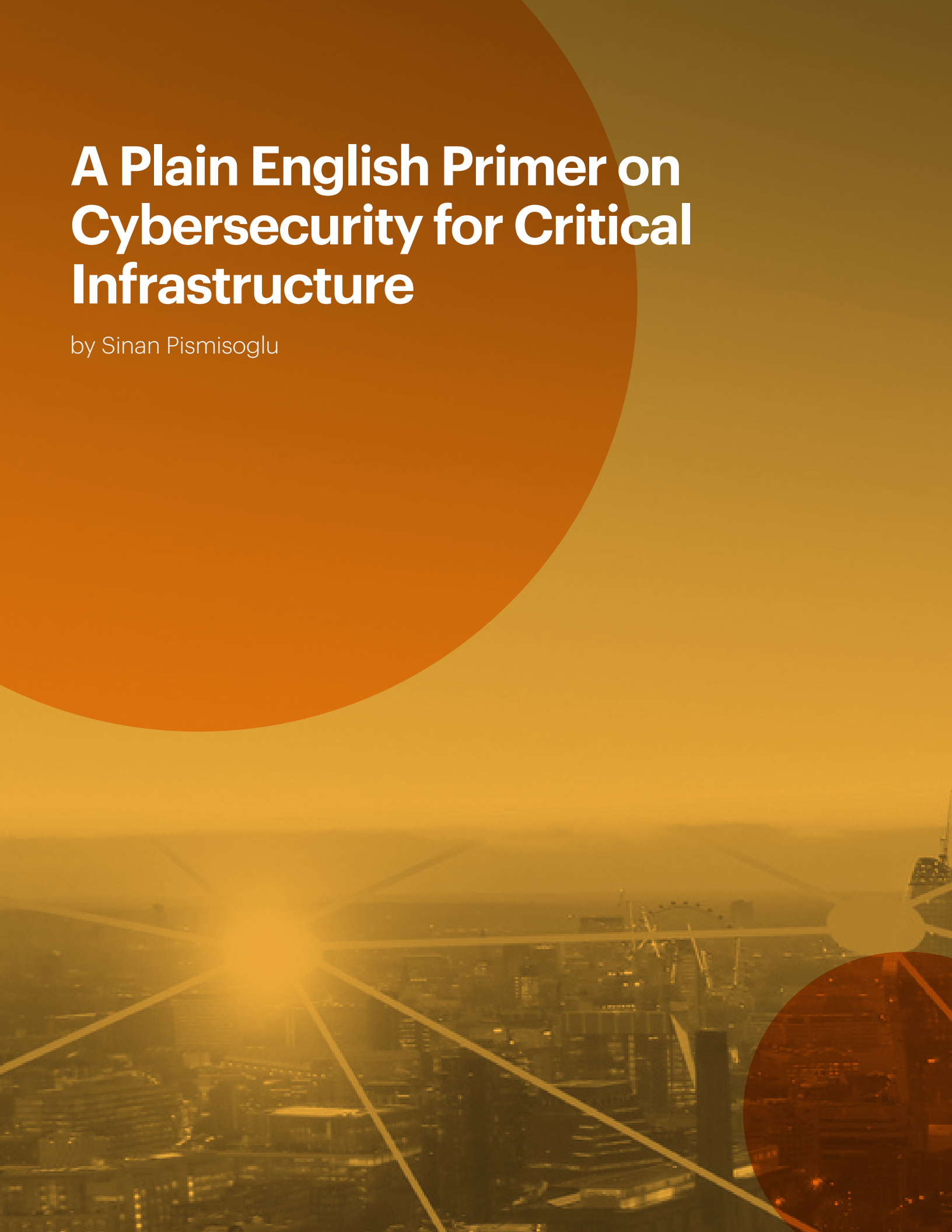
A Plain English Primer on Cybersecurity for Critical Infrastructure

by Sinan Pismisoglu



THE SMART CITY, CRITICAL INFRASTRUCTURE AND CYBERSECURITY

A Smart City's intelligence stems from the analytics performed on the data created by the Internet of Things (IoT) connected to networks throughout the city. In the absence of interconnectedness, a city's intelligence is dramatically reduced, but what level of interconnectedness is acceptable from a cybersecurity stand? Can critical infrastructure be both interconnected and safe? What will happen if the algorithms running the smart grid are compromised? Can a threat actor hack into a network on the smart grid to access or disrupt other, presumably distinct, operations of that critical infrastructure, and if so, how can we protect against this?

