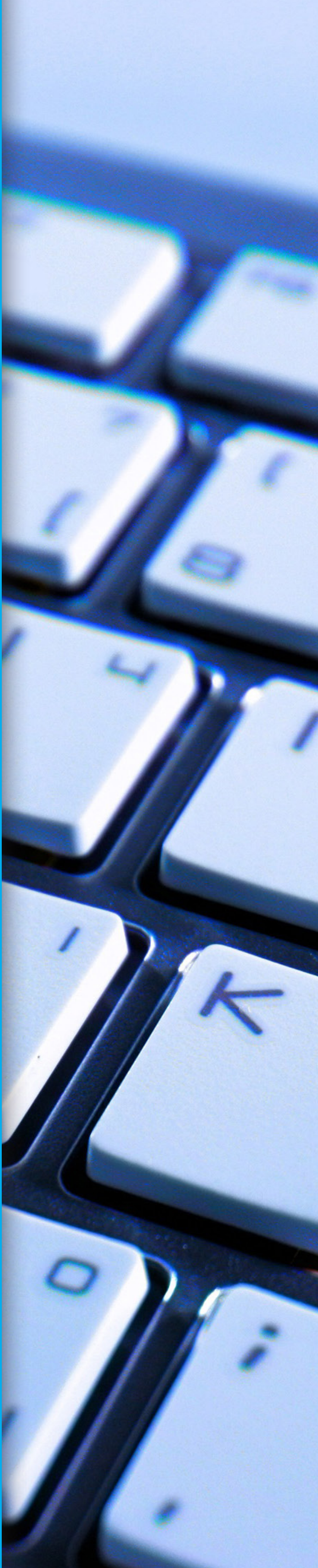
GLOBSEC
POLICY INSTITUTE

Good Neighbors Make Good Security: Coordinating EU Critical Infrastructure Protection Against Cyber Threats



www.globsec.org

GLOBSEC
POLICY INSTITUTE

Good Neighbors Make Good Security: Coordinating EU Critical Infrastructure Protection Against Cyber Threats

Philip Chertoff

www.globsec.org

Introduction

In October 2016, Meyer Werft Shipyard notified electricity provider, E.ON Netz, that the *Norwegian Pearl*, their newly-built cruise ship, would soon depart their factory and requested a disconnection of the Conneforde Diele 380 kV double line, so that the ship could pass upriver to the North Sea.[1] A mandatory procedure in cases where large ships, such as the *Pearl*, are set to approach electrical lines, E.ON Netz gave provisional approval to the *Pearl* for passage on November 5th.

At 9:38 PM, in anticipation of the *Pearl*'s arrival, E.ON Netz disconnected the Conneforde-Diele line. A minute later, the alarms went off. Transmission lines tripped both east and west of the disconnected lines and outages spread through Western Europe to Portugal and through Central Europe, all the way to the Balkans. Nearly half of Europe was shrouded in darkness. Most electricity was restored within two hours of the disconnection. During the outage, however, emergency services scrambled to rescue people left in vertical transportation, trains were massively delayed and electricity was cut off to some 15 million households. [2] The 2006 cascading failure was one of the worst in Europe's history.

In the days after the blackout, investigators learned that the shut-down of the Conneforde-Diele line had shifted load to a southern line which did not have the capacity to support it. After this connection was lost, load shifted to other lines without adequate capacity to carry the transmission of the two failed lines, tripping them and cascading the failure across the European continent. The major lesson which emerged from the 2006 blackout was that, because of the significant interdependence among the electricity transmitters of Europe, a small disruption could cascade into a massive failure. Less noted, however, is that the failure interrupted services beyond electricity transmitters. The failure of a single electricity transmission component impacted telecommunications, financial institutions, water transmission, and emergency services across the continent.

This paper will examine the current vulnerability of EU critical infrastructure to cascading failures caused by cyberattacks. It introduces the theory and implications of critical infrastructure interdependencies and explores past EU efforts to secure critical infrastructure from physical failures. Accounting for the damage and versatility cyberattacks on critical infrastructure, this paper suggests that the recently adopted "Directive on security of network and information systems" (NIS Directive), which aims to mitigate cyberthreats to critical infrastructure, will not be sufficient to handle the possible cross-industry and cross-border impacts of cyberattacks on critical infrastructure. The paper lays out several recommendations, inspired by North American efforts to manage cross-border critical infrastructure failures, which hope to encourage greater regional and inter-industry coordination on cyber defense and crisis management of critical infrastructure.

