

Cyber-Physical Security and Critical Infrastructure

Protecting nations and
societies in the era of
connected systems and
hybrid threats

February 2023

Table of contents

Foreword

04

Section I. Physical-Cyber Security

A. Introduction—Making Connections

06

B. Defining Critical Infrastructure and Protection Needs

08

C. Connected Operating Environments

10

D. Cyber-Physical Threats and Vulnerabilities

13

E. “Hybrid” or “Blended” Threats

16

F. Vulnerability from Security Silos

20

G. Benefits of Security Convergence

23

H. Security Convergence Framework

26



Section II. Issues in Physical-Cyber Security

1. Prospective Analysis of the Private Security Industry	31
2. Towards an Integrated Vision of the Cyber and Physical Governance of Organizations	33
3. Reimagining PPPs to Enhance Critical Infrastructure Resilience	35
4. Convergence of Physical and IT Security in Critical Infrastructure, Great! But what about OT?	37
5. Overcoming Barriers Between IT and Physical Security	40
6. Joint Risks Assessments and Penetration Tests	43
7. Using Metrics and Other Activities to Bridge Physical and Cybersecurity Strategy	46
8. A New Security Paradigm in the Threatening Cyber Era—from Physical to Converged Security Information Management	49
9. Cyber-Physical Security: Can EU Legislation and/or Standards Help?	51
10. Table of EU Legislation Relevant to Cyber-Physical Security	54

Every day, the press reports about cyber-attacks against organisations and companies, and Critical Infrastructure are a major target, primarily in the energy sector, but also in healthcare, communication, financial, and other sectors.

Foreword

Most attacks involve human intervention, intentional or not, and have consequences in the physical world; yet cybersecurity and physical security are still handled in silos, creating vulnerabilities. This White Paper explores the blurring frontier between these two worlds and describes how a holistic approach can help protect organisations and make them more resilient.

If the current conflict in Ukraine highlights cyber-attacks carried out in the context of war, it should be emphasized that they are also taking place in other regions experiencing tensions and latent conflicts, such as in the Middle East between Iran and Saudi Arabia. Everyone remembers the Stuxnet attack in 2010, but who knows that it had been active since 2009, and had already infected a dozen companies before attacking Iranian centrifuges? Stuxnet was different from any other virus or worm that had come before.

Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to physically destroy equipment those computers controlled. Then, in response to Stuxnet, there was the attack on Saudi Aramco by Shamoon in 2012, which compromised 30,000 computers. Finally, from 2016 to 2018, there were numerous attacks on Saudi Critical Infrastructure networks and on government agencies. And similar examples can be found in all parts of the world.

Cyber-attacks are a strategic weapon of choice in conventional conflict and have been for a long time. They are a primary way in which States, organisations and individuals can harm other States, organisations, and individuals, whether in a public or private setting. And while computers may be the targets of infection, human action has shown to be a constant factor in these attacks.



Magnus Ahlqvist
Chairman of the International
Security Ligue



Vinz Van Es
Chairman of CoESS

It should therefore be emphasized that protecting the access to information and systems is and will remain three-dimensional, consisting of physical protection, the human factor, and digital protection. It has become clear that there is no point in trying to protect, let alone respond, to an attack with a siloed approach. Likewise, protecting organisations against threats in the digital world, particularly cyber-attacks, can only be done with a holistic approach.

The consequences of cyber-attacks are also three-dimensional: IT infrastructures neutralized or destroyed; industrial production or services blocked or annihilated, with potentially serious industrial accidents; and finally, in human terms, injuries or deaths and job losses.

Whether through accident, negligence, or malicious intent, the human role is eminently present in the development and dissemination of cyber-attacks. As such, the human factor is a constant that must be fully integrated in a protection strategy capable of protecting against both an “involuntary vector” as well as a “malicious vector” (external or insider threat). It is because the human dimension cannot be dissociated from the defense strategy of organisations, that the notion of cyber-physical security has become essential.

Promoting the concept of cyber-physical security, the subject of this White Paper, represents a reasonable and critical response to today’s threat. It was written by experts from across the globe under the aegis of the International Security Ligue and CoESS, joining forces to protect people, organisations and infrastructure against combined attacks that unfortunately will continue to be made.

Section I. Physical-Cyber Security



A. Introduction—Making Connections

This white paper, a joint project of the International Security Ligue and the Confederation of European Security Services (CoESS), endeavors to help strengthen the world's critical infrastructure in a time of growing complexity and increasing threats.

It is divided into two sections. Section I provides background and context on the fight to protect critical infrastructure (CI). It explores the meaning of CI, the ramifications of connected systems, the rise of physical-cyber threats, and explores security convergence to counter them. Section II examines specific physical-cyber security issues in greater detail, advancing guidance for devising comprehensive solutions to current and future challenges.

Why this paper? Why now?

The world's critical infrastructure is a greater target and more vulnerable than ever, facts that demand a comprehensive approach to protection that aligns physical and cybersecurity. Now that many threats and technological solutions crossover between the two disciplines, it is natural that the mission of protection would need to undergo transformation.

The security of nations and citizens are at stake. Given today's threat environment, the world requires greater government and private sector attention to security issues and persistent investment in solutions—and it requires collaboration between the two entities.



