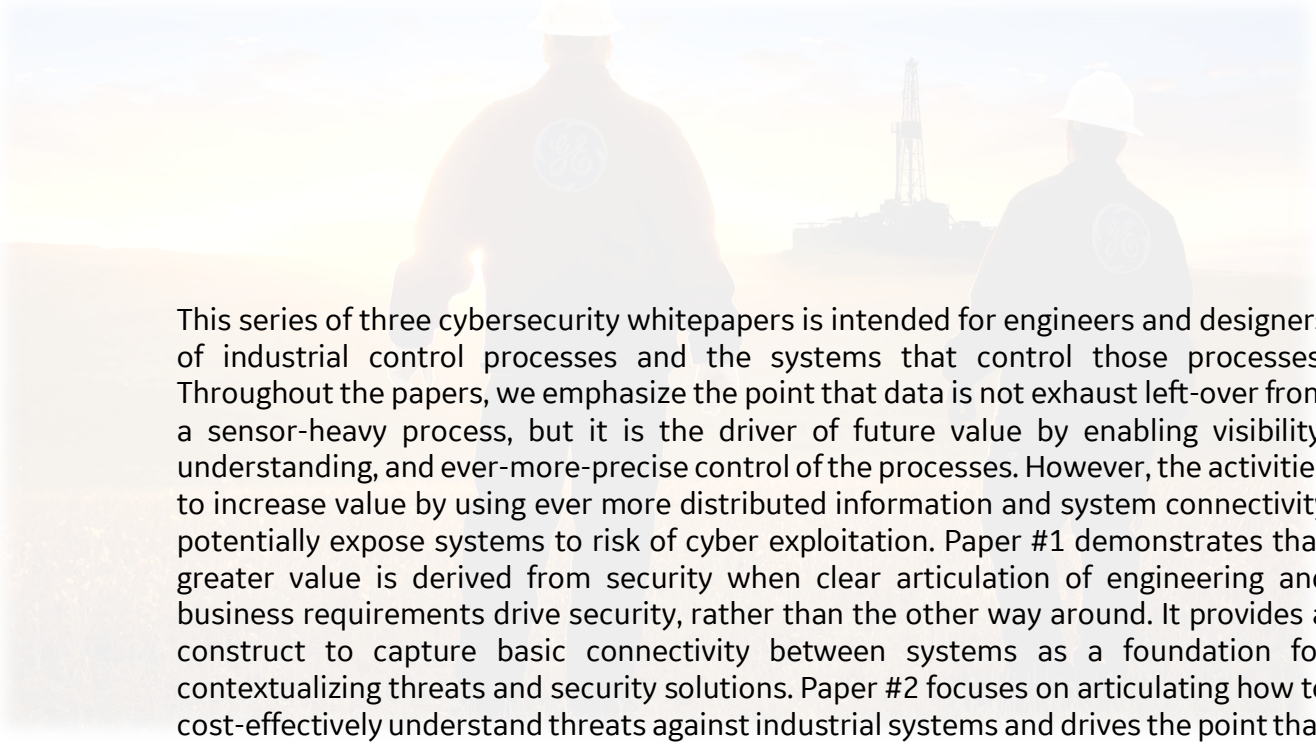
2018

Understanding Threats will Promote the "Right Amount" of Security

DESIGN AND BUILD PRODUCTIVE AND SECURE INDUSTRIAL SYSTEMS, WHITEPAPER #2

KENNETH G. CROWTHER (GENERAL ELECTRIC), ROBERT M. LEE (DRAGOS), K. REID WIGHTMAN (DRAGOS)

A COLLABORATION BETWEEN GENERAL ELECTRIC AND DRAGOS.