Critical Infrastructure and its Interdependencies

In the context of policy spheres and national protection strategies, 'infrastructure' refers to the networks of independent, man-made systems and processes that function collaboratively to provide a continuous flow of goods and services for the public.[3] Within infrastructure, there is a subset which can be identified as 'critical', referring to services deemed fundamental to the lives and operations of society and whose disruption could produce significant loss of life, financial cost, or physical damage. Different nations include different systems within their set of critical infrastructures, but most recognize energy, ICT, finance, healthcare, food, water, transport, and emergency services infrastructure as critical.[4] While certain states may still retain access over some critical infrastructure, the vast majority of critical infrastructure is privately-owned and maintained. Due to the essential nature of these services to the lives of citizens, however, states take an active role regulating private sector operators and require operators take steps to ensure continuity of service, both during normal circumstances and disruptive events.

[1] ERGEG "The Lessons to Be Learned from the Large Disturbance in the European Power System on the 4th of November 2006."

[2] BBC UK "BBC NEWS | Europe | Bid to Overhaul Europe Power Grid."

[3] Rinaldi et al. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." 12; Hämmerli et al. "Protecting Critical Infrastructure in the EU." 22

[4] Hämmerli et al. supra, at 23

Critical infrastructure does not operate in a vacuum and the continuity of their services is quite dependent on the proper operations of other infrastructure. The oil transmitter requires fuel for its generators, telecommunications for its systems, chemicals for its processing, etc. If one of these inputs fails, the critical infrastructure cannot optimally provide its own service. When these dependencies are bi-directional, meaning the services are mutually dependent on each other, these linkages are called *interdependencies*.[5] The telecom company, for example, is reliant on electricity to operate its transmitters, the electric utility is reliant on the signals from the telecom company to transmit electricity. These complex relationships mean that a disturbance in the normal operations of a critical infrastructure, even one component of a critical infrastructure, can impact other, even all other, critical infrastructure. In 1998, a computer failure aboard the Panamsat Galaxy IV telecommunications satellite shut down the transmission of television, radio, and data singles to organizations and businesses across the U.S.[6] Most significantly, it knocked out the pager systems for 90% of Americans who used pagers which, in the time before the widespread use of cellphones, was the most effective method for mobile contact. Television broadcasters were left without means to transmit programming, hospital administrators were unable to reach doctors away from their homes or offices, and credit card transactions were interrupted across the country. In 2005, a power failure, in the St. Gotthard region of Switzerland, shutdown the entire Swiss rail network for three hours, stranding 100,000 people.[7] A short circuit in a power line led to a diversion of current to southern power stations, creating an overload. The overload led to the complete shutdown of a nation-wide critical infrastructure and, in turn affected, disrupted the transportation of the goods and personnel, some of which support other critical infrastructure. The failure of a single component of critical infrastructure can transmit shocks and interrupt services across the interdependent critical infrastructure of a country.

However, the vulnerabilities of complex interdependence are not limited to national borders. Europe has long-standing history of interdependence among nation's critical infrastructure, reaching back to the early 20th century.[8] Since the 1990's, the continued integration of the EU Single Market, especially the continuing integration of the trans-European networks (TENs), has only increased these interdependencies which interlink the economies of EU members.[9] While numerous authors have written on the significance of European critical infrastructure interdependency, there is little publicly available data or analysis which scopes the size of this interdependency, itself indicative of a major gap on critical infrastructure risk management. There is, however, data available about incidence of critical infrastructure failure resulting from a dependency in another service. Since 2000, 501 of 1749 incidents of critical infrastructure failure were caused by infrastructure failures in other sectors.[10] Of those 501 incidents, 76 were the result of a second cascade, meaning that the failure in one service triggered a failure into a second service, which triggered a failure in a third. These incidents demonstrate that European interdependencies do stretch across multiple critical services and that shocks can ripple to first order, and even second order, connections. And while the damage of European cascading failures can be minimal, it can also be as significant as the massive disruptions of the Galaxy IV failure or St. Gotthard shutdown.

As the providers and regulators of critical services, business and political leaders have long been concerned about the continuity of critical services. The European Union was specifically spurred to action by the rise of the terrorist threat to critical infrastructure. In the aftermath of the 2004 al-Qaeda bombing of the Madrid train station, the European Commission adopted a set of suggestions for the enhancement of European preparedness, prevention, and response to terrorist attacks against critical infrastructure.[11] Since then, several EU initiatives have been established to provide for European-wide critical infrastructure protection (CIP), including:

[5] Rinaldi et al. supra, at 12

[6] Swanson and Kirk "Satellite Outage Felt By Millions."

[7] BBC UK "BBC NEWS | Europe | Swiss Rail Network Grinds to Halt"; "Short Circuit Paralysed Railway Network"

[8] See Van Der Vleuten et al. "Europe's System Builders: The Contested Shaping of Transnational Road, Electricity and Rail Networks."