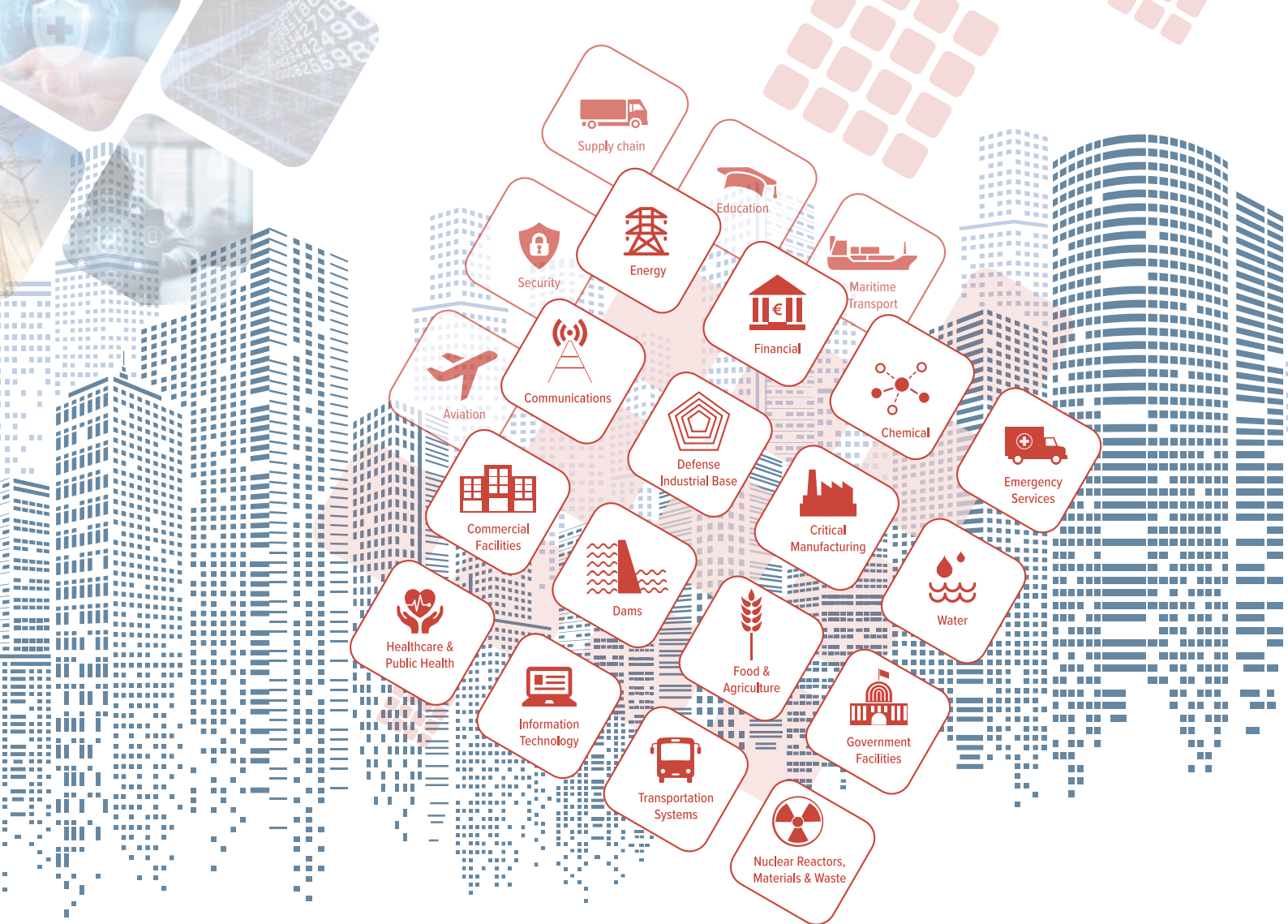
“Greater collaboration and partnership between the public sector and the private sector is unquestionably the direction we have to go in. We don’t have the luxury of not focusing on collective defense anymore. We must look at this as a team sport,” explained Jen Easterly, Director, US Cybersecurity and Infrastructure Security Agency, as she addressed the world’s economic leaders at Davos 2022. “At the end of the day, this is not a problem that we are going to solve. This is going to be a persistent problem, that we’re all going to need to work together on around the world.”

Security threats faced by critical infrastructure today aren’t cyber or physical—they’re both. And, just as often, countermeasures aren’t one or the other. But this convergence hasn’t spurred a great revolution in how security is managed.

Collaboration is imperative within critical infrastructure facilities, where there is typically a complicated division of responsibility for different aspects of protection. It may now be insufficient, as the threat surface has grown and threats overlap, to approach security purely at the functional level and to manage threats and deploy countermeasures department-by-department. Cooperation is needed at every level, with key stakeholders working together to support overall security, and with a collective understanding of what is most critical to protect.

The stakes are high, and the solutions must be comprehensive and process-oriented, capable of both combatting today’s threats and providing a platform for those to come. Critical infrastructure security is not a solution that can be implemented, it is a process that must be nurtured, requiring money, commitment, long-term strategic planning, and a holistic vision.





B. Defining Critical Infrastructure and Protection Needs

What is Critical Infrastructure? The term is both highly descriptive and somewhat ambiguous.

Critical infrastructure is generally regarded as the foundational assets that nations need for societies to function; the systems that underpin what people need to live and businesses require to operate. These are the assets and systems—that if destroyed or disrupted—would have a debilitating impact on a nation’s security, economy, or its health and safety. In short, it is the bedrock of civilization, and the point of departure for prosperity.

The term has evolved. Because of advances in technology and growing concern that critical infrastructure could be the target of attack, there has been a broadening of the context in which critical infrastructure is viewed. Beyond merely ensuring the adequacy of public works, critical infrastructure is now observed in the context of national security. This has generally expanded the number of infrastructure sectors and types of assets that are recognized as critical.

But exactly which industries should fall under the definition of critical infrastructure is a grey area, reflected by global disparity in the sectors and assets that nations include within it. Some sectors are widely and historically included, like Water Systems and Energy; others have been more recently added, like Information Technology and Telecommunications; and other assets are vital but not always included, such as Hospitals and Banks. Additionally, critical infrastructure sectors contain many physical assets of varying levels of importance and identifying which should be viewed as critical is a complicating factor in arriving at the “right” definition.

The number of industry sectors that should be included in the global discussion of critical infrastructure needs to expand, according to Jen Easterly, Director, US Cybersecurity and Infrastructure Security Agency. The Communications sector is an example: while not always falling under a critical infrastructure definition, it is an integral component of every country’s economy, underlying the operations of all businesses, public safety organizations, and government. “Critical infrastructure is the networks, systems, and data that we rely on every hour of every day, and that’s the water, it’s the power, it’s the telecommunications, it’s the healthcare, it’s the transportation—it’s all those things that underpin our daily lives,” she explained at Davos 2022.

The definition of “critical infrastructure” that nations adopt is meaningful. Most critically, it directs and focuses governments’ security strategies and spending on protection activities. Nations put more energy and resources to protect those assets that they have identified as being critical.

The definition is also important because much of critical infrastructure is privately held.

