Perry Center Occasional Paper

April 2016

Critical infrastructure in Latin America: connected, dependent, and vulnerable.

Dr. Boris Saavedra

William J. Perry Center for Hemispheric Defense Studies

National Defense University

The opinions, conclusions, and recommendations expressed or implied in this book do not necessarily reflect those of the William J. Perry Center for Hemispheric Defense Studies, the National Defense University, or the U.S. Department of Defense.

Editor in Chief: Pat Paterson
Layout Design: Viviana Edwards

Critical Infrastructure in Latin America: Connected, Dependent, and Vulnerable.

by Dr. Boris Saavedra

William J. Perry Center
for Hemispheric Defense Studies

Perry Center Occasional Paper

April 2016

Critical Infrastructure in Latin America: Connected, Dependent, and Vulnerable.

by Dr. Boris Saavedra

> If you think technology can solve your security problems, then you don't understand the problem and you don't understand the technology.
>
> *Bruce Schneier*

Introduction

Technological advances have benefited our world in immensurable ways, but there is an ominous flip side: digital technology can be turned against us. Hackers can activate baby monitors to spy on individuals, while thieves and terrorists are analyzing social media posts to plot everything from home invasions to disrupting critical infrastructure. Information and Communication Technologies (ICT) based on computers are the driving forces that have been created and can be hacked. This is a sobering fact given our radical dependence, connectivity, and vulnerability on these machines for everything from our individual needs to the financial and production services of a nation's power grid. The objective of this paper is to call the attention of those in the military and intelligence communities, and academic, industrial, and civic authorities in Latin America and the Caribbean about the vulnerabilities of critical infrastructure in the region particularly power grids and its security system in the cyberspace.

Cyber Crime and Critical Infrastructure

Cyber criminals have become adept at using the Internet for robbery on an almost unimaginable scale; siphoning off wealth or hijacking several million dollars is grand larceny. More worrisome is the increasing number of cyberattacks designed to collect enormous quantities of data in what appear to be wholesale intelligence-gathering operations. One of the most recent was one that targeted the U.S. government's Office of Personnel Management (OPM) which handles government security clearances for federal employee records. But as disturbing as these massive data collections may be, they do not even come close to representing the greatest cyber threat. Our attention needs to be focused on those who intend widespread destruction.

The Internet provides instant access to critical infrastructure systems. In this regard, power grids represent a perfect target to hit with cascading effect. Electricity is what keeps our society tethered to modern times. In today's nations, the very structure that keeps electricity flowing depends on computerized systems designed to maintain perfect balance between supply and demand. Maintaining that balance is not only an accounting measure, it is also an operational imperative. For the grid to remain fully operational, the supply and demand of electricity have to be kept in perfect balance. It is the Internet that provides the instant access to the computerized system that maintain the equilibrium. If a sophisticated hacker gained access to one of those systems and succeeded in throwing that precarious balance out of kilter, the consequences would be devastating.

Today we can take limited comfort in the knowledge that such as attack would require ample effort —it requires significant preparations and a highly expensive and sophisticated understanding of how the system works and where its vulnerabilities lie. Less reassuring is the policy, strategy, and knowledge whether Latin America and the Caribbean nation's expertise, and—even more unsettling—that criminal and terrorist organizations are in the process of acquiring it.

Latin America and the Caribbean are expected to grow at only a modest pace in the coming years given relatively low growth across the globe. The United States is growing more strongly reflected by the recent rise in U.S. interest rates. The preferred currency of financing has been highly stable and focused to a very large degree on the U.S. dollar. In turn, this implies that the cost of capital will likely increase for the region's government loans as U.S. policy rates rise. It mean a reduction in security and defense investments particularly in the area of cybersecurity.[1]

Connectivity

For centuries, the Westphalian system of sovereign nation-states has prevailed in our world. The system's structure has been preserved through borders, armies, guards, and guns. Controls are implemented to limit both immigration and emigration of people, goods, and services from a nation's territory. Though physical borders still matter, such divisions are much less clear in an online world. Bits and bytes flow freely from one country to the next without any border guards, immigration control, or customs declaration to slow their transit. The traditional transnational barriers to good and bad actors have been demolished in the online world, allowing unsavory individuals to freely enter and exit any virtual location as they please.