[9] Hämmerli et al. supra, at 13

[10] Luiijf et al. "Empirical Findings on Critical Infrastructure Dependencies in Europe." 304

[11] European Commission Communication on a European Programme for Critical Infrastructure Protection, 2006 O.J. C 786 final

- European Programme for Critical Infrastructure Protection (EPCIP)
- European Public-Private Partnership for Resilience (EPPPR)
- European Public Forum for Member States (EFMS)

These efforts required the identification and designation of MS national critical infrastructure, supported the development of a number of infrastructure warning systems, and established a series of best practices on protecting critical infrastructure.[12] Spurred as it was by a terrorist attack, however, the vast majority of critical infrastructure efforts mentioned have been concerned with physical threats to critical infrastructure, including terrorism, environmental hazard, user error, etc. The EPCIP has not been as concerned or delivered as notable advancements in the field of defending critical infrastructure against cyber threats.

The Cyber Threat to Critical Infrastructure

Since the beginning of the new millennium, the operation of critical infrastructure has been increasingly controlled by ICS (Industrial Control Systems) and managed by operators through SCADA (Supervisory Control Authority and Data Acquisition) systems. Using these systems, made up of hundreds of sensors and programmable controls, a few operators are able to control the operational flows of massive infrastructure, effect infrastructure processes from long distances, and share infrastructure information with relevant authorities and connected actors. While the efficiency gain may be great, the digitalization of critical infrastructure has also created opened it up to significant new threats. The incredible efficiency of this digital enablement has in turn created a reliance on the proper and accurate functioning of these underlying digital systems to maintain the standard operations of critical infrastructure. ICS' positions as the interlocutors between physical and cyber systems makes them the channel for web-based actors to influence or affect physical systems.[13] By manipulating the logic controllers operating the mechanized or wired infrastructure, external threat actors can damage or destroy the physical components of critical infrastructure. In the infamous *Aurora* test, the U.S. Department of Homeland Security hacked a replica of a power plant's control system and caused a power generator to self-destruct.[14] Actors ranging from lone mischief makers to state actors have all been empowered by the proliferation of system exploits to launch web-based attacks against physical infrastructure. Numerous authorities have described the extent of the vulnerability of ICS systems and the frequency of their exploitation by threat actors.[15] Our providers of essential services, which our societies rely upon for normal operations, are vulnerable to data theft, data manipulation, malicious software installation, and destruction.

Large-scale incidents of cyberattacks, which cause disruptions to critical services, have not been frequent but they have had significant impact. In 2012, the Shamoon virus wiped the data disks of Saudi Aramco, requiring the shutdown of its internal network.[16] More recently, in December 2016, the Russian hacking group Sandworm, cut power to 80,000 customers in Western Ukraine for six hours.[17] In this attack, hackers leveraged a massive phishing campaign to gain access to the systems of many government organizations and performed reconnaissance for months until they could escalate their

[12] Directorate-General for Energy – European Commission "Protection of Critical Infrastructure - Energy - European Commission."

[13] While the use of ICS and SCADA systems do not necessarily require connection to the Internet, the majority are connected to enable information-sharing and maintain the digital infrastructure. While some argue operators could mitigate cyberattacks by disconnecting systems from the web, called an 'air gap', there will always be some necessary connections to the web which attackers can compromise to gain network access (including file exchanges, program patches, personal devices, etc.). Perelman, Barak. "Air Gap or Not, Why ICS/SCADA Networks Are at Risk | SecurityWeek.Com."

[14] Swearingen et al. "What You Need to Know (and Don't) About the AURORA Vulnerability."

[15] See Hathaway and Stewart "Cyber IV Feature: Taking Control of Our Cyber Future"; Bronk "Two Securities: How Contemporary Cyber Geopolitics Impacts Critical Infrastructure Protection."; Etzioni "The Private Sector: A Reluctant Partner in Cybersecurity."; Onyeji et al. "Cyber Security and Critical Energy Infrastructure."

[16] El Dahan "Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces."

[17] Zetter "The Ukrainian Power Grid Was Hacked Again."

access to administrative privileges. When they finally wanted to disrupt energy services, they shut down the remote-terminal units that control substation breakers, preventing technicians from using the SCADA system to restore power remotely. The capabilities demonstrated in the Ukraine attack are not uniquely threatening to the Ukraine, Western systems are just as vulnerable. As one of the attack investigators commented, "Ukraine uses equipment and security protections of the same vendors as everybody else around the world. If attackers learn how to go around these tools and appliances in Ukrainian infrastructures, they can then go directly to the West. "[18] While Union members have not suffered as significant an attack as these, the capacity of actors to leverage these techniques makes them a reasonable security threat.

