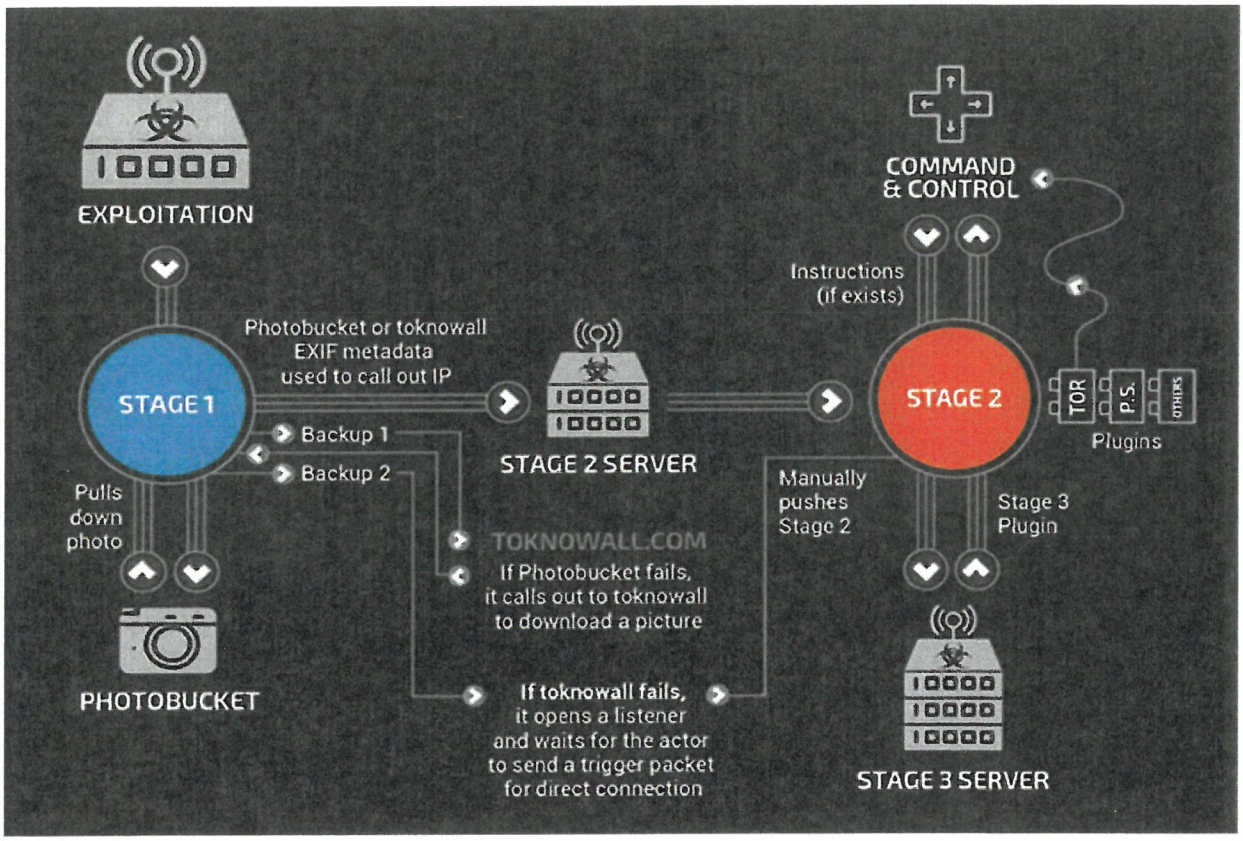
[13] Treasury Sanctions Russian Federal Security Service Enablers, Treasury Department News Release June 11, 2018

[14] ICS/CERT Alert (TA18-145A) Cyber Actors Target Home and Office Routers and Networked Devices Worldwide, Original release date: May 25, 2018 VPNFilter botnet: a SophosLabs analysis, part2
Corporate•SophosLabs•SophosLabs Uncut

[15] VPNFilter was also the subject of sanctions announced by Treasury on June 11, 2018.

[16] SophosLabs analysis, part2 Corporate•SophosLabs•SophosLabs 25 MaY 2018

Note that CISCO failed to attribute this malware campaign to Russia or its MOD/GRU, but reports malware linkages to ***BlackEnergy,*** seen in the GRU campaign in the US in 2014 and the subsequent long history of MOD/GRU testing such systems in the Ukraine. DHS/ICS CERT issued an Alert that briefly describes ***VPNFilter***, though without attribution to the Russian GRU. The FBI and DOJ had no hesitation, however, in citing ***APT 28, Fancy Bear*** and the many other names applied to the MOD/GRU actors. DoJ authorized the FBI to shut down the US internet site ***"toknowall",*** used by the GRU in this campaign. This is of only temporary value since the developers included in ***VPNFilter*** several workarounds to ensure persistence.