In many countries, the private sector owns most critical infrastructure, with up to 85% of all critical infrastructure in private hands, which means that the vulnerability of nations is largely out of its immediate control. Thus, the definition of critical infrastructure is critical because it:

- can encourage such operators to recognize their critical role in society and the need for them to invest in protection for the good of the country and its citizens;
- facilitates the sharing of security information between private industry and governments, which is critical to increase awareness of vulnerabilities and address them; and
- functions as the foundation for the imposition of government security mandates, including guard requirements, on infrastructure which is largely private.

Critical infrastructure are the essential building blocks that allow people to live their everyday lives, and governments must define the term accordingly. **It encompasses more business sectors than is commonly recognized, a fact that governments must recognize if they are to strengthen the security of nations and ensure the resilience of societies.**



- **The definition of “critical infrastructure” is important, influencing security prioritization, the allocation of resources, and regulation.**
- **The number of industry sectors that are part of global discussions of critical infrastructure must expand.**



C. Connected Operating Environments

While critical infrastructure is the foundation that allows people to conduct their everyday lives, connected systems underpin much of the critical infrastructure that keeps nations running. There is an increasing interconnectedness to everything people rely on, from the delivery of electricity to financial services.

Efficiency is driving the rapid connectedness of systems, allowing for automation, greater productivity, enhanced capabilities, and lower costs. Businesses also see connectivity as a competitive differentiator, fueling even more rapid adoption.

These are not only lures for private owners of critical infrastructure but for governments as well. To isolate cyber and

physical systems from one another is to miss opportunities to reduce pollution, lower energy consumption, and keep pace in an increasingly digitized and connected world. Digital connectivity allows nations to manage growing populations and meet demands for higher standards of living.

Fueling this revolution is the Internet, the Internet of Things (IoT) and its subset, the Industrial Internet of Things (IIoT), and related wireless connectivity technologies like 5G and Wi-Fi. Conservative estimates suggest there are more than 30 billion sensors, platforms, and devices comprising this vast network confluence and data sharing.

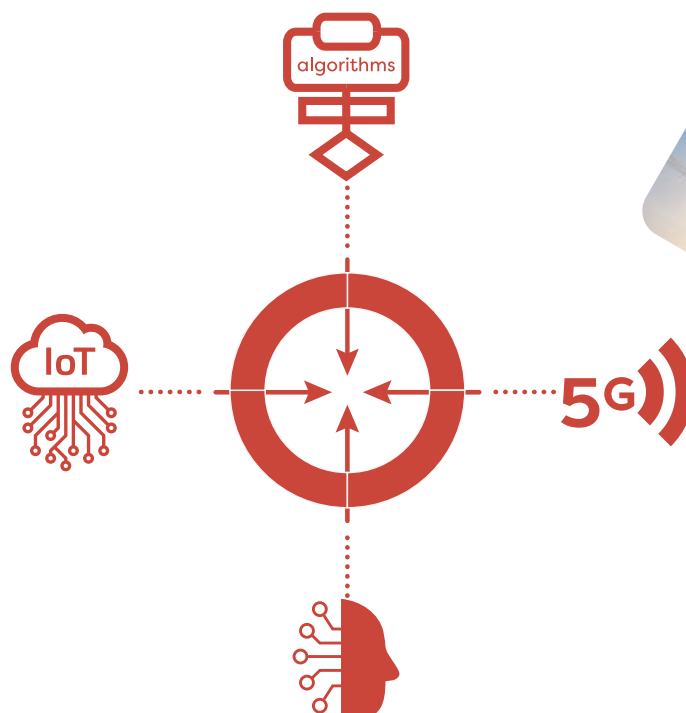
IoT is a catchall that refers to the array of physical objects in the environment—

computers, devices, appliances, vehicles, wearables, sensors, and so on—that contain embedded technology to communicate with each other and feed data back and forth. It is seen in factories using sensors to more precisely track materials and coordinate supply chain logistics; to people wearing devices to track activities, health, and fitness; to mining companies that use remotely controlled heavy equipment so they can operate in isolated, dangerous locations without threatening worker safety; to restroom paper towel dispensers signaling when they need to be refilled. **Technologists envision a future in which just about everything is a node on a network, and the future is well underway.**

Many of the same technologies that link people, homes, and businesses, are used by critical infrastructure and in industrial environments (IIoT), for similar purposes. Owners of critical infrastructure assets are embracing connected systems to enhance productivity and efficiency. Traditionally isolated devices in Supervisory Control and

Data Acquisition systems and Industrial Control Systems now employ IIoT to transmit data, from power plants to water treatment facilities.

It is now common for computers and other technologies to be integrated into the design and function of physical infrastructure. Computers have long been incorporated into numerous physical systems, such as vehicles, heating and cooling systems, and manufacturing devices, and are now integrated into physical infrastructure, which is most clearly observed in the development of “smart grid” technology, where networked computers and communications technology work autonomously to resolve problems in the electric grid, manage energy use, and administer electricity generation. Automated traffic control has become part of transportation infrastructure and “smart” water systems proactively monitor the health of their own physical infrastructure.



Moving forward, 5G and other enhanced mobile broadband technologies will further facilitate applications across critical infrastructure facilities, and Artificial Intelligence will permit untold progress in making efficient use of sensor data, to understand why a piece of equipment failed, for example, or to help locate and extract natural resources, or facilitate rapid emergency response. Connectivity of critical infrastructure provides the floor on which future “smart cities” will be built.

Among the current and envisioned use cases are:

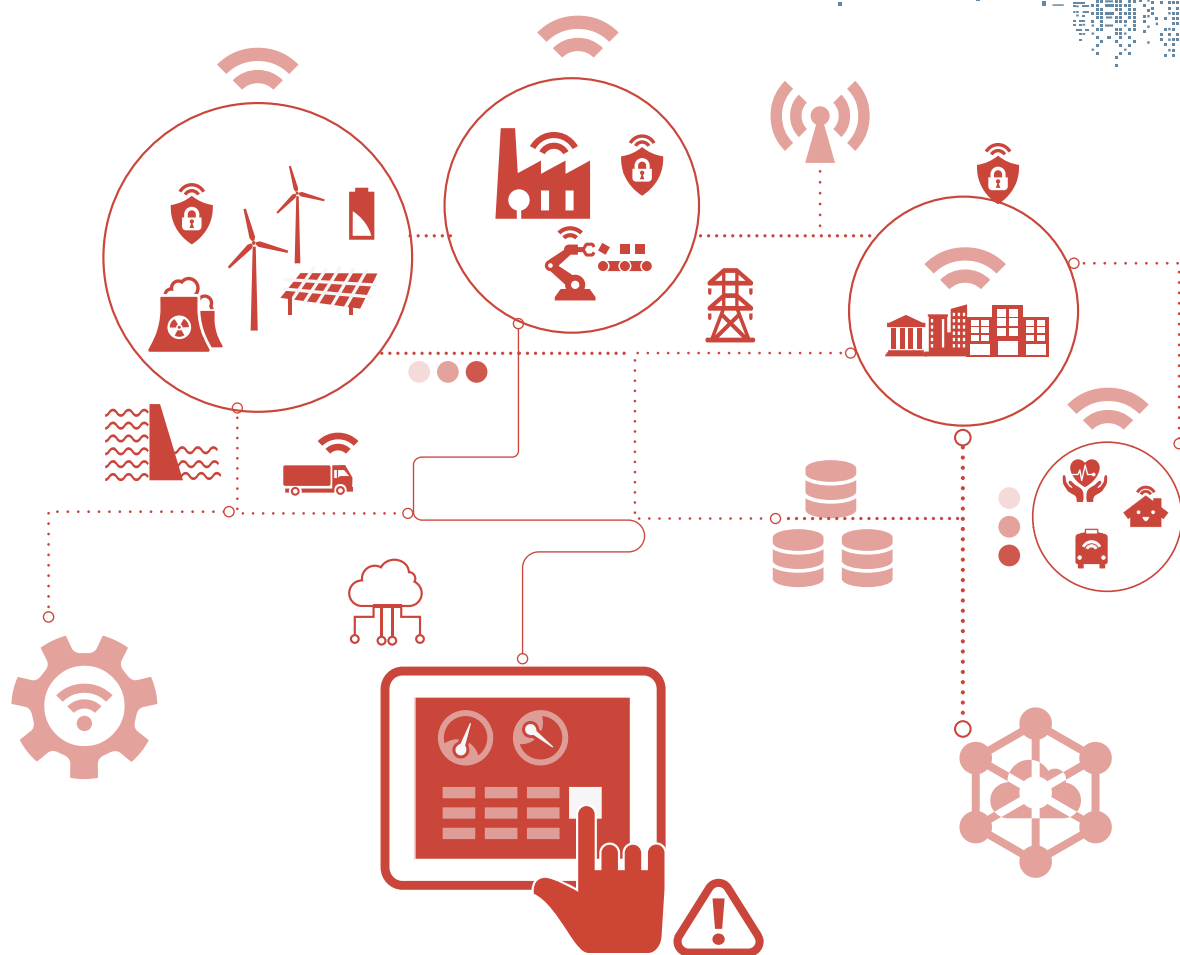
- Smarter systems, such as heating and cooling systems that improve air quality and reduce energy consumption.
- Industrial machines that can gather information about performance and alert when maintenance or cleaning is required, thus reducing unscheduled maintenance or downtime.
- Sensors that can alert agricultural producers about soil conditions that help manage water resources and increase crop yield, or sensed roads, bridges, and rail lines that report on their state of wear and alert when they need repairs.

Much of future human progress will arise from making use of data from connected systems. However, this connectivity brings with it momentous change. Namely, an end to the separation between computer networks and physical systems, between operational technology and information technology. In its place is a complex and interconnected mesh of cyber-physical systems serving as the foundation for the world’s critical infrastructure, supporting or delivering infrastructure services, and providing the basis for the future advancement of societies.

“Much of the future progress will arise from making use of data from connected systems. This will mean the end of the separation between computer networks and physical systems, between OT and IT.”



- **The division between physical and computer systems is being erased, replaced by an interconnected mesh of cyber-physical systems.**
- **Connected systems allow for greater productivity and enhanced capabilities and will serve as the foundation for future human progress.**



D. Cyber-Physical Threats and Vulnerabilities

Connectivity has a cost

While there are countless benefits from aggregating and analyzing data from multiple endpoints, when devices in the field communicate back to network data centers, and computer systems are connected to the Internet, the attack surface expands exponentially.

With connected systems, a company's security perimeter extends to devices operating outside of secured locations and may link to its critical systems. **Connectivity highlights the fact that defense-related activities are linked, with each representing a link in a chain. And, like any chain, it is only as strong as its weakest link.**

The threat of Internet attacks on physical systems at critical infrastructure operators

has grown: SCADA (supervisory control and data acquisition) networks became more vulnerable when owners took these formerly closed systems and began to allow access to them from computers that also had Internet access.

This can be a particular problem for older critical infrastructure, warned panelists at Davos 2022. Legacy critical infrastructure systems being opened to communication and pushed to the cloud could collide with today's rising geopolitical tensions with devastating consequences for societies. From recent attacks on Israeli water systems and electricity grids in India and Ukraine, global leaders warned that critical infrastructure is a greater target and more vulnerable than ever.

Connected devices within critical infrastructure pose risks by introducing new avenues for potential remote exploitation of enterprise networks, with the infrastructure used to enable IoT devices being beyond the operator's control. Any failure in IoT device management—that may leave devices unmonitored and unpatched—represents a vulnerability that can be attacked. And, with connected systems, any avenue inside the network has the potential to end in a catastrophic breach.

Most company-connected IoT devices are, in turn, connected to the wider internet—to allow vendors to deliver updates, for example. Attackers, using standard scanning tools, can find those devices, and there are even search tools to help them (a Google for IoT hackers). Once found, connecting to those devices, and hacking into them, tends to be easy. They often have no built-in security, run on legacy operating systems, have weak default passwords, and are difficult to patch.

Even if a device isn't strategically important itself, it can provide intruders a way into systems that are. A vulnerability in a single device or database can compromise entire networks and operations.

Awareness of the risk from IoT devices has grown, certainly, but the threat hasn't diminished. On average, there is still substantial lag time—several months—between when a vulnerability is announced, and a patch issued, to when a device is made secure. Meanwhile, attackers have substantially improved their ability to exploit that gap.