It important to recognize that this digitalization is not just an additional interdependency between critical infrastructure but rather an additional layer of interdependencies, which open infrastructure up to a whole new set of disruptions. Within the standard physical dependency, the shutdown of electricity infrastructure might disrupt health services or the transmission of oil. But leveraging the cyber modality, a threat actor could alter the flow of electricity, create overcapacities in certain areas and undercapacities in others. It could selectively target oil transmitters, while leaving health services unscathed. Beyond the simple failure of a component causing a sub-optimal or failure of a critical service, threat actors can manipulate interdependences to achieve a whole spectrum of outcomes. In a previous instance, Sandworm disrupted the Ukrainian energy grid by wiping the data of grid computers, effectively crippling operator ability to restore breakers to operation. As mentioned, in the 2017 case, they just shut-off breakers, allowing technicians to turn them back on once they restored control over the SCADA system. The spectrum of activities that threat actors can use to affect the operations of critical infrastructure is limited only by their will, access, and knowledge of the targeted system.

In recent memory, the most significant cascading failure, due to a cyberattack, was the 2016 DDos attack on Dyn, a Domain Name System (DNS) provider. Leveraging a massive botnet composed of Internet-connected devices, the still unknown attacker launched tens of millions of DNS lookup requests, with an estimate throughput of 1.2 terabits per second, which disrupted the ability of Dyn to provide DNS lookup requests for its customers.[19] Without DNS lookup, legitimate users were prevented from connecting to the host of their desired web services.[20] During the Dyn attacks, users were cut off services such as Paypal, Shopify, and Amazon. Viewed through the critical infrastructure interdependence model, the disruption of one critical infrastructure, a DNS lookup service, cascaded into financial services and ecommerce infrastructure and interrupted the critical services for citizens and their businesses, to significant financial cost.[21]

What Next After NIS

The most significant step by the EU to combat cyberattacks against critical infrastructure has been the recently adopted NIS directive. Adopted in 2016, member states are directed to designate operators of essential services and establish security and notification requirements to establish a high level of security for critical infrastructure. [22] The security requirements include technical and organizational measures proportional to operator risk, network and information system security measures proportional to risk, and incident management to minimize risk to IT systems. Operators will be required to report serious incidents to their designated national authority and the severity of incidents will be evaluated based on number of users affected, duration of incident, and geographic spread, with

[18] Ibid.

[19] Murgia and Kuchler "Cyber Attack Hits Hundreds of Websites."

[20] DNS, or Domain Name System, refers to the decentralized system linking entered domain names (ex. www.google.com) with the IP address which identifies the servers hosting desired content (ex. 213.81.154.222). As the IP addresses of associated with domain names must frequently change, dynamic DNS services manage requests to lookup the IP for a specific DNS. If a DNS service supporting a website is disrupted, the only method for users to connect to that website is to directly enter the website's IP address (which, unless it is static, is constantly subject to change).

[21] LaFrance "How Much Will Today's Internet Outage Cost?"

[22] Parliament and Council Directive 2016/1148 194/2

digital service providers also evaluated on the extent of service disruption and impact on economic and societal operations. Each state will have a national point of contact to liaise among Member states and Computer Security Incident Response Team (CSIRT) to operate as the reporting and incident response authority for service disruptions by essential operators. The directive also provides for the establishment of a "Cooperation Group" to "support and facilitate *strategic* cooperation between the Member states regarding the security of network and information systems".

While the NIS directive is an important step to raising the overall level of cybersecurity throughout the EU, it treats requirements more as establishing market standards or consumer protections within each of the member states, rather than treating attacks against critical infrastructure as public security needs or crisis situations. The directive attempts to add greater force and pressure on essential operators in all member states to mitigate long-standing security concerns and to provide prompt information-sharing to relevant authorities when incidents do occur. Cooperation and coordination among member states appears to be on a loose, voluntary basis. The establishment of a CSIRT network only retreads longer-standing networks, including the international network FIRST, regional networks like the Central European Cyber Security Platform, and informal working relationships among the national CSIRTS, without offering any additional value or requirements to suggest it will be any more effective. The networks efforts also seem focused primarily on the sharing of information on incidents within their borders.[23] As for the Cooperation Group, it may yet prove to be a valuable venue to discuss further cybersecurity reforms for the EU but at the moment the Directive itself recognizes that, for it to be effective, member states must first meet the 'minimum' capabilities for a 'high' level of security. Even if that is completed by May 2018, the deadline for Member States to transmit the principles of NIS into national law, the Cooperation Group, by definition, seems to have no specific aims or authority, only some kind of platform for vague dialogue. The NIS directive should help improve security standards of the EU, especially in those states where it has been less of a priority on the national agenda. It does not offer, however, any significant action on coordination, mutual capacity-building of critical information protection or other security issues, beyond basic information-sharing.