Source: CISCO TALOS

Other GRU APT 28 Excursions

Security Research firms regularly turn up GRU activities that appear to be focused on specific missions vice generic tool kit needs. Whether these are ordered up by Russian authorities or independent choices of the GRU is unknown. Examples include:

1. ***LoJack*** is an application that permits a company or an individual to locate a missing phone or laptop. Modifications to the device-locating application that points the agent to a C&C server instead of the owners control, a small modification of the application binary. However, this trojan has functionality that permits much broader control of the victim's infrastructure. It's not clear if that is the objective or if ***LoJack*** is a simpler surveillance tool.

2. ***APT 28,*** the GRU was active aggressively during the 2018 Olympics infecting some 300 computers simulating North Korean identity, a ***"false flag"*** excursion.
3. Recently ***APT 28*** was identified as the perpetrator of ***"ISIS -originated"*** emails to dependent wives of armed forces members, another **"false flag"** effort.
4. A reasonable assumption is that the MOD/GRU has, by now, developed specialized teams for cyber operations and has moved into development of unique capabilities for cyber warfare and more broadly, for information operations. And not only in the classical military venues one would expect, but with major targeting of civil infrastructures, such as the Grid. Being subordinate to the Federation Ministry of Defense, it also has the broader mission of support to Federation Armed Forces. Those linkages are much more obscure but have been seen in combat operations in the Ukraine and Syria.

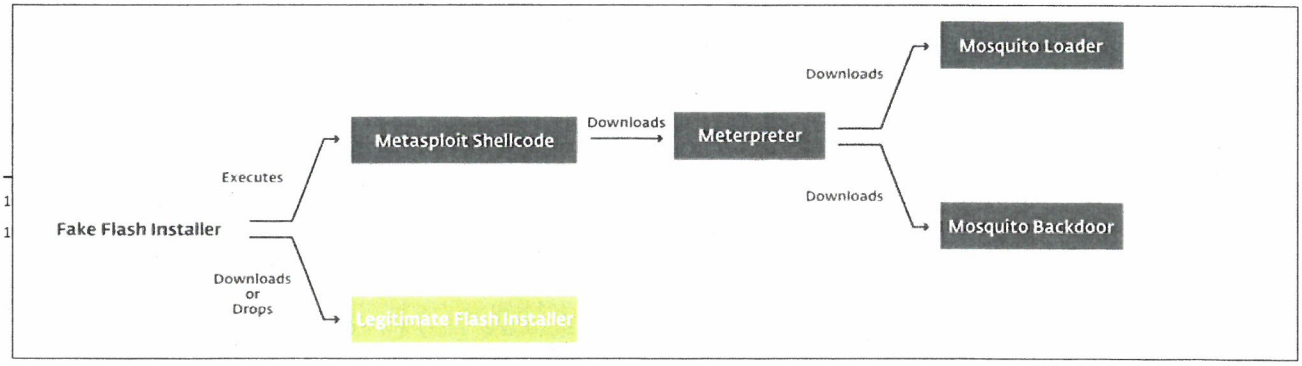
Other Federation Initiatives

Turla

A major cyber espionage operation has been labeled ***"Turla"*** by the security community. It has been tentatively traced back to the mid 90's, undoubted KGB in origin, making it one of the oldest, continuous operations of its kind. It involves classic cyber collection operations with a global character, but with the absence of "***active measures***" (destructive) but assured persistence. There are Russian language and cyrillac artifacts and tentative forensic linkages to SVR malware (eg., ***MiniDuke***) but care is obviously being taken to preserve ***TURLA's*** anonymity. ***TURLA*** fits the SVR foreign intelligence mission but may also support FSB interests in former USSR/European Satellite and current dissident/terrorist needs. The Federation clearly has a need to coordinate but also deconflict SVR and FSB cyber collection efforts which can be done with joint development and deployment of these technologies.