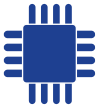


This series of three cybersecurity whitepapers is intended for engineers and designers of industrial control processes and the systems that control those processes. Throughout the papers, we emphasize the point that data is not exhaust left-over from a sensor-heavy process, but it is the driver of future value by enabling visibility, understanding, and ever-more-precise control of the processes. However, the activities to increase value by using ever more distributed information and system connectivity potentially expose systems to risk of cyber exploitation. Paper #1 demonstrates that greater value is derived from security when clear articulation of engineering and business requirements drive security, rather than the other way around. It provides a construct to capture basic connectivity between systems as a foundation for contextualizing threats and security solutions. Paper #2 focuses on articulating how to cost-effectively understand threats against industrial systems and drives the point that security should be adapted based on connectivity requirements from the business and the threats to the processes, rather than published vulnerabilities and exposures. Paper #3 ties the two pieces together and further explores details of how engineers can guide the implementation of good industrial control system (ICS) security into the future as next generation control systems and connectivity requirements emerge. It assumes some knowledge of the basics, and focuses on what engineers should learn to design next-generation security around the business and engineering requirements of ICS.

CYBER-ESPIONAGE AND ATTACKS ON CONTROL SYSTEMS CAN CREATE LOSSES

ATTACKS HAVE AND WILL CONTINUE TO TARGET CONTROL SYSTEMS

Cyber threats against industrial control systems (ICS) are increasing and should not be ignored. Consider a couple nontrivial examples of reports of cyber-caused outages of industrial control systems from the last couple years (2016-2018):



Taiwan Semiconductor Manufacturing Co. estimates $256 million in losses from production shut-downs resulting from WannaCry infection on its production lines over a weekend. [1]

Maersk (large logistics company) estimates $300 million in losses from an outbreak of NotPetya ransomware. They wiped and reinstalled 4,000 new servers, 45,000 new PCs, and 2,500 application to restore their logistics operations. They were able to maintain about 80% of operations in manual mode while product systems were out.[2]

CRASHOVERRIDE malware was deployed against a transmission level substation in Ukraine and caused a loss in power. The malware's impact resulted in roughly 30% of the load lost. This specific family of malware was the first ever to target electric grids directly and presents a blueprint for future adversaries.[3]

A Saudi Arabian company lost production from a shutdown caused by the TRISIS malware on its safety instrumented system controller.[4] Down-time in such plants can cause roughly $9 million lost revenue per day.[5] The purpose of this attack was to remove the safety functionality and kill people; luckily the attacker failed this time.

Recent attacks on industrial systems and recent malware tailored for control systems, such as CRASHOVERRIDE and TRISIS, show that attackers can obtain knowledge about process and automation networks for new attacks that engineers may have considered obscure or highly technical. With the obvious need for security, measured approaches must be considered instead of knee-jerk reactions that may be inconsistent with engineering and business requirements. Engineers need to understand enough of their requirements and potential threats to ensure security is adequate to defend the intended processes (or the intellectual property contained in the process data) instead of dictating non-useful security measures. With increasing connectivity and associated value also comes increased risks to manage.

---

[1] E.g., see https://arstechnica.com/information-technology/2018/08/the-debilitating-wannacry-worm-shuts-down-key-iphone-supplier-for-2-days/

[2] E.g., see https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/

[3] E.g., see https://www.wired.com/story/crash-override-malware/

[4] E.g., see https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[5] Based on about 100,000 barrels per day, average breakdown of outputs, and wholesale prices about $88 for each processed barrel of crude. There is no published data about outage duration or losses.

When considering threats to ICS, it is important to note that the "threat" is the human adversary. It is a mistake to simply focus on studying malware or patching vulnerabilities because many attacks can be done with native features and functionality already present in industrial networks. Process architects and engineers need to develop a general understanding of threats to control systems so they can work and collaborate with control network experts and security engineers. As adversaries evolve their capabilities, it will be increasingly important for security decisions to be the product of a collaborative effort, based on a shared understanding of system requirements and threats. (See Figure 1.)