Further, the NIS directive, while recognizing that threats to critical infrastructure pose a significant danger to the safety and security of member state citizens, treats incident response to cyber threats as an effort which only needs to take place on the cyber-plane. However, the very reason that critical infrastructure is identified as such a priority is because critical infrastructure operates at the intersection of the cyber and physical domains and attacks on network infrastructure can produce physical effects. In the event of a cyberattack on a critical infrastructure, responders may not only need to mitigate the threat to the critical infrastructure network but also the possibly resulting threat to the physical components as well. The NIS Directive makes no obvious recognition of the fact that incident response to cyberattacks on critical infrastructure must be a coordinated effort of technical and physical solutions. The reality is that in the best-case scenario, in the event of a cyberattack on critical infrastructure, there will be two, uncoordinated responses to the situation—an attack mitigation response by the national CSIRT and a crisis management reaction by the industry regulators and/or civil protection agencies.

Threat actors also have significantly greater abilities to damage critical infrastructure using a cyber modality. The addition of the digital layer to critical infrastructure has only increased the interdependencies and the sensitivity of European critical infrastructure to shocks from disruptions. This has generated a number of avenues for cyberattacks to take advantage of the interdependence of critical infrastructure in the EU. The first, operating similarly to physical disruptions of critical infrastructure, is the shut down or interruption of a critical infrastructure operations. The failure in this critical infrastructure can then trigger further disruption in other pieces of critical infrastructure. The second takes advantage of the omnipotent ability of a cyberattack to target multiple locations at the same time. Considering that critical infrastructure leverage many of the same types of equipment and security measure, a motivated attacker may be able to disrupt multiple critical infrastructure at the same time, greatly increasing the size, duration, and impact of a disruption to critical services.

[23] Since 1990, FIRST has connected security and incident response teams from government, business, and academic sectors, all around the world, to share best practices and exchange vulnerability information. https://www.first.org/about

The third, slightly more subtly, would consist of the attacker manipulating the data inputs and outputs of critical infrastructure in order to strain the operations and decrease the operating capabilities of critical infrastructure. While this would not cause a significant disruption, this more indirect manipulation can have political, economic, or social impacts without revealing the access of attackers to the target network. Regardless of the technique used, the cyber dimension of critical infrastructure offers attackers the capability to dramatically increase the flexibility, damage, and scope of their attacks, with likely far greater ability to disrupt further interdependent critical infrastructure. These disruptions could spread to other pieces of critical infrastructure in their own industry, other pieces of critical infrastructure in different industries, and even infrastructure across borders. Unfortunately, the relative novelty of this problem means that there are few actors that have come up with mature solutions and protection of critical infrastructure. European critical infrastructures' unique situation as a highly interdependent region also affords an additional practical wrinkle. However, there have been some policy efforts between the U.S. and Canada which can offer some inspiration for institutions and capabilities that would provide greater coordination and capacity for response to cyber-attacks against critical infrastructure.

The North American Approach

In the late 1990's, the specter of the Y2K bug prompted a massive effort by governments, corporations, and intergovernmental organizations to plan for possible failures of critical infrastructure and interruptions of critical services.[24] Y2K contingency planning was one of the first instances where businesses and government agencies began to consider the possibility of failures transmitting through interdependencies, causing failures in the same sector, different sectors, and across borders.[25] While there was a lot of effort globally, driven by the UN and World Bank, the U.S. and Canada, as neighbors with cross-border infrastructure, independently established joint steering committees and public-private working groups to mitigate the possible cross-border threats of the Y2K bug. In the aftermath of Y2K, this collaboration between the U.S. and Canada continued with the *Joint Framework for Canada- United States Cooperation on Critical Infrastructure Protection*, which established the first working groups to "address horizontal issues such as research and development, interdependencies, mapping and threat information-sharing".[26] The efforts of these groups have been sustained in several subsequent initiatives including the *Canada-United States Action Plan for Critical Infrastructure* (CUSCI), *Beyond the Border Action Plan* (BTBAP), and the *Cybersecurity Action Plan* issued in 2010, 2011, and 2012 respectively.