A typical enterprise of 5,000 employees could have as many as 20,000 IoT devices, and there is now significant permeation of IoT devices across market verticals, including those that are highly regulated or that manage sensitive data and are likely to be considered critical infrastructure, including healthcare, energy infrastructure, government, and financial services. A presence of IoT within these industries is a

cause for concern, especially given studies that suggest a misunderstanding of IoT risks and an unpreparedness to manage them.

While they increase operational efficiency and help move operations into the digital world, any connected device becomes part of their networks, and brings with it security risks. For example, connected devices often use beaconing—repeatedly using their connectivity to call “home”—for a variety of reasons. While not inherently malicious, it does pose a risk for the device operator. Attackers can potentially monitor such devices for network activity and examine usage patterns, and it presents an additional attack surface that can be targeted if a device-specific exploit is discovered.

Securing data in transit from field devices to a cloud is one critical priority, but operators must also be sure that the cloud handling the data is secure and that the device itself is secure. Physical security is a critical part of network security, and unless there is a strict protocol for adjusting physical security as devices are added and systems are redesigned or reconfigured (as they often are), even the most highly fortified network assets can quickly become vulnerable.

Connected systems and increasing proliferation of IoT devices in environments such as healthcare and other critical infrastructure provides malicious parties new avenues to cause havoc or steal data. Attacks against IoT devices are already commonplace, from IP cameras with weak security controls to smart meters with basic encryption flaws. Device manufacturers do not always engineer security controls into their devices and, to date, the rush to deploy IoT devices at scale appears to be outpacing concern over their security implications. The European Union is working on legislation to make IoT more secure (the future “Cyber Resilience Act”) but by the time it is adopted, many objects will have been put on the market, which will not be subject to this Act.

Problematically, many IoT devices go unmanaged. They are connected to networks but outside of an operator's ability to control—or even see. A search for those devices inside a security management system may not even discover those devices exist. The existence of a vast network of hidden connected devices raises numerous privacy and security questions, and individuals concerned with security should expect that—as the number of connected devices explodes—many will be vulnerable to attack and prone to unintended consequences. Segmentation, along with a robust network infrastructure and strong policies and procedures, can help critical infrastructure withstand the threat that IoT presents, but it is only possible if all endpoints are mapped and managed.

There is much to be gained from connectivity, but much can go wrong. Global studies of energy and utility companies reveal that most have experienced at least one breach in the past year. They also suggest a lack of readiness. Most critical infrastructure operators fail to actively watch for advanced persistent threats, do not use state of the art technology to stop SCADA system attacks, and rely on a reactive, rather than proactive, SCADA security strategy.

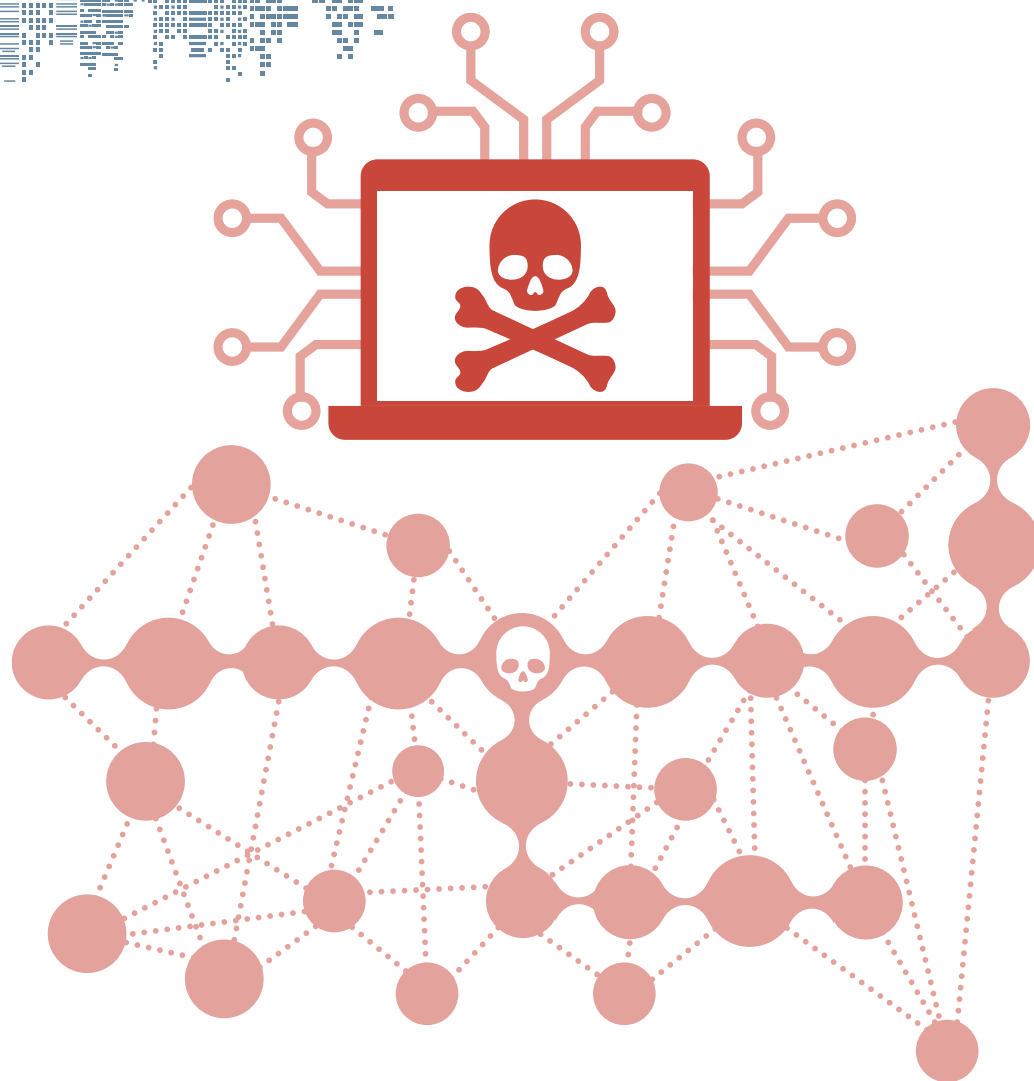
“Today you can destroy infrastructure at the touch of a button, that is the level of criticality of what we’re discussing,” explained economic advisor Pranjal Sharma as host of a panel discussion on securing systemically important critical infrastructure at the World Economic Forum Annual Meeting in Davos, Switzerland. “This is a common challenge for every government, every society, and anybody who is in the infrastructure business.”