WHY IS OUR CRITICAL INFRASTRUCTURE SO CRITICAL?

The Cybersecurity and Infrastructure Security Agency[1], which is a subdivision of the Department of Homeland Security (DHS), designates the infrastructure sectors that are vital to the United States' public-safety as "critical." Sixteen designated critical infrastructure sectors are operating the nation's critical systems, and they all need to be secure, functioning, and resilient. A typical city hosts facilities and structures comprising many, if not most, of the 16 critical infrastructures: hospitals, transportation, energy, chemicals, dams, emergency services, government facilities, water and wastewater systems, among others.

INDUSTRIAL CONTROL SYSTEM(S) (ICS)

Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC) are different versions of ICS[2]. ICS are used to operate critical infrastructure for electricity generation and distribution, water and wastewater systems, oil and natural gas production and transportation, transportation systems, chemical plants, pharmaceutical manufacturers and developers, pulp and paper production, food and beverage production and processing, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). What makes ICS "critical" is that unlike conventional IT systems (e-mail, document processing, payment systems, online shopping), operations controlled by ICS directly affects the physical world. Compromise of ICS may risk the health and safety of human lives (think nuclear leakage at an energy plant or failure of life-support units at hospitals), may cause serious damage to the environment (such as floods from a dam),

1 https://www.cisa.gov/infrastructure-security
2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

and may have devastating effects on the nation's economy (for example economic depression due to interruptions in manufacturing and production)[3].

THE VULNERABILITY OF CONNECTED ICS

In the 1960s, before the interconnectedness era, cybersecurity was not of primary concern when designing ICS. They were designed to work in a stand-alone manner, and their security relied on air-gapped networks and proprietary protocols for securing the system.

The industrial use of IoT in combination with cloud computing and network connectivity forced an accelerated evolution of ICS, mixing the inflexible, static and centralized architecture of SCADA with seemingly unlimited options under IoT connectivity[4]. Today, SCADA systems connected to IoT are distributed, networked, and dependent on open protocols for the internet, which make them vulnerable to unauthorized access, and cyber-terrorism[5].

THE IOT BACKBONE OF A SMART CITY IS ITS GREATEST STRENGTH BUT ALSO ITS GREATEST VULNERABILITY

IoT is the backbone of a smart city. IoT is a set of electronic and photonic devices (sensors, actuators, cameras, processors, smart cars, smart refrigerators, smart aquariums, smartphones, smart meters, smart grid, eHealth devices, and so forth) that communicate over the internet wirelessly without human intervention[6]. The forecast is that IoT device shipments will reach 10 billion units in 2022[7].

The IoT is the central technology for a smart city. IoT contributes to the three key aspects of a city's intelligence: smart mobility (transportation systems, traffic and parking management, and so forth); smart sustainability (waste management systems and street lighting equipped with sensor technology to optimize usage and monitor conditions); and smart living (e.g., advanced location-based services and CCTV technologies to notify responders and the family members of emergencies involving children, the disabled, or the elderly)[8].

Integrating network sensors is another step towards progress within a smart city. IoT creates big data that is processed to extract useful information through real-time analysis and computing to manage smart city operations and to fine-tune the provision of services. The smart city can use the IoT data to analyze the condition of infrastructure to reduce the maintenance costs and failures and to extract useful information to optimize city operations. The efficiency of IoT data increases through the unification of data from multiple resources and real-time analyses of reliable data through uncorrupted algorithms[9].

Processing of IoT data also enables the smart city to discover, locate, and treat anomalies occurring in urban environments. IoT is the backbone of a smart city but also its greatest vulnerability[10].