CUSCI, BTBAP, and the Cybersecurity Action Plan continue previous work and make a number of recommendations for managing possible critical infrastructure failures, ranging from local to national efforts, including:

- setting up a cross-border framework for emergency management issues
- forming U.S.-Canadian government and private sector councils to develop mechanisms for cross-border collaboration
- creating virtual critical infrastructure risk analysis cells to produce shared infrastructure risk analysis, vulnerability assessments, and prioritization methodologies
- establishing compatible mechanisms and protocols for information-sharing, respectful of U.S. and Canadian legal and regulatory environments
- developing coordinated information dissemination procedures and communication systems in the case of disruptions.

[24] The Y2K bug, or the millennium bug, was a computer bug based on an assumption in 20th century software which represented the year with the final two digits, failing to distinguish a 20th century year from a 21st century year. This assumption was predicted to cause numerous errors, ranging from incorrect date recording to failures of date-related processing. Organizations worldwide remediated the bug and very few Y2K-related computer failures were reported on January 1, 2000.

[25] Laat "Beyond the Border Action Plan: A Tool for Enhanced Canada-U.S. Cooperation on Critical Infrastructure and Cyber Security - Or More Window Dressing." 455

[26] Department of Homeland Security "Canada-United States Action Plan for Critical Infrastructure"

- assessing regional plans for shared critical infrastructure risk, starting with the Maine-New Brunswick border region
- holding joint briefings with relevant private sector and stakeholders

The great benefit of the efforts outlined in these cross-border approaches is their prioritized-hazard and bi-lateral approach. Rather than only building out prevention mechanisms, these approaches recognize the likelihood that events will occur and plan for the most likely scenarios to emerge. The programs recognize that disruptions in critical infrastructure can spur effects and specifically attempts to model and develop responses to the most likely situations to emerge. The bi-lateral arrangement of these efforts provides for effective decision-making and specific solutions. By organizing small, focused groups which tackle particular scenarios and threat issues, these strategies encourage stronger working relationships and greater predictability (meaning that in the case of an incident, responsible parties have a better sense for how their counterparts will react). The continuing and expanded bilateral efforts under the auspices of the program appear to demonstrate its success.[27] The bi-lateral engagement between the U.S. and Canada has progressed on a good pace without significant slowdowns, a characteristic which can sometimes hamper the collaborative efforts of multi-stakeholder or hierarchical processes. Some may argue that after years of effort, the levels of coordination and resulting products may appear meagre. However, it is important to recognize that the U.S. and Canada's level of interdependence is far looser and more localized than that of Europe. For example, in the electricity sector, for 2012, electricity exports from Canada to the United States constituted just 1-2% of U.S. nationwide consumption.[28] That consumption is also highly localized to border areas in New England and the Midwest. Accordingly, most efforts on cross-border critical infrastructure protection are focused at the regional level. For the EU member states, with much higher levels of interdependence among their critical infrastructure and their neighbor's critical infrastructure, such programs are far more needed and provide far more utility.

Recommendations

Considering the scope and complexity of interdependencies among critical infrastructure in the EU, and the vulnerabilities available from cyber infrastructure, the EU should take steps to build out institutions and processes for preventing and responding to cascading and cross-border critical infrastructure disruptions due to cyberattacks. The previous policies of the U.S. and Canada to coordinate protection efforts can provide valuable inspiration. In a different tact from current strategies which assign protection responsibility to EU organs, a number of these recommendations focus on possible efforts between bordering states and thus require bi-lateral or regional critical infrastructure protection strategies. Institutions, policies and agreements which would support this effort include:

- **Formation of a critical infrastructure attack management consultative group**: As it stands now, ENISA is in the position of advising on the implementation and development of all national cybersecurity strategies, advising and validating the identification and individual protection of critical infrastructure, as well as supporting a whole host of other European cybersecurity activities. As an institution, ENISA is also most pointedly focused on cybersecurity incident management and not on resulting damage or disruption to the physical infrastructure. The creation of a Cyber Attack Management Consultative Group, including members of both ENISA and the individual critical infrastructure protection authorities in MS (like the Ministry of Interior in Germany), would provide an authority which can share best practices and advise on the development of cyber incident and service continuity response plans, which plan for both cyberattack mitigation process and crisis management of the physical infrastructure disruption.
- **Collaborate on cross-national, sector-specific response planning**: As the infrastructure threats and security measures vary by industries, member states should urge their national sector-specific protection agencies/regulatory authorities to organize bi-national or regional cyberattack

[27] Public Safety Canada "Canada-United States Beyond the Border Action Plan Implementation Report."; Public Safety Canada "2015 Beyond the Border Implementation Report."

[28] Energy and Commerce Committee "North American Energy Infrastructure Act Will Bolster U.S.–Canada Electricity Relationship."

response mechanisms and joint attack response exercises—preferably in forums which engage the private sector operators on both sides of the border. These collaboratives should prioritize the establishment of compatible mechanisms and protocols for information-sharing, setting achievable goals for states to align data sharing with their interdependent industries and neighboring state collaboratives. They would also help develop more specific processes and procedures for responding to attacks on individual industries' critical infrastructure and cultivate the working relationship between their security operators.