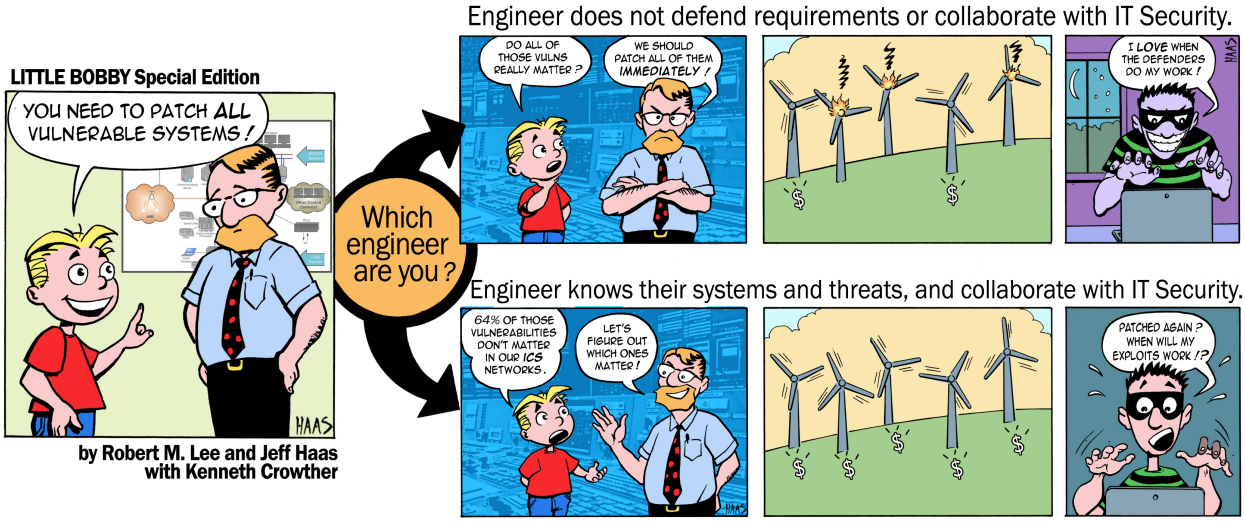


FIGURE 1. EFFECTIVE CYBERSECURITY WILL REQUIRE COLLABORATION BETWEEN ENGINEERS THAT DESIGN AND MAINTAIN INDUSTRIAL PROCESSES AND THE CYBERSECURITY EXPERTS THAT UNDERSTAND CONTROL NETWORKS AND CYBER THREATS.

Even though studying malware is insufficient to protect systems, it is instructive to be familiar with a few families of ICS-tailored malware to begin the discussion of threats to ICS. Not all of them caused process disruptions (e.g., malware that leveraged the OPC protocol, identified as HAVEX, was just a spy tool). Each were tailored and targeted toward a specific company or industry and their systems. Beyond specific families of ICS malware, there have been numerous compromises targeting industrial networks specifically; these are far more numerous than make into the news or community advisories. These growing breaches and attacks are targeted toward ICS and can initiate from a wide variety of connections including the site's IT network (Level 3) as well as remote vendor and integrator connections. No matter how sophisticated the attack, they are visible and defensible with modern industrial network and system monitoring techniques. Sometimes, the ICS attacks of most concern are those that figure out how to exploit native "features" (not flaws or weaknesses) in the control systems.

Consider the following ICS-tailored malware as an introduction to ICS-specific threats.

STUXNET (discovered 2010)

A complex and carefully targeted worm that faked control sensor signals to damage centrifuges – thus reducing the nuclear fuel refining capabilities of Iran. While it did infect other computers in other companies, it did not have much effect because it was so highly targeted to controllers at the specific Iranian facility. This is an early example of an adversary building/delivering an expensive and targeted malware to disrupt physical operations.

HAVEX (discovered 2013)

A malware with a variety of capabilities including the ability to scan networks for specific ports and protocols widely used by industrial controllers, or leverage OPC to gather information directly and send the information back to internet connected servers where the adversaries accessed the information. It is a tool for learning about control systems at scale and primarily targeted thousands of companies in defense, energy, aviation, and petrochemical sectors of North America and Europe. This is the first example of an adversary designing malware to bulk gather targeted information about ICS networks. This information could be used in future attacks or for espionage.