“Today you can destroy infrastructure at the touch of a button, that is the level of criticality of what we’re discussing.”

Economic Advisor—Pranjal Sharma



- **Connected devices have shown an array of vulnerabilities in communication and other components that make them susceptible to remote attacks.**
- **The explosion in the number of devices being added to networked systems is exponentially multiplying security risk and increasing the number of ways attackers can gain entry into cyber-physical systems.**
- **With connectivity, the threat surface extends outside of secured locations and may link to critical operational and physical systems.**



E. “Hybrid” or “Blended” Threats

Imagine network hackers discharging millions of liters of sewage from a thousand miles away by tampering with remotely controlled valves over IP. Or weak physical building security, combined with connectivity in unoccupied workstations, providing an adversary a cheap, effective, and anonymous opportunity to hack an energy company’s distribution network.

These threats—born from the networking of critical infrastructure—may go by any number of names, including converged, hybrid, or blended threats. **They arise from unauthorized physical penetrations resulting in hacked information or operational systems or network hacking that creates a physical harm.**

While some fanciful scenarios are strictly the stuff of movie plots—like remote hacking of a prime minister’s pacemaker device—linked attacks are both real and a growing risk. Extremist groups and activists actively discuss using blended attacks against critical infrastructure, including energy and utility plants, transportation systems, and corporate buildings; attractive targets include vital systems, such as those in plants that regulate valves, temperature, and pressure.

The growing trend to connect industrial control systems to other networks is a major concern related to the cybersecurity of critical infrastructure, and the risk has been drawn into sharp relief by both real-world examples of inter-linked attacks and in security tests, such as one in Australia of the world’s largest technology provider.

In the test case, researchers hacked into the company's building operations from which they were able to access numerous control panels, including those named "active alarms" and "alarm console," and easily cracked encrypted employee passwords, including administrator passwords. The intruders could see just about everything about the building, from floor plans to the layout of water pipes, and had the attack been malicious they could have installed malware to gain access to other building control systems linked to the compromised one. All that from exploiting a single unpatched vulnerability in the system's building management system platform.

Real world examples are numerous: In 2017, a virus penetrated the network of the world's largest container shipping company through a single computer's outdated accounting software, resulting in a disruption in operations across hospitals, power companies, airports, banks, and government agencies, and crippling the global shipping industry for more than a week. In 2019, hackers exploited a firmware vulnerability to cause a power grid operator's firewall to continuously reboot, leading to a communications outage. In June 2020, a group of 19 vulnerabilities known as Ripple20 impacted millions of connected devices, including smart home devices, power grid equipment, healthcare systems, industrial gear, transportation systems, mobile and satellite communications equipment, and commercial aircraft devices.

Penetration tests often highlight the immediate attention that converged threats warrant. In one, for example, a utility company hired a Red Team to assess whether its physical systems might be vulnerable to a network attack. They dug into organization distribution lists to obtain email addresses for employees possessing access to its supervisory, control and data acquisition (SCADA) networks and sent them emails about a potential reduction in benefits. Several recipients clicked on

a Web site link that promised additional information about it, which downloaded malware onto the user's machine that gave the Red Team the ability to take control of them. In less than one day, the utility company saw how attackers could gain access to disrupt, damage, or alter power production and distribution for an entire region. In a second test, researchers posed as maintenance workers were able to get inside a controlled facility and accessed a logged-on but unattended computer from which they could have carried out any number of attacks.

Complicating the security picture is that **most operators of critical infrastructure admit to being unsure whether or not they have ever experienced a physical security breach that resulted in a network attack or a network attack that caused a physical world disruption.** That uncertainty is a likely a reason that security executives on both the physical and cyber sides of the equation have failed to comprehensively address the threats.

What might a linked attack entail?

Researchers who study the possible strategic and economic consequences of attacks on critical infrastructure often express concern that operators are not thinking as creatively as determined adversaries are. While critical infrastructure has done much to toughen both physical security and network systems to withstand the damage that casual hackers or youthful troublemakers might inflict, there has been scant attention paid to protecting against more insidious schemes that determined attackers are likely to devise.

Many of these vulnerabilities involve attack strategies and aspects of information systems that have not previously seemed especially important from a security standpoint. For example, most IT network defenses aim to protect financial and personal information during Internet transmissions, but terrorists, for example, are more likely to carry out creative attacks

on data at rest. Such attacks could go undetected for several weeks and would be designed to maximize real-world damage from the cyber infiltration.

Unauthorized physical access to network servers is perhaps the plainest example of a hybrid threat, and while most servers today are well-protected, with strong physical access controls in place, security holes persist, and protection must be continually upgraded to meet new threats. Given their criticality, strong security solutions must be deployed to restrict physical access to server locations, such as requiring two- or three-factor authentication, including biometrics, and control must be maintained through physical penetration tests of network server rooms and other locations containing critical network components, such as network wiring closets.

The fact that a physical security solution can become a threat vector further exemplifies the threat. Even though they are designed to provide protection, connected security devices can create critical network vulnerabilities. A typical search will turn up nearly 300,000 surveillance cameras connected to the Internet, for example.

When security devices like video surveillance cameras or access control panels are connected to an organization's network, denial-of-service (DoS) attacks against the network can render such systems and devices inoperable, or remote attackers can potentially gain unauthorized access to them and function as authorized users. **The network attack can have real-world consequences, with attackers using them as a springboard to attack industrial control systems or to make possible a physical infiltration of a critical infrastructure facility.**

Critical infrastructure operators must evaluate whether their network defenses are too singularly focused on mundane threats and vulnerabilities and if strategies must widen to protect against creative blended threats. These may include:

- Inserting malware to alter manufacturing specifications and other business processes. For example, an attack on a critical manufacturer could result in machines that burst into flames after being in operation for a specified duration or could also result in defective products.
- Altering information to cause public hysteria. Adversaries could target any number of sensitive systems in healthcare, for example, to alter medical data such as dosages or treatment schedules. And then announce it to the public to cause widespread panic and disrupt financial markets.
- Gaining physical access to systems to alter codes to create public chaos. In one real world incident, striking traffic engineers infiltrated a city's traffic light system, fooled with programming codes, and caused dangerous traffic snarls throughout the city.
- Compromising vulnerable electronic vehicle charging stations to potentially disrupt the larger energy grid.