IOT-CONNECTED SCADA SYSTEMS

With the evolution of IoT into industrial systems, SCADA systems have adopted IoT, cloud technology, big data analytics, artificial intelligence (AI), and machine learning. The integration of these technologies has created a real-time environment. Industrial use of

---

3 file:///Users/spismisoglu/Downloads/the-potential-human-cost-of-cyber-operations.pdf
4 https://doi.org/10.1002/spe.2688
5 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7445139
6 http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf
7 McClellan, S. & Jimenez, A & Koutitas, G. (2018). Smart Cities: Applications, Technologies, Standards, and Driving Factors. Springer.
8 Ejaz, W., & Anpalagan, A. (2019). Internet of things for smart cities. Springer.
9 Rathore, Muhammad Mazhar & Paul, Anand & Hong, Won-Hwa & Seo, HyunCheol & Awan, Imtiaz & Saeed, Sharjil. (2017). Exploiting IoT and Big Data Analytics: Defining Smart Digital City using Real-Time Urban Data. Sustainable Cities and Society. 40. 10.1016/j.scs.2017.12.022.
10 M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali and M. Guizani, A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security, in IEEE Communications Surveys & Tutorials, doi: 10.1109/COMST.2020.2988293.

IoT and cloud computing is revolutionary in smart industrial sectors that provide enhanced automation and information sharing facilities, combining cloud computing, cyber systems, and connectivity.

Today's "fourth generation" SCADA system utilizes the commercial cloud-computing services through the integration of IoT technology into the inflexible and static SCADA design. IoT-enabled SCADA systems are easy to maintain and integrate data accessibility, cost efficiency, flexibility, optimization, availability, and scalability. Among other advantages, IoT data allows prediction of failure cases using interconnected network devices and can efficiently operate in geographically inaccessible areas.[11]

The cybersecurity risk associated with the IoT integrated SCADA systems arises from the use of old inflexible and static SCADA systems on the interoperable IoT networks without employing new cybersecurity strategies that can mitigate the risks on such tremendously large attack surface created by the IoT network[12]. In the digital universe, the term "attack surface" refers to the physical and digital vulnerabilities running on a network that covers all the running software and the devices operating on the network. In brief, each IoT device is a separate entity and will typically possess an attack surface of its own.[13]

With this description in mind, one can imagine the level of vulnerability of a static system being connected to the IoT network comprised of tens of thousands of connected devices: smart meters, light sensors, algorithms, cloud computing, a host of hardware and software devices (i.e., desktop computers, laptops, routers, wireless networks connected to the business network of the ICS operator).

When SCADA systems are integrated into the cloud, they are exposed to the same risks as typical cloud infrastructure. For instance, the ownership privileges of the SCADA systems organization are transferred to the control of the Cloud Service Provider, or an attacker can easily gain access to IP addresses, usernames, and other private credentials when authentication and encryption techniques are weak.[14]

Moreover, because each network connection is an attack surface, the network connections between SCADA systems and the cloud may be exploited and used as backdoors to attack ICS. Overall, the ICS commands and information for the critical infrastructure can be modified, sniffed, lost, or spoofed during communication because the reliance on cloud communication makes the SCADA systems more open.[15]

Expert scientists are working on developing and perfecting responsive intrusion detection systems (IDS), which can alert the system managers about the possible attack on the system and network. These detection systems use a signature, specification, behavior, or machine learning-based models for enhanced security.[16]

Even under the protection of ICS systems supported by AI and machine learning, several attacks on the SCADA systems have been reported. AI and machine learning have not reached the level of advancement to stop advanced persistent threats (APT) attacking a network by exploiting a vulnerability not yet known to the programmer of the software or the operating system (zero-day attacks). APT attacks differ from other kinds of attacks due to extreme sophistication in their design.

---

11 Yadav, Geeta & Paul, Kolin. (2020). Architecture and Security of SCADA Systems: A Review.

12 Anam Sajid, Haider Abbas, and Kashif Saleem. (2016) Cloud-assisted IoT based SCADA systems security : A review of the state of the art and future challenges. IEEE Special Section on The Plethora Of Research In Internet of Things (IoT)

13 Rizvi, S., Orr, R., Cox, A., Ashokkumar, P., Rizvi, M. R., (2020), Identifying the attack surface for IoT network, Internet of Things, Volume 9, March 2020, https://doi.org/10.1016/j.iot.2020.100162

14 Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. IEEE Access, 4, 1375-1384.

15 S. N. Islam, Z. Baig and S. Zeadally (2019) Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures, in IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6522-6530

16 Suaboot, J, Fahad, A., Tari, Z., Grundy, J., Mahmood, A. N., Almalawi, A., Zomaya, A. Y., Drira. K., (2020). A Taxonomy of Supervised Learning for IDSs in SCADA Environments. ACM Comput. Surv. 53, 2, Article 40 (April 2020), 37 pages. https://doi.org/10.1145/3379499

Almost all APT attacks are designed by nation state-sponsored attacker groups with access to technical and intelligence resources.[17]

When defending a network against an APT attacker, the use of conventional detection and protection systems is not adequate. When critical infrastructure is at stake, once the hacker is in, the damage is done. Thus, ICS, primarily when operating critical infrastructure, is protected by a "defense-in-depth strategy" (DiDS) [18]., providing for a holistic approach to cybersecurity.