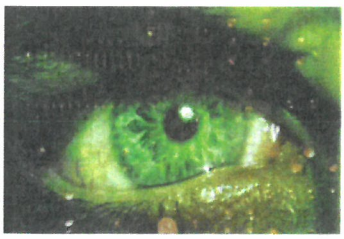
TURLA targeting is extremely precise with spearphishing and watering hole attacks the common credential-stealing methodologies. The value of the target is carefully assessed before comprehensive intelligence collection efforts are mounted. Droppers are usually customized to the victim's machine and the attackers' strategy is to maintain access to the victim as long as necessary. Targets are foreign embassies, ministries of trade, commerce, foreign affairs, consulates, NATO and EU military, and research universities.

TURLA[17] typifies the stealthy, totally customized nation-state cyber espionage operation, both global and domestic in scope, cataloguing potential targets until moving in for deep data penetration on high value facilities. It has several tool kits; their use depending on target and target systems. A unique feature of ***TURLA*** is its ability to download its Flash Player installer from a legitimate (Akamai) server that supports Adobe services, (a Supply Chain vulnerability of the 1st order.) Recently, ***ESET***[18] (the experts on ***TURLA***) spotted first time use of a generic exploit (Metasploit); a fundamental change in **TURLA's** technique.



A standard ***TURLA*** technique employs misleading emails to entice a victim to download a flash attachment containing a variety of embedded malware tools for eventual exploitation of a victim's system. A watering hole gambit may also be used. The trick is to encourage the victim to open his system to the ***TURLA*** exploits, funneled through the ***MOSQUITO*** backdoors.

FURTIM



Not observed since its 2016 appearance is the extremely sensitive malware, named ***FURTIM***.[19] ***Firefox*** is credited with its discovery. Two security firms that pieced ***FURTIM*** together in 2016 were ***EnSilo*** and **SentinelOne.** The former named it after the Roman word for "Stealth" after it failed to be detected by any of the 56 anti-virus programs tested by ***VirusTotal*** service. Although seen in one Energy firm, the consensus is that its intended purpose is far from clear. Based on the current state of defense in the energy industry, it would be absurd overkill for attacks on the Grid.

FURTIM's extreme stealth suggests it is intended for precision espionage, perhaps coupled to the most sophisticated Information Operations. For example, ***FURTIM*** won't install itself if it identifies on the target machine one of a huge array of security products used throughout the industry. It's sophistication, the extreme care taken in its development, and the absence of any significant evidence of use since 2016 is extremely worrisome (or should be) to observers of the Russian Federation's determined goal of supremacy in world-wide information operations.

[19]See, for example, 'Furtim's Parent, Stuxnet-like Malware, Aimed at Energy Firms" EWeek, By Sean Michael Kerner Posted 2016-07-12 and "EnSilo's Blog on Furtim", 10 August 2016.

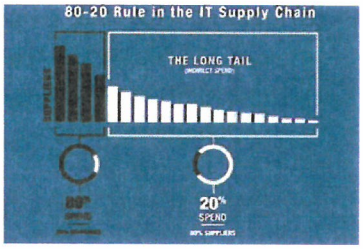
Appendix IV - Vulnerabilities, Vendors and Supply Chains

Introduction

No category of cybersecurity is more troublesome than the prospect of adversarial exploitation of supply chains for technologies, products and yes, even services essential to reliability of the nation's electric system. Utilities can not assure themselves of the security integrity of systems in use, or security of future systems that modernize the Grid. Active defenses, firewalls, encryption, SIEM technologies etc. themselves become the targets for malware developers; and even component hardware can no longer be trusted, with the internationalization of the semi-conductor industry and the ability of nation/states to exploit those sources. Malware compatibility with international standard protocols ***(Industroyer***) and the emerging ***FURTIM*** malware (***Appendix III)*** are but two examples that illustrate the Supply Chain problem.

Vulnerabilities

Unlike almost all other cybersecurity challenges, supply chain vulnerabilities lie almost entirely outside utilities' direct control. Obviously, the further up the supply chain, controls will be increasingly obscure, perhaps non-existent. For Operational Technologies, ignoring the potential for engineering errors. deliberate exploitable OT flaws should be unacceptable. OT vendors must be held accountable, precisely why Whitelisting and Blacklisting and Certification are on the table.