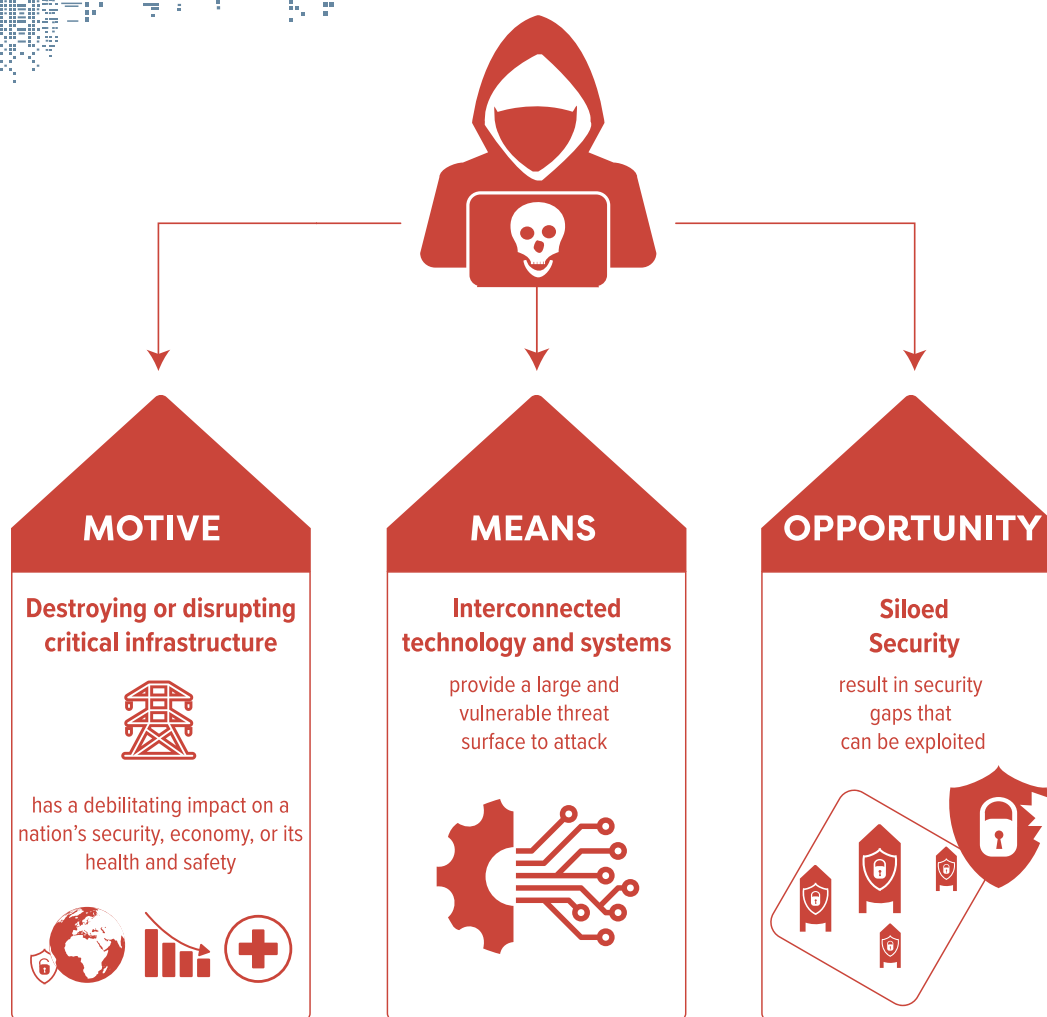


Interconnected technology is a threat vector for converged attacks on critical infrastructure, and vulnerability primarily stems from the failure of global critical infrastructure to examine how physical and cybersecurity threats intersect. Networked transformers, for example, are designed to withstand operational risks such as lightning strikes, hurricanes, and network power fluctuations—but they are extremely vulnerable to intentional physical attacks. **Leaders in both security disciplines—cyber and physical—must examine how physical security vulnerabilities can result in system breaches and how cyberattacks can create physical harm.**

Critical infrastructure operators must do more to account for the broadening scope of emerging threats and the combination of physical and cybersecurity threats. Although blended physical-cyber threats are not new, much of the world's critical infrastructure is simply unprepared to handle such multilayered threats. Time and again, huge vulnerabilities are discovered at critical infrastructure companies that claim to be fully compliant with all existing standards.



- **The trend of connecting industrial control systems to other networks is a major concern for the security of critical infrastructure.**
- **From a physical or network intrusion, it is possible to create untold havoc, from taking over entire smart building systems to disrupting the basic services societies need to function.**
- **Physical and cybersecurity threats now intersect: vulnerability in one area provides a means for attackers to do damage in the other.**



F. Vulnerability from Security Silos

When two things are pieced together to form a new whole, its weakest spot is often the glue holding its two halves together. This is something criminals know and exploit, so it is understandable why blended/hybrid threats have become a primary source of security weakness at the world's critical infrastructure. Additionally, it's why the silos of security responsibility that exist at critical infrastructure are a leading cause of unrecognized vulnerability and unmitigated threats.

Security is a patchwork: consisting of physical security, operational security, cybersecurity, and subsets like people security and crisis response. One group may have responsibility for protecting employees and visitors, while another conducts facility management, and yet

another conducts patrols, investigates offenses, and responds to incidents.

The security threats faced by critical infrastructure crossover between all these disciplines, as well as others, a fact that is generally understood; yet the goal of holistic security management has not been attained by many infrastructure owners. Why is this the case?

At the root of the problem are silos of security, and it is understandable how they evolved. There has been a rapid expansion in the type of assets that need protecting, from traditional physical assets to intangible ones, like information, data, and reputation. As new protection requirements have formed, new teams have been created to develop strategies and



implement solutions. But as new teams formed, they typically had a narrow focus on the emerging area of security risk, and devised strategies independent from other security functions and without regard to how they aligned with existing strategies, including those of physical security teams. Each addressed their piece of security risk without much thought to how the entire “security puzzle” was coming together.