BLACKENERGY 2 (discovered 2014)

Originally designed as a common malware framework leveraged by many different adversaries for denial of service attacks, an adversary augmented it to include HMI specific exploits to gain access to remotely connected HMIs across multiple vendor families. It was used to target a wide range of industries in Europe, US, and the Middle East. A further upgraded version called BLACKENERGY 3 was used to gain access to the enterprise networks of multiple power companies in Ukraine in 2015. From there, the adversaries leveraged their access to move into the control centers and cause disruption after learning how to leverage the distribution management systems. This is an example of an existing malware being repurposed and extended to target ICS and resulted in the first cyber-attack-caused power outages.

CRASHOVERRIDE (discovered 2016)

It is more like a malware platform than a specific application. It is able to communicate correctly in ICS protocols such as IEC104, IEC61850, and OPC and deliver targeted directions to change process states (e.g., open a circuit breaker and keep it open despite commands from the operator to close). The malware was deployed against a transmission level substation in Ukraine in 2016 to cause a power loss. The malware was not vendor-specific nor did it require any vulnerabilities to work correctly; it is an example of malware that takes advantage of native ICS knowledge and weaponizes its features.

TRISIS (discovered 2017)

It is a framework for delivering and executing malware in safety instrumented systems (SIS). This malware represents the expansion of malware targets and methods of execution. It requires a high level of knowledge of the system and significant effort to access and deploy. It also represents the first time that safety features of a system have been targeted and compromised directly. It was deployed against a SIS at a petrochemical plant in Saudi Arabia. The attackers were attempting to remove the safety features which would have allowed them to target the distributed control system (DCS) and cause an attack that would kill people. However, due to a small coding error the attack failed, tripped the SIS, and shut the plant down. The adversary that deployed TRISIS, identified as XENOTIME, has been found in multiple other facilities outside of Saudi Arabia, however variants of TRISIS have yet to be discovered.

These ICS-tailored malware and malware-platforms should alert us to the fact that tactics and techniques of adversaries are evolving and ICS is attackable. However, it should also provide some level of reassurance that the community is able to learn from these attacks and engineer/apply defenses that counter these and similar attacks in the future. Figure 2 shows an illustrative sliding scale of sophistication to demonstrate that adversaries exist across a range of sophistication. The sliding scale provides generic examples, such as a cyber vandal that reuses malware or a cyber warrior that seeks to degrade critical infrastructure using tailored malware. The scale also provides a number of example hacker campaigns with titles from a variety of threat intelligence organizations. The titles of the adversaries for these campaigns come from multiple sources; for example, HawkEye is a name given by Trend Micro, FIN7 by FireEye, Dragonfly by Symantec, and Xenotime by Dragos. Most malware against ICS networks will likely be on the lower-end of sophistication, such as phishing emails to the site LAN to try to collect login credentials. Larger, more well-connected ICS that are part of critical infrastructure (e.g., Power, Transportation, Healthcare) in large countries are more likely to be targeted by more-sophisticated threats.