The interconnectivity the Internet provides through its fundamental architecture means that disparate people from around the world can be brought together as never before. While the advantages of the online world are well documented and frequently highlighted by those in the tech industry, there is also a downside to all of this interconnectivity. Our basic services are a critical infrastructure dependent on computers. Each day, we plug more and more of our daily lives into the global information and communication grid without pausing to ask what it all means. What should happen if and when the technological trappings of our modern society—the foundational tools upon which we are utterly dependent—all go away? What is humanity's back up plan? In fact, none exists.

[1] Andrew Powell. "The Labyrinth: How Can Latin America and the Caribbean Navigate the Global Economy," *Latin American and Caribbean Macroeconomic Report, Inter-American Development Bank,* March 2015. https://publications.iadb.org/handle/11319/6850?locale-attribute=en

The nature of the Internet means that we are increasingly living in a house of glass and in a borderless world. Today anybody with good or ill intent can virtually travel at the speed of light halfway around the planet. For criminals, this technology has been a boon as they hop from one country to the next virtually hacking their way across the globe in an effort to frustrate government control. Criminals have also learned how to protect themselves from being tracked online. Smart hackers never directly initiate an attack against an institution or organization. Instead, they would route their attack from one compromised network to another in different geographic locations. This ability to country-hop, one of the Internet's greatest strengths, create enormous jurisdictional and administrative problems for enforcement agencies and is one of the main reasons why cybercrime investigation is so challenging and often feckless. Government authority remains within national borders.

Connectivity generates a vulnerability for which hackers can craft computer attacks known as "zero day exploits" that take advantage of previously unknown flaws for which no defense has been built. (The target has had "zero days" to prepare for the attack). Zero day is the most effective cyber weapon. It provides the element of surprise, which is one of the ultimate advantages in battle. The zero day exploit is tailor-made to use against a specific target. Because that defenseless point in a system is likely to be patched as soon as the target realizes it has been hit with a zero day, it may be used only once.[2] The targets that are most vulnerable to a devastating zero day attack are electrical power plants, nuclear facilities, natural gas and oil pipelines, and other critical infrastructure, including banks and financial services companies.

More connections means more vulnerability. According to Pew Research Center, the Internet of Things (IoT) is a "global, immersive, invisible, ambient-networked, computing environment built through the continued proliferation of smart sensors, cameras, software, databases, and massive date centers in a world-spanning information fabric."[3] Thanks to advances in circuitry, software, and

[2] Shane Harris, @*War the Rise of the Military-Internet Complex*. New York: Eamon Dolan/Houghton Miffin Harcourt, 2014.

[3] Marc Goodman. *Future Crimes Everything Is Connected, Everyone Is Vulnerable and What We Can Do about It.* (New York: Doubleday), 2015.

miniaturization, it is possible to build an Internet of Things whose devices fall broadly into one or two categories: sensors and microcontrollers.

In order for things to go online and communicate with one another, they must first be enabled with the technological equivalent of speech. In order to make this happen, the IoT relies on a series of competing communication technologies and protocols. Cellular and mobile data transmission standards such as LTE, 4G, GSM, and CDMA connect devices to the mobile phone network. The result is billions of embedded chips in things using standards such as Wi-Fi, Bluetooth, ZigBee, Z-Wave, near-field communications, and radio-frequency identification in order to communicate.[4]

The basic communication protocol that rules nearly all traffic on the Internet, the backbone of today's Internet, runs on what is known as Internet Protocol Version 4 (IPv4). It has been around since 1983 with a capacity about 4.3 billion addresses each one representing a connected device. In the future, IoT will require expansion of current capacity. The answer to this problem is IPv6 which will supplant IPv4 and profoundly increase the size of the addressable space available on line. The new protocol will increase the length of the phone number from 32 bits to 128 bits. Mathematically, IPv4 can only support about 2^{23} bits or 4.3 billion connections. IPv6 on the other hand, can handle 2^{128} or 340,282,366,920,930,463,463,374,607,431,768,211,456 connections. That means IPv6 would allow a trillion IP addresses to be put in one grain of sand.[5]