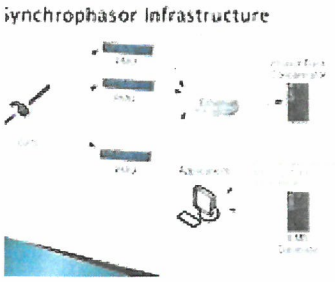
Information Technologies (IT) that underpin OT systems, or utility security products are a different security matter. These require the industry (and supporting OT vendors, state and federal governments, other industries) to force IT firms to significantly increase testing and supply chain controls to substantially reduce the risks to critical infrastructures. 150 plus patches in just one month's Microsoft release (March 2018) should shake confidence across the fabric of American critical infrastructures. Microsoft will continue to default to its users to find product flaws. CISCO's offerings are "edge" products, accessible to attackers and the firm's business practices (foreign dependencies) rule out any change in its approach to security. Mandatory and enforceable standards are overdue. Realistic? No. Alternatives? No.

Vendors

The Electric Industry almost completely avoids using its collective heft with its vendors to achieve standardization, to leverage Research and Development, or to pressure vendors to address vulnerabilities. As interoperability progressed over decades, NERC had to develop essential ***Reliability*** standards that have forced vendors to meet stiff interface and stability measures for Operational Technologies (OT). But with the substantial transition from analog to digital systems, the process has become much more complex, extending well beyond physical interfaces. Data flows have magnified vulnerabilities and utilities are facing new "data interoperability" issues. There is no apparent mechanism to manage cybersecurity issues in this badly fragmented industry. Neither

their industry organizations (e.g., EPRI) nor their regulators nor the federal government attempt to address the overall supply chain challenge. They have been consigned to the ***"too-hard-pile"*** by the feds and the industry.

Unlike Reliability Standards, CIP Standards give vendors a free pass. Under guidance from FERC to NERC on development of supply chain cybersecurity standards, with prodding from NERC, FERC stated: ***"In addition, the Commission stated that NERC's response to the Order No. 829 directive should respect the Commission's jurisdiction under FPA section 215 by only addressing the obligations of responsible entities and not by directly imposing any obligations on non-jurisdictional suppliers, vendors or other entities that provide products or services to responsible entities."*** It also mitigates responsible entities' role; example: PG&E's very minor penalty for its vendor's major breach of data security in 2016.[1] Here FERC is getting a clear signal from NERC and the Industry, we are at the limits of what we wish to do to secure this critical infrastructure, and FERC agreed.



Another example is captured in the Appendix I discussion of the impact of Synchrophasor Units (PMUs, PDCs) on Grid modernization. There is regrettably, no organized effort by the industry or federal overseers to leverage this major development in either Reliability Standards or Cybersecurity Standards. Thus, many different products are going into the Grid with poor or non-existent cybersecurity features. DoE PMU Grants beginning in 2009 left encryption and security as an optional choice to utilities. NASPI, a coalition of researchers, several interested vendors, centers-of-excellence etc., maintain collaborative exchanges of PMU information and development initiatives but technical standards revert to NIST-IEEE working groups and since it is an international process, there is very low priority on cybersecurity. Thus, Synchrophasors are one of the few, major opportunities for cybersecurity to be "built in" during development and address the glaring insecurities of Distribution systems - a lost opportunity.

While it is very hard to believe that Russian subversion of three of the most-used electric industry control systems went two years before revealed in the 2014 US Grid attack, that appears to be accurate and speaks legions about the ineffectiveness of CIP standards. The details remain hidden from the public's view. And it only came to light because its use depended on a Microsoft zero-day exploit, caught by forensic analysts investigating presence of Russian-developed malware (***HAVEX*** and ***BlackEnergy2***) in US networks.

An important aspect to all this is the growing dependency of utilities on vendor direct access to operational systems for maintenance, often across the Internet. The PG&E breach previously described was one such event. This is a major supply chain vulnerability, made worse by the total exclusion of internet connectivity from CIP standards. Shielding the vendor from responsibility works to the distinct advantage of the adversary.

---

[1] See FERC Dockets Nos. NP18-7-000 and NP18-10-000. NERC and FERC's approval of the WECC settlement with an Unidentified Responsible Entity (aka PG&E) for the known, most severe utility data breach of 590 days duration, exposing tens of thousands PG&E cyber assets including Critical Cyber Assets, asserting that anonymity and settlement claims required CCII protection, was an egregious example of vulnerability and compliance failures of CIP Standards. A settlement of only $2.7M for a corporation earning close to $20B in revenue in 2017, is patently absurd and says volumes on the cybersecurity shell-game played by this industry and its regulators.

Supply Chain Standards

FERC Order Nr. 829[2] contained a directive requiring NERC to develop Supply Chain standards. FERC NOPR of 18 January 2018[3] proposed to approve NERC's submission, essentially modification to Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). However, adequate supply chain standards should involve, at a minimum, whitelisting, blacklisting or certification. How else to put pressure for security on vendors?