- **Creation of virtual risk analysis cells**: One of the central principles of emergency management is a commitment to 'all-hazards' planning, which some interpret to mean planning for any and all possible eventualities of emergencies. Virtual risk analysis cells instead prioritize and provide risk assessments of the most likely critical service disruption scenarios which could occur. Virtual risk analysis cells both among interdependent national critical infrastructure and between bordering member states could help develop infrastructure risk analyses, vulnerability assessments and prioritization methodologies in cases of cross-border infrastructure impact. In crisis scenarios, predictability and practiced response are often key requirements for mitigating damage, so standard protocols would help reduce delay to response time. By jointly developing information dissemination procedures and engaging in joint incident responses, bordering states are more likely to be prepared for cascading and cross-border critical infrastructure disruptions.
- **Construction of a European critical infrastructure protection test bed**: Last year, the U.S. National Renewable Energy Laboratory's Cyber Physical Systems Security and Resilience Center launched the Test Bed For Secure Distributed Grid Management. This system uses all the hardware and software that are required for controlling and energy distribution system to recreate the communications, power systems, and cybersecurity of a utility power distribution system.[29] The NREL researchers are then able implement different security products and attempt to hack the system, providing valuable insights into the vulnerabilities of infrastructure security products and security strategies. The EU should establish its own European Test Bed, or several national Test Beds, both to test the cybersecurity strategies of various critical operators, the cross-sectoral impact of critical infrastructure attacks, and the protection measures of cross-border critical infrastructure. These Test Beds would be extremely valuable for testing the security strategies of essential service operators, confirming that they meet a high degree of security and even providing enough data to set defined, technical standards on EU-wide operators. They would also help provide a venue for testing the inter-industry and cross-border critical infrastructure protection strategies and coordinated incident response strategies and capabilities. The data would all be extremely helpful for crafting realistic and data-driven risk assessments and response mechanisms.

While the prospect of cross-sectoral and cross-border impacts from cyberattacks on critical infrastructure may appear far beyond the current threat landscape of the EU, it should not take the damage of a crisis like the 2006 Blackout or 2004 Madrid bombing to prompt a response from European leaders. Taking steps now can help to prevent a costly and frightening future disaster. The benefit of the institutions and capabilities offered in these recommendations is that they do not only offer a defense against disaster and cascade scenarios. They also build up the individual defensive capabilities, knowledge basis, and experience of the operators and government representatives of all EU member states, both to defend against less sophisticated attacks on their national critical infrastructure and offer procedures to assist their neighbors in case they fall prey to such threats. While the NIS Directive hopes to encourage member states and their operators to develop their defense capabilities individually, these supplementary recommendations try to push member states to develop their capabilities together, for the protection of all, interdependent, EU critical infrastructure.

Philip Chertoff is Research Fellow at the GLOBSEC Policy Institute

[29] Eber "NREL's Cybersecurity Initiative Aims to Wall Off the Smart Grid from Hackers - News Feature | NREL."

Bibliography

BBC UK "BBC NEWS | Europe | Bid to Overhaul Europe Power Grid." Accessed May 19, 2017. http://news.bbc.co.uk/2/hi/europe/6117880.stm.

BBC UK "BBC NEWS | Europe | Swiss Rail Network Grinds to Halt." Accessed May 19, 2017. http://news.bbc.co.uk/2/hi/europe/4121072.stm.

Bronk, Chris. "Two Securities: How Contemporary Cyber Geopolitics Impacts Critical Infrastructure Protection." International Journal of Critical Infrastructure Protection 8 (January 2015): 24–26.

Department of Homeland Security. "Canada-United States Action Plan for Critical Infrastructure," 2010. https://www.dhs.gov/sites/default/files/publications/ip-canada-us-action-plan-2010-508.pdf.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016 O.J. L 194/2 [hereinafter NIS Directive]

Eber, Kevin. "NREL's Cybersecurity Initiative Aims to Wall Off the Smart Grid from Hackers - News Feature | NREL." NREL, January 4, 2016. http://www.nrel.gov/news/features/2016/21612.

El Dahan, Maha. "Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces." Reuters, January 23, 2017. http://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR.

ERGEG. "The Lessons to Be Learned from the Large Disturbance in the European Power System on the 4th of November 2006." Council of European Energy Regulators ASBL, February 6, 2007. http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_PAPERS/Electricity/2007/E06-BAG-01-06_Blackout-FinalReport_2007-02-06.pdf.