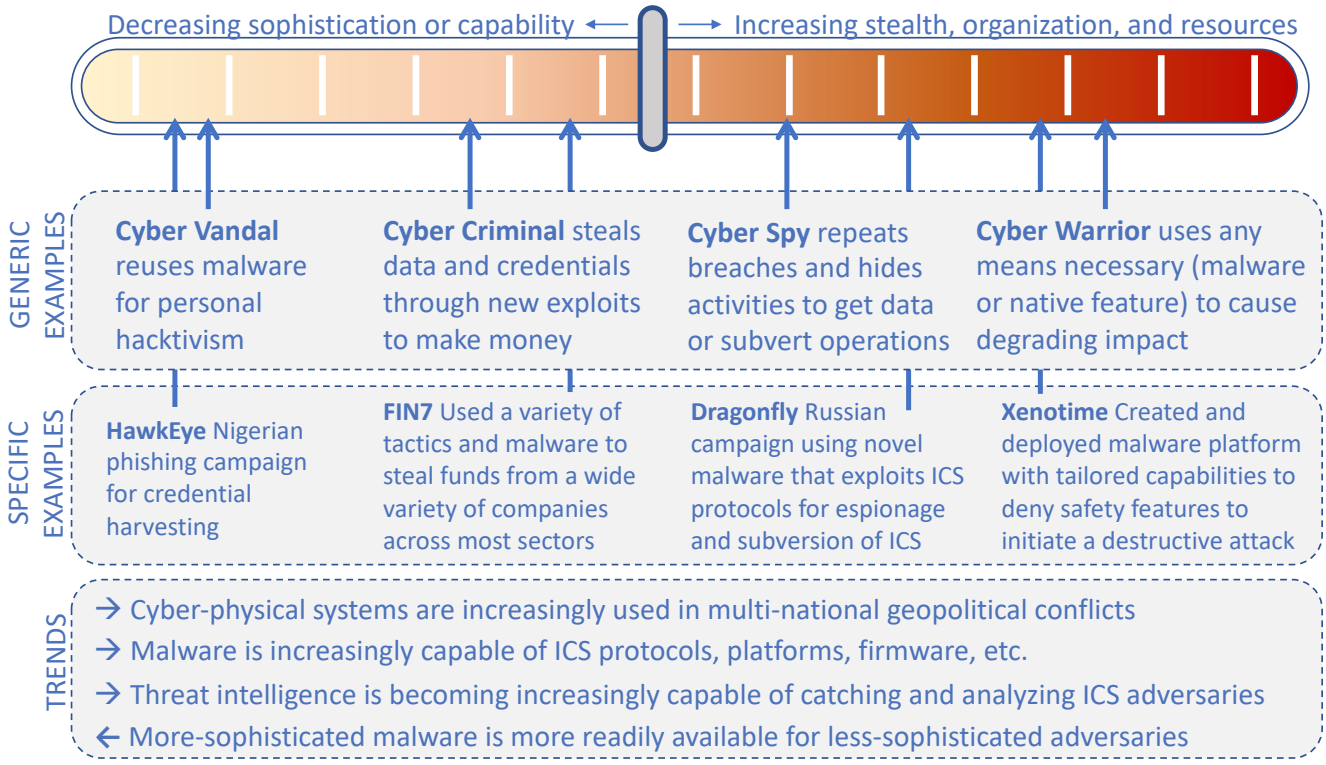


FIGURE 2. THREAT ACTORS EXIST ON A SLIDING SCALE OF SOPHISTICATION, TRENDING TOWARD GREATER SOPHISTICATION.

A sliding scale helps to educate about the diversity of adversaries, but effectively leveraging threat intelligence requires a framework for navigating information about the victim personas (e.g., Are they in your industry? Do they use similar products or operations?) and the adversarial capabilities (e.g., How do they get credentials? How do they pivot to ICS? What controllers are vulnerable to their malware?). This type of information is generally captured in a "diamond model." Each adversary can be characterized by their capabilities and methods (i.e., their tradecraft), the infrastructure they leverage to deliver those capabilities, and the victims they target. *Considering your similarity to victims can yield insights into the types of adversarial capabilities you should protect against* – which helps to keep tabs on weaknesses and prioritize countermeasures and mitigations. Various entities, such as Dragos, Symantec, ICS-CERT, FireEye, Trend Micro, and others provide this type of information.