According to Marc Goodman, founder of the Future Crime Institute and the Chair for Policy, Law, and Ethics at Silicon Valley's Singularity University, "connecting everything to a global Internet of Things may indeed have tremendous value, connecting everything insecurely does not." Before adding billions of hackable devices and communicating with hackable data transmission protocols, important questions must be asked about the concomitant risk of security, crime, terrorism, warfare, and privacy. Finally, the expansion of the Internet using IPv6 will add 340 undecillion (340 trillion, trillion, and trillion) new potential nodes to the global information grid with an additional $6.2 trillion value to the global economy and fifty billion online devices by 2020.[6] The question is what are the global security implications of this expansion? What are the measures that our region need to take to confront a major threat that is moving at the speed of sound?

In Latin America, some electrical, nuclear, natural gas, and oil pipeline are under government control. Others are controlled by private companies. For example, the Argentine power sector is one of the most competitive and deregulated in South America. However, the fact that the Energy Secretariat of the Argentine government has veto power over *Compañía Administradora del Mercado Mayorista Eléctrico* (CAMMESA) has the potential to alter the functioning of the competitive market. Generation, transmission, and distribution are open to the private sector, but there are restrictions on

[4] "The Internet of Things," *Alexander Von Humboldt Institut Fur Internet und Gesellschaft*, 2011 http://www.hiig.de/en/events/berlin-symposium-on-internet-and-society/

[5] Goodman, 226.

[6] Ibid, 227.

cross-ownership between these three functions. Argentine law guarantees access to the grid in order to create a competitive environment and to allow generators to serve customers anywhere in the country.

On the other hand, countries of the Caribbean region face crucial energy challenges on electricity generation, interconnection, and fuel supply strategies. Paramount among them is to manage their high dependence on oil (and oil products) that fuel their domestic economies, in particular the power sectors. Most countries' power plants rely primarily or entirely on imported diesel and heavy fuel oil (HFO). Most have small and fragmented power systems and there are no existing interconnections. Some regional projects, such as the Eastern Caribbean Gas Pipeline (ECGP), have been proposed but not yet materialized. Customers in the Caribbean countries already face some of the highest electricity tariffs worldwide and their governments are increasingly concerned about the environmental burden of the current power generation, especially in tourist-driven economies.

There are alternatives to nearly exclusive use of diesel and heavy fuel oil for power generation. Liquefied natural gas (LNG), compressed natural gas (CNG), and pipeline natural gas may be economically and financially viable. Agricultural wastes, coal, and petroleum coke may also be viable options for fueling power generation. Geothermal, solar, wind, and hydro power plants exist in the Caribbean today and expansion of those renewable energy options may be feasible. Finally, development of submarine cable electrical interconnections among the countries would enable them to share lower cost resources, provide mutual support, gain economies of scale in power plants and systems, and obtain the benefits of power pools generally.

Dependability

When institutions or companies find out about a risk in their systems, it is up to them to apply patches and defensive fixes. Their technological fluency of companies vary.[7] Some may be prepared to patch systems quickly. Others may not even realize they are using a vulnerable piece of software. They, quite literally, may not have received the memo from the vendor warning that they need to install an update or change the security setting on a product in order to make it safer.

Even if the institution or company is using software that receives regular updates over the Internet, the company's system administrators have to consistently download those fixes, make sure they are applied across the institution or company, and stay on watch for more updates. Some find doing that for hundreds of thousands of computers in a single facility a daunting task.

In Latin America and the Caribbean, cyberattacks on energy power plants could become the most serious threat to any country for the impact on the population and physical destruction of structures in an extremely wide area. Most countries have laws and protocols on cybersecurity, but they are very incipient and militarized. Therefore, the government institution tasked to monitor and respond to a cyberattack is often the military. At the present, most of these institutions are precluded from doing

[7] Shane Harris, *@War the Rise of the Military-Internet Complex*. New York: Eamon Dolan/Houghton Miffin Harcourt, 2014.

so by the lack of a comprehensive strategy, laws, and specific training. Additionally, scarce budget and resources prevent the government from acting proactively in a coordinated way with civilian authorities and private sector to confront breaches of infrastructure security.