DiDS is described in DHL's *Recommended Practice Guidelines for Improving ICS Cybersecurity with Defense in Depth Strategies*. The cybersecurity controls for SIDS are determined in NIST Special Publication 800-82 Revision 2 for ICS security.[19]

DiDS foresees seven layers of administrative, technical, and physical security controls working together to protects the ICS[20].

1. **Human Element Layer:** Faces the outer world and connects to the business network. Awareness & Training and Insider Threat Programs are the administrative controls focusing on the elimination of unintentional or malicious threats arising from the human-factor. Various administrative, physical, and technical controls are present at this level (biometrics, physical access system e-mail security, malware analysis, deceptive honey pots).
2. **Physical Layer**: Separates the Network Layer from the business network by a Data Diode (Unidirectional Security Gateway). Data Diode allows only one-way network traffic.
3. **The Network Layer**: Hosts Network Security tools, i.e., IDS, IPS, Enclave Firewall, perimeter firewall, web proxy content filtering, network-access managed, access control lists).
4. **Endpoint Security Layer:** Hosts the patch management, IDS/IPS, control security as anti-virus/malware, and overall enforces endpoint security protocol.
5. **Application Layer** Provides an additional layer of user management and hosts the database monitoring and scanning, as well as the secure database gateway.
6. **Data Integrity Layer** Data is classified, encrypted, stored.
7. **Mission Critical / Safety-Critical Assets Layer,** which is the core of the sphere, and it is protected by another layer of Data Diode[21].

In Europe, a research funded project called Prevention Protection and Reaction to Cyberattacks to Critical infrastructures (PRECYSE)[22] has undertaken studies seeking to define, develop and validate a methodology, an architecture and a set of technologies and tools to improve the security, reliability, and resilience of the ICS supporting the critical infrastructures.

The primary goals for ICS security set out by PRECYSE[23] focuses on the following issues: (i) investigating privacy and ethical issues; (ii) improving resilience through a security architecture; (iii) providing tools for preventing and protecting against cyberattacks on SCADA systems and controlling the reaction to such attacks; (iv) presenting a methodology for identifying assets and their associated vulnerabilities and threats; and (v) deploying prototypes at two sites, one in the transport sector and the other in the energy sector.

17 T.C. Truong et al., Artificial Intelligence and Cybersecurity: Past, Presence and Future, published in Das, S., Lakshmi, C., Dash, S. S., Panigrahi, B. K. (2020) Artificial Intelligence and Evolutionary Computations in Engineering Systems. Singapore: Springer Singapore.

18 https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

19 https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

20 Knapp, E. & Langill, J. T. (2015) Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress

21 https://www.advenica.com/en/blog/2019-02-19/what-is-a-data-diode-and-how-does-it-work#

22 https://cordis.europa.eu/project/id/285181

23 http://precyse.eu/

The guidelines provided by NIST, PRECYSE, and DoD are the most effective tools for the operators of the critical infrastructure for building the cyber defenses against the emerging threat vectors.

EFFECTS ON THE PHYSICAL WORLD: STUXNET APT MALWARE ATTACK

Industrial viruses like Stuxnet are global threats to critical infrastructure. They are designed to manipulate ICS to destroy a facility and cause devastation in the physical world. Stuxnet infected at least 14 industrial sites in Iran, including a uranium-enrichment plant, rendering them all inoperable. There have been Stuxnet attacks in several other locations, but most have gone unreported.

Stuxnet's design was so sophisticated that it was able to attack and destroy specific infrastructure. For example, in one instance, Stuxnet only became active when it detected that the ICS was running PLCs for Siemens-manufactured high-speed centrifuges that were commonly used for enriching nuclear fuel. Once activated, Stuxnet would take control of the PLCs and manipulate the data, causing the centrifuges to spin themselves to failure while at the same time sending false feedback to the control room, ensuring that the anomaly remained undetected.[24]

Variations of Stuxnet, such as Duqu, Flame, Shamoon, and Triton, have appeared. Shamoon attacked oil and energy sectors in the Middle East by wiping and overwriting the system files and denying access to the infected computers. Duqu was designed as a key logger to gather information to be used to develop a future attack. Duqu created a local file on ICS to prevent detection and terminated itself after thirty-six days of operations. Triton altered the safety systems in the targeted ICS leaving the ICS vulnerable to a future planned attack.