Filings with FERC[4] in opposition to these modifications to standards, have had little effect. Such filings noted the nation's adversaries' exploitation of Supply Chain vulnerabilities that would easily avoid CIP, highlighted the exclusion of so-called low impact assets, re-emphasized the unaddressed Internet connectivity issue and cited specific examples of the complexity of these vulnerabilities. It was pointed out that Microsoft patch Tuesday (in March 2018) listed 157 vulnerabilities across its product set, most of which are within the IT underpinnings for vendor technologies comprising this end-to-end data exchange. ***Q: Can any "Responsible Agent" exercising its responsibilities under the Supply Chain requirements in this NOPR understand and contend with the March 2018 Microsoft vulnerabilities, or is it the vendor's responsibility that employs the Microsoft systems in the IT portion of its offerings?*** This conundrum surely proves the shallowness of current CIP processes (which NERC would further delay in implementation for 18 months), and argues for stiffer standards, I.e., whitelisting, blacklisting, vendor certifications for example.

With this filing, NERC and the industry went to a full court press, flooding FERC with filings from industry associations and major utilities supporting NERC's standards, with no apologies for completely excluding from these weak standards, the 90% of so called low impact cyber assets (transmission facilities) not under CIP Standards. (see table in ***Appendix II***). FERC has yet to file a formal rule on Supply Chain Standards.

Summary

FERC will undoubtedly approve the NERC proposals, with its usual "it's better than nothing" circumlocution. This vulnerability vector is of primary importance to adversaries as a back door into victim's systems. NERC and industry's fixes in CIP Standards put impossible pressure on utilities since those standards are procedural, non-technical "objectives", not show stoppers for sophisticated, embedded malware, firmware and hardware

Utilities do not have the skills or manpower to do reverse engineering of complex systems to determine if they are safe to use, which is what the proposed standards would require. Further, many other flaws in CIP Standards make detection much more complicated. Where did the infection take place? Do systems remain vulnerable because of Internet connectivity? Is it a major flaw in a commercial IT undercarriage (e.g., operating system)? Is it a zero-day vulnerability with no known signature? Is it a hardware bug deliberately designed into a component? Is it a safety-critical system deactivated on command?

---

[2] Docket No. RM16-18-000, Cyber Systems in Control Centers (Issued July 21, 2016)

[3] [Docket No. RM17-13-000 Supply Chain Risk Management Reliability Standards (January 18, 2018)

[4] Isologic LLC filing: NOPR Supply Chain Risk Management Reliability Standards, (January 18, 2018) [Docket No. RM17-13-000].

Utilities face a quadruple supply chain whammy. First there is the uncertainty of delivered flaws in vendor's operational systems. Second, there are the considerable vulnerabilities of the utility's installed IT systems that underpin vendor's offerings. [5] Third, there are the commercial IT systems that deliver management functions to EMS, EACMS and other utility installations[6], and fourth, there are the network connections including direct internet accessibility for actual supply chain attacks, that link all this together.[7]

Supply Chain vulnerabilities are surely the last straw in the futile regulatory cybersecurity process. Surely the IT industry will not be policed on their contributions to the supply chain problem. Surely the industry and its vendors cannot afford the costs for even moderate protection for OT supply chain flaws. ***Surely supply chain risks point directly to the need for the National Critical Infrastructure Deterrence polity outlined in this paper.***

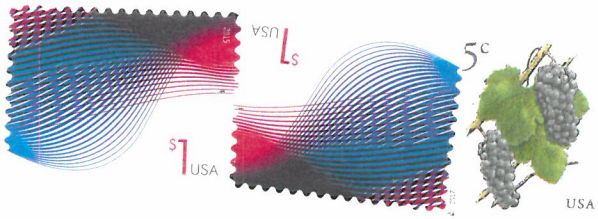
---

[5] Merely examine Microsoft's monthly Patch Tuesday release, usually delivered directly to Utilities IT systems. Example: newsletters@news.computerworld.com July 4, 2018. Note mention of follow-up required for flaws and vulnerabilities.

[6] Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans, June 2017

[7] NERC Remote Access Study Report, Docket No. RM15-14-__, June 30, 2017

Mr. George Cotter
193 Southdown Rd.
Edgewater, MD 21037



Kristine L. Svinicki, Chairman,
Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852

JUL 16 RECD