For example, Colombia has had a liberalized energy market since 1995. The sector is characterized by an unbundled generation, transmission, distribution, and commercialization framework.

The structure of the Colombian energy market is based on Laws 142 (Public Services Law) and 143 (Electricity Law) of 1994. The Ministry of Mines and Energy is the leading institution in Colombia's energy sector. Within the Ministry, the Unit for Mining and Energy Planning (UPME) is responsible for the study of future energy requirements and supply situations, as well as for drawing up the National Energy Plan and Expansion Plan.

The Regulatory Commission for Gas and Energy (CREG) in Colombia is in charge of regulating the market for the efficient supply of energy. It defines tariff structures for consumers and guarantees free network access, transmission charges, and standards for the wholesale market, ensuring the quality and reliability of the service and economic efficiency. CREG is responsible for providing regulations that ensure the rights of consumers, the inclusion of environmental and socially sustainable principles, improved coverage, and financial sustainability for participating entities. The provision of public services (water, electricity, and telecommunications) to final users is supervised by the independent Superintendence for Residential Public Services, or SSPD.

Public-Private Partnership

Countries where electric power companies are privately owned are at risk. This is the model known as vertical integration. In these cases, companies own the plants that generate the power, the transmission facilities, and the equipment that ultimately deliver the electricity to schools, business, hospitals, and homes. The managers of these industries have to be equally invested in securing the equipment that generate the power, safeguarding the transformers and lines that transport it, and protecting the hardware that delivered it to the consumers. Electricity is generated by variety of means, including nuclear, coal, natural gas, and hydro; whatever the energy resource, the business model is essentially a monopoly, whose interests demand attention to every aspect of the system. Therefore, the best way to accomplish the security demand in cyberspace is with the combination of Public-Private Partnership (PPP) in cybersecurity.

Policy, strategy, and legislation should be formulated on two main principles: common good and profit to avoid tension between the private and public sector. For example, although Colombia has strong public and private participation in the electricity industry, they do not have a specific cybersecurity policy, strategy, and protocols based on Public-Private Partnership to share information that protect and preserve this very important aspect of the country's critical infrastructure.

Information-sharing by private and public sectors is essential to deterring cyberattacks on the critical infrastructure of the nation.[8] There is an unavoidable tension between industry's insistence that it be allowed to operate within a free enterprise system and government's responsibility to develop high standards of safety and security for what may be the nation's single most critical piece of infrastructure.

The system maintenance and protection reside in so many different hands though because its complexity has made each player more dependent on computerized control system. The electrical grid is also more vulnerable than it used to be. There are new pathways through which malicious cyberattacks may travel. Security and day-to-day reliability become a shared responsibility and, as with any other chain, the electric power grid may only be as strong as its weakest link. Leaders in government and industry will have different arguments. In the private sector, those who have invested enormous resources in protecting their infrastructure and have lean profit margins are simply not inclined to spend a great deal on cybersecurity. In the other hand, companies under government control will argue the lack of budget to invest in cybersecurity limits them. In both cases, the weakest links in this system tend to generate poor security and maintenance practices. They do not have the infrastructure or the resources to do what actually needs to be done.

One might assume that the government, in the interest of safeguarding what is arguably the most critical infrastructure network in the country, can simply impose security and maintenance stan-

[8] Ted Koppel. *Lights Out: A Cyberattack A Nation Unprepared Surviving the Aftermath* (New York: *Crown Publishers,* 2015), 15.

dards on the industry. Beginning with those countries where the government owns the electrical power plants, they should comply with these regulations. For those countries where the industry have been privatized, they must impose security standards to these companies in charge.

Meaningful Public-Private Partnership (PPP)

Government efforts to protect the people against everyday cybercrime and security threats have been wholly inadequate. The need for more serious and profound collaboration between the public and private sectors is compelling. Without it, we will make little meaningful progress in improving the overall state of our security. The need is particularly vital when it comes to protecting critical infrastructure at the global level, 85 percent of which are in the hands of private sector.[9] Recognizing the need for PPP institutions as diverse as defense and security institutions, the European Union and the World Economic Forum have established programs to foster greater cooperation among those responsible for running the world's critical infrastructure.