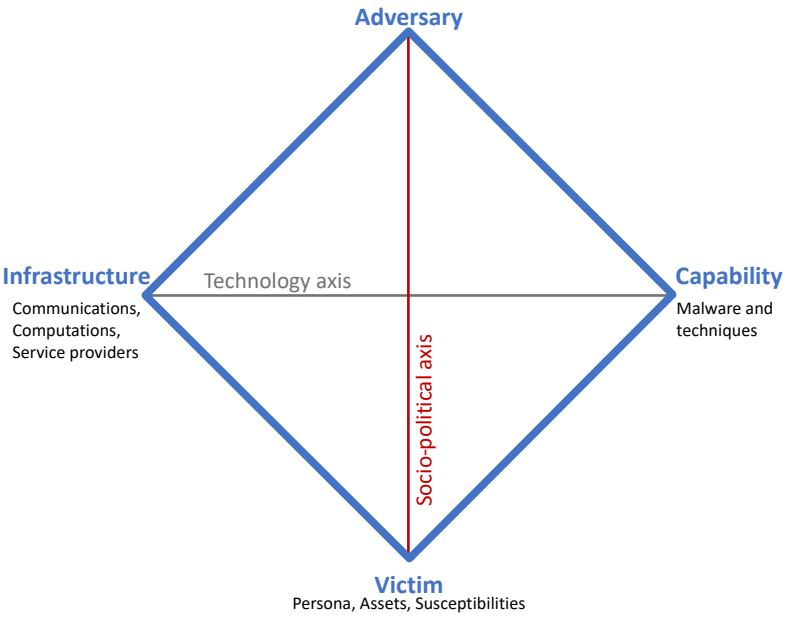


FIGURE 3. THE DIAMOND MODEL PROVIDES A FOUNDATION FOR UNDERSTANDING THE RELATIONSHIPS BETWEEN DIFFERENT FEATURES OF THREAT INFORMATION.

A diamond model helps gain insights into threat intelligence, because it helps you understand how to use the information that you have to formulate queries. For example, consider the diamond models in Figure 4 that use sample information from Dragos. Each adversary (top) leverages different infrastructure (left) to deliver different capabilities (right) to target different victims (bottom). Once you understand your relationship to the victims, then you can prioritize knowledge received regarding how those adversaries were successful in exploiting their victims, and can use this knowledge to target resources to advance system protection.

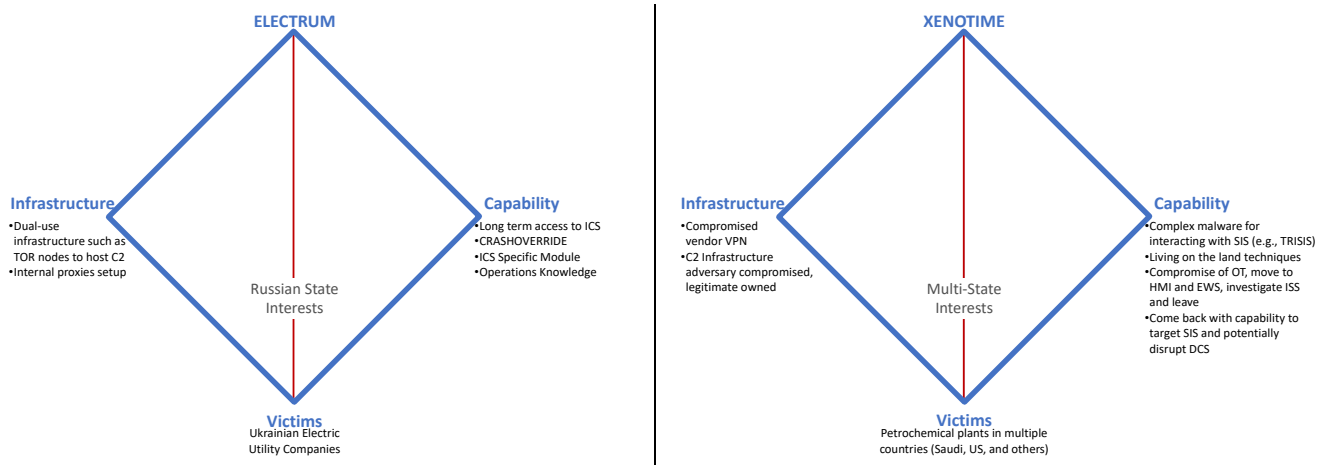


FIGURE 4. EXAMPLE DIAMOND MODELS OF ELECTRUM AND XENOTIME SHOW DIFFERENT VICTIMOLOGY AND CAPABILITIES.