Etzioni, Amitai. "The Private Sector: A Reluctant Partner in Cybersecurity." Georgetown Journal of International Affairs, 2014, 69–78.

European Commission Communication on a European Programme for Critical Infrastructure Protection, 2006 O.J. C 786 final [hereinafter ECPIP Communication]

Hämmerli, Bernhard M, Andrea Renda, and Centre for European Policy Studies. "Protecting Critical Infrastructure in the EU." Brussels: Centre for European Policy Studies, 2010. https://www.ceps.eu/system/files/book/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf.

Hathaway, Melissa, and John Stewart. "Cyber IV Feature: Taking Control of Our Cyber Future I," July 25, 2014. http://journal.georgetown.edu/cyber-iv-feature-taking-control-of-our-cyber-future/.

Laat, William de. "Beyond the Border Action Plan: A Tool for Enhanced Canada-U.S. Cooperation on Critical Infrastructure and Cyber Security - Or More Window Dressing." Canada-United States Law Journal 37, no. 2 (January 1, 2012): 451.

LaFrance, Adrienne. "How Much Will Today's Internet Outage Cost?" The Atlantic, October 21, 2016. https://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/.

Luiijf, Eric, Albert Nieuwenhuijs, Marieke Klaver, Michel van Eeten, and Edite Cruz. "Empirical Findings on Critical Infrastructure Dependencies in Europe." In Critical Information Infrastructure Security, edited by Roberto Setola and Stefan Geretshuber, 5508:302–10. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. doi:10.1007/978-3-642-03552-4_28.

Murgia, Madhumita, and Hannah Kuchler. "Cyber Attack Hits Hundreds of Websites." Financial Times, October 21, 2016. https://www.ft.com/content/08ca940e-97a1-11e6-a1dc-bdf38d484582+&cd=1&hl=en&ct=clnk&gl=us.

"North American Energy Infrastructure Act Will Bolster U.S.–Canada Electricity Relationship." Energy and Commerce Committee, May 7, 2014. https://energycommerce.house.gov/news-center/press-releases/north-american-energy-infrastructure-act-will-bolster-us-canada.

Onyeji, Ijeoma, Morgan Bazilian, and Chris Bronk. “Cyber Security and Critical Energy Infrastructure.” The Electricity Journal 27, no. 2 (March 2014): 52–60. doi:10.1016/j.tej.2014.01.011.

Perelman, Barak. “Air Gap or Not, Why ICS/SCADA Networks Are at Risk | SecurityWeek.Com.” SecurityWeek, August 9, 2017. http://www.securityweek.com/air-gap-or-not-why-icsscada-networks-are-risk.

Public Safety Canada. “2015 Beyond the Border Implementation Report,” September 29, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-bynd-brdr-mplmntn/index-en.aspx.

———. “Canada-United States Beyond the Border Action Plan Implementation Report,” December 2013. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-2013-bynd-brdr-mplmntn/archive-2013-bynd-brdr-mplmntn-en.pdf.

Directorate-General for Energy – European Commission “Protection of Critical Infrastructure - Energy - European Commission.” Energy. Accessed May 22, 2017. https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure.

Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly. “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies.” IEEE Control Systems Magazine 21, no. 6 (December 2001): 11–25. doi:10.1109/37.969131.

“Short Circuit Paralysed Railway Network.” SWI Swissinfo.ch. Accessed May 19, 2017. https://www.swissinfo.ch/eng/short-circuit-paralysed-railway-network/4579658.

Swanson, Steven, and Jim Kirk. “Satellite Outage Felt By Millions.” Tribunedigital-Chicagotribune. Accessed May 19, 2017. http://articles.chicagotribune.com/1998-05-21/news/9805210138_1_galaxy-iv-satellite-outage-pager-customers.

Swearingen, 09/01/2013 | Michael, Steven Brunasso, Joe Weiss, and Dennis Huber. “What You Need to Know (and Don’t) About the AURORA Vulnerability.” POWER Magazine, September 1, 2013. http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/.

Van Der Vleuten, Erik, Irene Anastasiadou, Vincent Lagendijk, and Frank Schipper. “Europe’s System Builders: The Contested Shaping of Transnational Road, Electricity and Rail Networks.” Contemporary European History 16, no. 03 (August 2007): 321. doi:10.1017/S0960777307003967.

Zetter, Kim. “The Ukrainian Power Grid Was Hacked Again.” Motherboard. Accessed May 19, 2017. https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report.

GLOBSEC
POLICY INSTITUTE

Klariská 14
811 03 Bratislava
Slovak Republic
Phone/Fax: +421 2 5441 06 09
info@globsec.org

www.globsec.org