Initial efforts at PPP have proven helpful, to be certain, but some PPP efforts have been criticized for having ill-defined goals and few if any specifically articulated objectives beyond "sharing information." The private sector generally lacks trust in the government to maintain its confidentiality, particularly when it comes to revealing cyber-threat data to competitors, let alone protect it from antitrust risk. The government also takes challenges; it must figure out how to share knowledge of particular cyber risk, many of which are classified, with companies and technical personnel that lack the required clearance to see the classified material.

One positive aspect that should be taken into consideration is to reach out beyond those in the government and industry who make fighting cyber threats their full-time occupation. Another massive force can be brought to bear on the technological challenges we face: a smart and engaged general public.

Vulnerability

It is not easy to explain how and why the electric power grid is so surpassingly vulnerable to cyberattack. We need to understand a little more about the exchange and conveyance of electricity. In some countries, reforms to the electric power industry broke up the old, vertical integrated industrial monopolies. Those companies generated the electricity, sent it across great distances along high-voltage transmission lines, and then distributed that electricity to the consumers. Now different companies or combination of government and private companies are responsible for different phases of the process. The company that distributes electricity in one community is different that the company that generate

[9] Goodman, 379.

or transmit electricity. Breaking up the industry into a marketplace of interconnected parts introduced competition which subsequently lowered prices. It also increased the system's vulnerability to cyber intrusion.

In most Latin American and Caribbean countries, there is no specific government agency best equipped to monitor infrastructure for signs of cyberattack. In those countries where the military is in charge of cybersecurity, they are precluded from doing so by the lack of policy, strategy, laws, and protocols that are designed to prevent a cyberattack on power grids. In those countries where power grid functions such as generation, transmission, and distribution are combined between government and private companies, there are not legal mandates to share information where there are breaches of infrastructure security.

Brazil is a good example of a nation in which the military in charge of cybersecurity is constrained in its effectiveness because of the current governance of the electricity industry and lack of specific policy, strategy, and protocols. In Brazil, large government-controlled companies dominate the electricity sector. Federally-owned Eletrobras holds about 40 percent of capacity (including 50% of Itaipu dam complex), with state-companies Companhia Energetica de Sao Paulo (CESP), Companhia Energetica Minas Gerais, (Cemig), and Companhia Pananaense de Energia S.A (Copel) controlling 8 percent, 7 percent and 5 percent of generation capacity respectively. About 27 percent of generation assets are currently in the hands of private investors.

Transmission has remained almost exclusively under government control through both federal (Eletrobras) and state companies mainly Sao Paulo-Companhia de Transmissao de Energia Electrica, Minas Gerais-Cemig, and Parana-Copel) until recently. However, under the new sector regulatory model, there are about 40 transmission companies. Additionally, there are 49 utilities with distribution concessions and about 64 percent of distribution assets are controlled by private sector companies.

Required Policy and Regulations Reforms

The Ministry of Energy and Mines (MME) in Brazil has the overall responsibility for policy setting in the electricity sector while the Electricity Regulatory Agency (ANEEL), which is linked to the Ministry of Mines and Energy, is the Brazilian Electricity Regulatory Agency created in 1996 by Law 9427. ANEEL's function is to regulate and control the generation, transmission and distribution of power in compliance with the existing legislation and with the directives and policies dictated by the central government. The National Council for Energy Policies (CNPE) is an advisory body to the MME in charge of approving supply criteria and "structural" projects while the Electricity Industry Monitoring Committee (CMSE) monitors supply continuity and security. However, there is not a specific policy on cybersecurity issues in the industry and the responsibilities of the military in charge of cybersecurity at national level.[10]

[10] Global Investment & Business Center, USA. *Brazil Energy policy, Laws and Regulations Handbook Volume 1* Strategic Information and Basic Laws, Washington DC, 2012.

The potential for high-stakes duels between corporations and government regulators exists, the consequences of which could be cybersecurity regulations so patchwork and inadequate as to be one of the chief sources of the grid's vulnerability. General Keith Alexander, who retired as director of National Security Agency (NSA) in 2014, explained the issue as a simple cost/benefit ratio.[11] Small companies that are in charge of distribution cannot afford very expensive cybersecurity investment.