For example, Dragos published information about ELECTRUM targeting Ukrainian utility companies using stealthy, persistent activities that are specifically targeted and carefully crafted to be disruptive. (See the left side of Figure 4.) These types of attacks are possible against any utilities that have assets and protocols similar to those used by the Ukrainian utilities. By focusing on the adversary's tradecraft, or the infrastructure and capabilities by which the adversary achieved success, we can prioritize or design protections against any similarly-styled attacks in the future. As an example, utilities could design ICS specific security controls for the way ELECTRUM moved into the environment and the use of specific protocols (e.g., OPC, IEC 61850, DNP3). This would encourage ICS-specific network and operations monitoring as well as the creation of incident response plans that deal with CRASHOVERRIDE-like scenarios. Alternatively, XENOTIME was successful against a petrochemical plant in Saudi Arabia. (See the right side of Figure 4.) If you are a petrochemical plant, then you should consider paying special attention to your SIS through configuration management and careful safety engineering with supplemental physical/mechanical safety systems. When purchasing a SIS, you might consider those with code signing in a way that would prevent TRISIS-like code augmentation. In both cases it is a best practice to exercise the incident response plan as well as a table-top exercise bringing engineers, operators, and IT security together to talk about their respective roles and responsibilities. Monitoring these threat reports and paying attention to the similarities between your assets, operations, vulnerabilities, or exposures and those of the victims described in the reports is key to making defensible assumptions about threats that can help to prioritize protection.

Designing new malware only requires understanding system vulnerabilities and exposures and writing code to accomplish specific objectives in the context of those vulnerabilities and exposures. A threat diamond model captures information about adversarial tradecraft at the behavioral level – what is being targeted, what infrastructure is leveraged for delivery, what capabilities will be used for exploitation. *Changing these behaviors is difficult and expensive for adversaries, and as such, provides a strong foundation for targeted cybersecurity protections*. Process engineers and architects that understand threats at this level can improve their ability to collaborate with cybersecurity experts as they design connected and remotely controlled operations in an emerging Industrial Internet of Things or Industry 4.0 environment. This knowledge of threats will aid in appropriate budgeting for the security aspects of projects that involve industrial control systems, improve tailoring of security requirements into process design, and overall enhance the potential to consistently produce value through connectivity and control that maintains availability and safety of operations.

The previous paper (Paper #1 titled, *Building security to achieve engineering and business requirements*) emphasized that engineering and business requirements should drive industrial operations, but will need to drive ever-more-innovative security strategies. This paper describes methods for conceptualizing and leveraging knowledge of the threats against ICS to position your business to appropriately prioritize security innovations. The next paper in this series (Paper #3 titled, *Blending resilience and security hardening will achieve greatest security for the most business viable systems*) describes solutions to evolve security and resilience in response to your control network requirements and threat assumptions.

FURTHER READING:

M. Assante and R. Lee, 2015. *The Industrial Control System Cyber Kill Chain.* (https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297) This paper identifies steps that adversaries have to take to attack industrial control systems with high confidence. It adapts the traditional "kill chain" paper written by Lockheed Martin analysts for purposes relevant to industrial control systems. One of the major focuses is showing that attacks are not singular isolated events but instead steps an adversary has to take giving defenders numerous opportunities to defend.

S. Caltagirone, A. Pendergast, and C. Betz, 2013. *The Diamond Model of Intrusion Analysis.* (http://www.dtic.mil/docs/citations/ADA586960) This paper introduces and provides details on the threat diamond and various implications and utilizations of it to evaluate and understand threats against your systems. It is not necessarily ICS focused, but provides a good overview of threat information processing.

DRAGOS, 2017. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations* (https://dragos.com/blog/crashoverride/CrashOverride-01.pdf) This paper is focused on the CRASHOVERRIDE platform, but describes some of the other threats to ICS and their evolution. It also provides a broad understanding of the types of capabilities that CRASHOVERRIDE provided at the time of the analysis, which will provide a sense for the type of threat intelligence that is available.