Threats to critical infrastructure can be so severe that the need for reliability, performance, and security may trump efficiency and privacy concerns related to these systems. In the context of smart and interconnected cities and communities, this raises an important question: what is a city's risk appetite for efficiency versus its desire for security? Can a city be smart and connected and still avoid the risk, for example, of being the next Chernobyl because of a malicious attack on critical ICS on a nuclear power plant? What if an attacker hacks the ICS of a dam or flood control system to inundate a city? What if traffic lights are manipulated to cause a chain accident? These are just a few examples of the kinds of security concerns that a smart and connected city may face.

THE WAY FORWARD: SECURITY BY DESIGN & THREAT INTELLIGENCE

There is no one-size-fits-all solution in the cyber world. The market is full of fancy products claiming they deliver magical results, but none of these products yet has proven to be the ultimate solution against cyberattacks. So, what is next?

Cybersecurity is regulated by standards, not rules, and each operator needs to tailor cybersecurity solutions in a manner that best fits its operations. This approach is called security by design (SbD). SbD advises that every time a new process is to be introduced into the operations of a facility, its design takes into account, or is modified to address, the relevant security concerns. NIST standards, DoD guidelines, and the studies by PRECYSE are valuable resources based on the security SbD principle. These documents do not promulgate any rules or advocate any particular technology. They simply guide stakeholders on the implementation of appropriate controls under a structured methodology fit for securing the relevant ICS.

Smart city leadership can coordinate with private sector operators of critical infrastructure, academia, and stakeholders' operators to explore the adoption of basic cybersecurity principles into the operations controlling the critical infrastructure and to foster a culture of threat intelligence. Threat intelligence or cyber threat intelligence is an invaluable tool for the critical infrastructure operators and city leaders to understand the cybersecurity threats that have, will, or are currently

24 Jon R. Lindsay (2013) Stuxnet and the Limits of Cyber Warfare, Security Studies, 22:3, 365-404, DOI: 10.1080/09636412.2013.816122

targeting critical infrastructure. This information can then be used to identify, prepare for, and prevent cyber threats and to develop alternative defense mechanisms to mitigate the risks.

One important big step towards such coordination will be to identify the opportunities for smart city leadership to communicate with the Information Sharing and Analysis Center (ISAC)[25] and Information Sharing and Analysis Organizations (ISAOs). ISAC was established in 1998 by a presidential directive, and it is an industry-specific organization that gathers and shares information on cyber threats to critical infrastructure. ISAOs were formed in 2015 by a White House directive to promote voluntary cyber threat information sharing within industry sectors. DHS encourages the development of ISAOs for private companies, nonprofits, government departments, and state, regional, and local agencies. For instance, an ISAO member EnergySec[26] is a threat intelligence platform for sharing Indicators of Compromise through the Department of Homeland Security's Automated Indicator Sharing program, which also provides threat sharing tools to its members operating in the energy sector. EnergySec is just one of many platforms; many other organizations are actively working on developing and improving threat sharing and vulnerability disclosure programs. A coordinated partnership among a smart city, ISAO, and ISAC will be a great tool to create an informed opinion for the smart city leaders on the emerging threats that may affect the safety of their city.

There is no one-size-fits-all solution in the cyber world.

25 https://www.a-isac.com/faqs
26 https://www.energysec.org/

Sinan Pismisoglu is a member of Dentons' Intelligence & Strategic Services practice group, working directly with the firm's Global Chief Security Officer. He is a certified information privacy professional for the US Sector (CIPP/US). His practice focuses on data-breach management through forensic analysis, incident response, and breach notification coordination under a variety of legal regimes around the world, and has expertise in cybersecurity and privacy issues and compliance. Among other things, he designs sophisticated tabletop exercises based on real-life APT attack scenarios, and advises clients on breach management, setting up malicious and unintentional insider threat programs, insider threat technical monitoring, and jurisdictional restrictions on monitoring.