On the other hand, conveyance of electricity along transmission lines has to be scheduled. Electricity functions not simply as conveyance directly from Point A to Point B; instead it's all about maximum efficiency and maintaining overall balance between demand and supply throughout the system. To coordinate this, the industry has set up regional authorities, the regional transmission organizations, and independent system operators which monitor traffic to ensure that no transmission lines in their area become overburdened.

Leaders in the industry argue that this monitoring process, while routine, also creates a dangerous point of vulnerability. If someone was able to hack into a Regional Transmission Organization (RTO) or Independent System Operators (ISO) and deliberately overload the lines, the impact would be swift and physical.[12] The line would start to droop from the heavy load. They would overheat. When the lines dip, they can set a tree on fire, or they can melt the line. There are built-in controls to ensure that such an overcapacity never happens, but if a hacker got into the system and targeted those controls, the controller sitting in the operations center may not detect it. There would be no relationship between the operations center dashboard and reality. Such a situation could quickly escalate out of control. If the hacker can break key transmission lines, he or she could produce cascading, potentially catastrophic outages.

The question today is: is it possible? It is anything but simple. It would require detailed mapping and lengthy reconnaissance operations to conclude what to target and how to find a critical point of failure in the system. But it is, technically speaking, more plausible today than ever before. According to the experts, we generate power in very efficient quantities at specific locations and then move that power oftentimes at great distances to where it's being consumed. If someone was knowledgeable about the functioning of a Supervisory Control and Data Acquisition (SCADA) system and succeeded in hacking into it, that individual could engineer a series of events that seem totally unrelated but which could, according to experts, turn the lights out very quickly over large areas.[13]

[11] Koppel, 29.

[12] Ibid, 37.

[13] Ibid, 39.

Analysis

In terms of the power grid, the number of attacks has increased exponentially with the integration of everyday devices on the Internet. Where a prospective hacker in the past might have had to go after a server or a desktop computer to gain access to an electric company's corporate network, now he or she can do it by way of devices that enable a consumer to program the light or heating and air conditioning in his or her home remotely or automatically.[14] In other words, the smart thermostat that automatically lowers the temperature in a consumer's or customer's home at night or warms his or her kitchen before he or she gets up in the morning has to be connected to the company's billing department which in turn needs to be connected to whatever department actually conveys electricity to the home. Each connection provides another potential attack surface.[15]

Another vulnerability is the concept that the administrative network is "air gapping" for the operational side of each power company, meaning that there is no physical connection between the two. Power companies insist that those two networks are absolutely separate and not connected. However, the problem with air-gapping, according to experts, is that it fails to take the human factor into account. "Every time a worker brings in a thumb drive or laptop from home and hooks it up to an isolated system, the mobility of workers bridge the air gap", one industry worker said.[16]

In this way, would-be hackers, operating on what is sometime referred to as the "Sneakernet," can introduce their malware, their viral programs, by way of an employee's insecure iPhone or thumb drive. Anything less than absolute hygiene provides a potential attack surface. Absolute hygiene may be theoretically possible, but it would be prohibitively expensive—not just for smaller, local companies but also for regional authorities tasked with monitoring vast areas.

There are two different aspects that need to be taken into consideration. First, artificial intelligence (AI) refers to the study and creation of information systems capable of performing tasks that resemble human problem-solving capabilities, using computing algorithms to do things that would normally require human intelligence such as speech recognition, visual perception, and decision making. Second, black-box algorithms with encoded math are formula written by human being and designed to carry out their instructions, their decision analyses, and their biases.[17]

Algorithmic hacking could also cause major problems for society and its critical infrastructure because altering just a few lines of code among millions in an intelligent agent's programming could be nearly impossible to detect but could lead to drastically different outcome in the algorithms behavior. The attack against the uranium centrifuges at the nuclear enrichment facility in Natanz, Iran, is a perfect example of this type of threat, a subtle change that destroyed enrich centrifuges and took years to discover. How would we know if one of the electric power plant algorithms were felly or mali-

[14] Ibid, 42.
[15] Goodman, 230.
[16] Koppel 59.
[17] Goodman 321.

ciously subverted? The criminal opportunities afforded by the combination of these two elements AI and black-box algorithms will grow in their use and sophistication, but they may pale in comparison to what becomes possible with stronger, more cap able, and rapidly evolving forms of artificial intelligence in the near future.[18]

Potential solutions

Defending against a cyberattack is something that only a coalition between government and private industry can even attempt. So it is to be expected, perhaps, that government's primary emphasis remains on prevention—proposing a government-industry cyber war council to stave off terrorist attack. It will be integrated by private industry executives and deputy-level representatives from security and defense sector agencies. This outreach to government is a measure of rising alarm in the ranks of private industry and big business.

There is not yet widespread recognition that we have entered a new age in which we are profoundly vulnerable in ways that we have never known before. Therefore, there is neither a sense of national alarm nor the leadership in most nations of Latin America and the Caribbean to take actions where we need to go in this complex matter. At the present time, regional leaders are in a precarious place. This is the first time in the history of warfare, that small group, even individuals, can undermine the critical infrastructure of a state.

What would result directly from an attack to the electrical grid—the population flow, the extended distribution of emergency supplies, and the likelihood of civil unrest—would require the combined expertise and resources of many government agencies, but all would fall, inevitably, under the overall control and management of the military. It is the only organization with the equipment, training, and manpower equal to the task. That will become all too self-evident after an electric power grid is disabled.

In the absence of any preparation, in the absence of any serious civil defense campaign that acknowledges the likelihood of such as an attack, predictable disorder will be compounded by a profound lack of information. It would be the ultimate irony that in the information age characterized by instant communication and information, the government failed to disseminate the most elementary survival plan until the power was out and it no longer had the capacity to do so.

Technological changes occur and we accept them for the most part. The changes have been happening so fast that we haven't really evaluated their effects or weighed their consequences. We can start by renegotiating the bargains we're making with our critical infrastructure. Our political leadership, and experts in security and defense in public and private sectors in Latin America and the Caribbean need to be proactive about how we deal with cybersecurity for critical infrastructure particularly with electrical power grids. We need to think about what we want our policy, strategy, and technological infrastructure at the national and regional level to be, and what values and priority we want it to embody.

[18] Ibid 322.

There is a literacy problem around the world and it is not the one most obvious. It is the problem of technical literacy. In a world replete with gadgets, algorithms, computers, Radio Frequency identification (RFID) chips, and smart phones, only a minimal portion of the general population has any idea how these objects actually work. The objective is not for every single person to become a computer coder. The objective is for citizens to have a basic understanding of how the technologies around them operate, not just so that they can use these tools to their full advantage, but also so that others cannot take advantage of their technological ignorance and harm them. Education is key and the state of our cybersecurity education is abysmal.

The effort needs to be greatly expanded if we are to meet the level of threat heading our way across a wide array of technological developments, such as the IoT that needs to be handled at a systemic level. Individuals have to understand the risk and take responsibility to protect themselves and their families to the fullest extent possible.

The way forward

Cyberattacks happen—they cannot all be stopped. The challenge of emerging technology is to create a more resilient capacity to an attack. A resilient system will continue to perform its most critical functions, though other less important activities may go off-line or cease to operate. Much of the technological infrastructure is subject to common single points of failure, the most obvious of which is power. No electricity, no Internet. Worse, no electricity, no water distribution, food production, financial transaction, communications, or transportation. We need to isolate these singular failure points so that they do not spread. We also need to have alternative power sources that we can scale to prevent these types of "blackouts"—not just for electricity of course, but for all the technological tools that make our modern civilization possible.[19]

Critical infrastructure, particularly electrical power, have little or no chance of withstanding a cyberattack even with resilient capability. Weak cybersecurity standards with wide-open communication and networks virtually guarantees success to major nation state and competent hacktivist, the electric power industry, according to experts in the field of cybersecurity, is vulnerable if this grid if subject to a sophisticated attack. When such attacks occur, make no mistake, there will be major loss of life and serious crippling of national security capability of national security capabilities.[20]

Let us conclude this paper by reiterating its objective, calling the attention of those in the military, and intelligence communities, and academia, industrial, and civic authorities in Latin America and the Caribbean about the real status of critical infrastructure in the region particularly, power grids and its security system in the cyberspace. Starting with acknowledging ignorance is often the first step toward finding a solution. The second step entails identifying the problem. According to Ted Koppel, "for the first time in history of warfare, governments need to worry about force projection by individual laptop. Those charged with restoring the nation after such an attack will have to come

[19] Ibid 360.

[20] Koppel 49.

to terms with the notion that the Internet, among its many, many virtues, is also a weapon of mass destruction".[21]

Public-Private Partnership Energy in Latin America and the Caribbean[22]

Country	Generation	Transmission	Distribution
Argentina	60% private 40% public	100% private 0% public	70% private 30% public
Brazil	30% private 70% public	10% private 90% public	60% private 40% public
Chile	90% private 10% public	90% private 10% public	90% private 10% public
Colombia	70% private 30% public	10% private 90% public	50% private 50% public
Peru	60% private 40% public	20% private 80% public	80% private 20% public
Jamaica	20% private 80% public	0% private 100% public	0% private 100% public
Trinidad and Tobago	40% private 60% public	0% private 100% public	0% private 100% public
El Salvador	40% private 60% public	0% private 100% public	100% private 0% public
Honduras	62% private 38% public	0% private 100% public	0% private 100% public
Nicaragua	70% private 30% public	0% private 100% public	100% private 0% public

[21] Ibid 139.

[22] Herz, Rafael, Jan Kappen, and Lucio Monari. *ESMAP Technical Paper. Study on Investment and Private Sector Participation in Power Distribution in Latin America and the Caribbean Region.* Technical paper no. 089. Washington D.C.: International Bank for Reconstruction and Development, The World Bank. December 2005. Information on Honduras and Nicaragua drawn from Wikipedia, "Electricity sector in Honduras" and "Electricity sector in Nicaragua."

Bibliography

Goodman, Marc. *Future Crimes Everything Is Connected, Everyone Is Vulnerable and What We Can Do about It*. New York: Doubleday, 2015.

Harris, Shane. *@War: The Rise of the Military-Internet Complex.* New York: Houghton Miffin Harcourt, 2014.

Herz, Rafael, Jan Kappen, and Lucio Monari. *Study on Investment and Private Sector Participation in Power Distribution in Latin America and the Caribbean Region*. ESMAP Technical Paper no. 089. Washington D.C.: International Bank for Reconstruction and Development, The World Bank. December 2005.

Kaplan, Jerry. *Humans Need Not Apply.* New Haven and London: Yale University Press, 2015.

Koppel, Ted. *Lights Out: A Cyber Attack, a Nation Unprepared, Surviving the Aftermath.* New York: Crown Publishers, 2015.

Kupchan, Charles. *No One's World: The West, the Rising East, and the Coming Global Turn.* New York: Oxford University Press, 2012.

Naim, Moises. *The End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge Isn't What It Used To Be.* New York: Basic Books, 2013.

Powell, Andrew. *The Labyrinth: How Can Latin America and the Caribbean Navigate the Global Economy.* Latin American and Caribbean Macroeconomic Report, Report Inter-American Development Bank, March 2015.

Schmidt, Eric, and Jared Cohen. *The New Digital Age: Reshaping the Future of People, Nations and Business.* New York: Alfred A. Knopf, 2013.

Schneier, Bruce. *Data and Goliath: The Hidden Battle to Collect Your Data and Control Your World.* New York: W.W. Norton & Company, 2015.

Van Kranenburg, Rob, Dan Caprio, Erin Anzelmo, Alessandro Bassi, Sean Dodson, and Matt Ratto. *The Internet of Things*, Conference Draft. Alexander Von Humboldt Institut Fur Internet Und Gesellschaft. 2011.

William J. Perry Center
for Hemispheric Defense Studies
260 5th Avenue, Building 64
Abraham Lincoln Hall, Fort McNair
Washington, D.C. 20319-5066
chds.dodlive.mil