It is necessary to remove barriers between security functions, as vulnerability often resides in the lack of coordination between the various owners of security, including physical security, IT, and others. Additionally, failures of a weak link in a connected system can reverberate to all parts of it, a fact that underscores the need to account for interdependencies in protection disciplines.

To bolster the protective shield against security threats, all departments that perform security risk reduction activities need to work more closely together—something that decades of “security silos” makes a challenge.

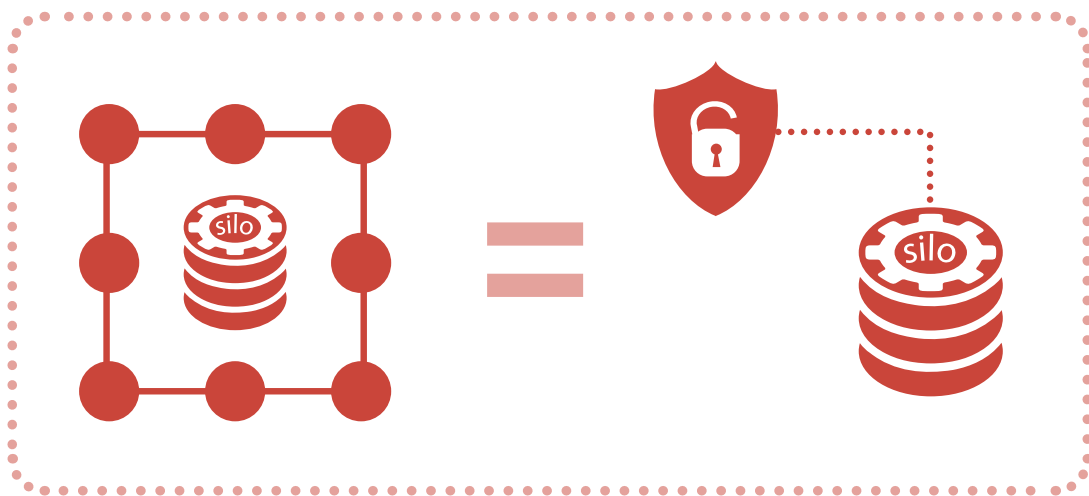
What are some of the obstacles?

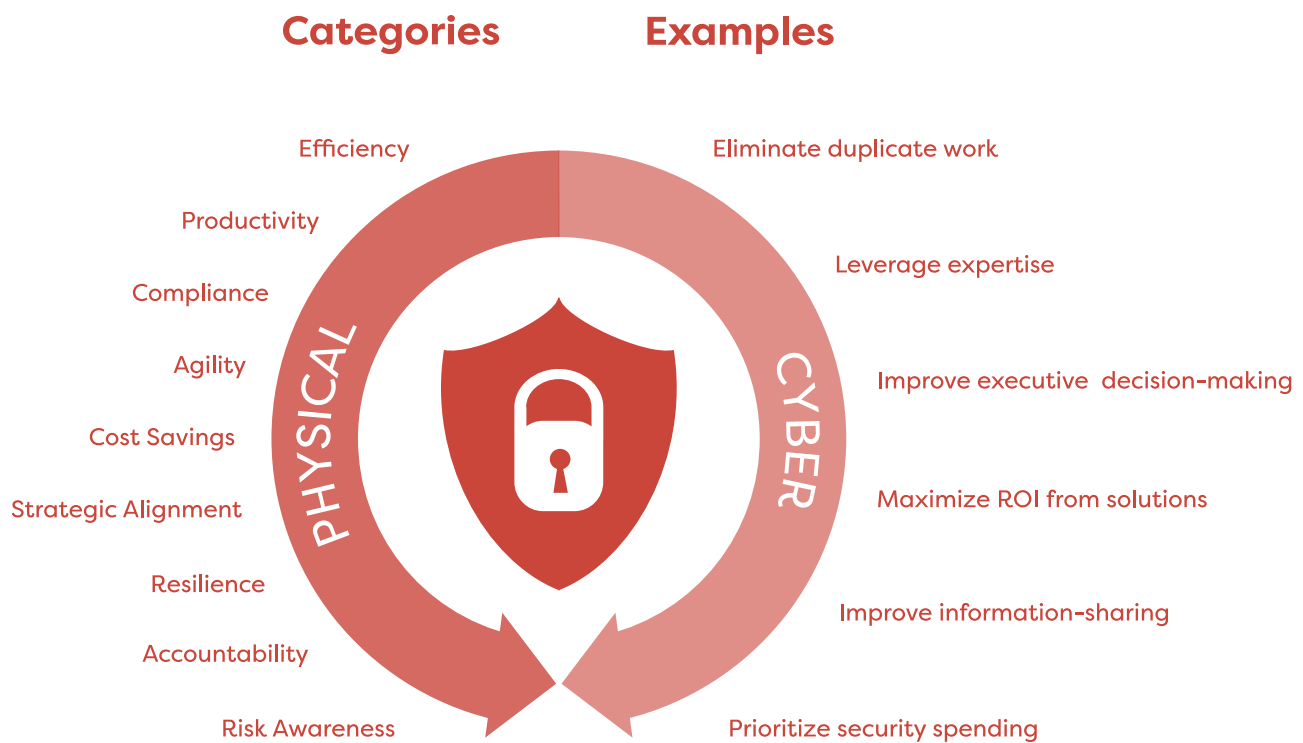
- Perspective is often at the core of problems. Depending in which functional areas practitioners perform, the very idea of what “security” means will vary, complicating the ability to forge a broader view of security that supplants it. Creating a new mindset—so when organizations think about security strategy it brings up the broad spectrum of what that means—requires new approaches.
- Physical, operational, and IT security solutions are often very different, with differences in design, functionality, implementation, maintenance, and management.
- Breaking down security silos is a multifaceted challenge that includes technical, organizational, and skills-based issues. For example, when special systems or devices are added to the IT infrastructure, the owner or end-user must ensure necessary information is given to expert systems personnel who can help integrate it into the IT infrastructure and who will be needed for systems management, networking, and change processes.
- Key people may be missing in driving connectivity projects forward. While personnel related to physical-cyber projects may dutifully concentrate on their aspects of it, there is often a lack of big-picture analysis for how to maximize benefits and minimize risks from connecting various special systems and devices. Or risks may go unaddressed because those who conduct systems training are not well versed in the risk from hybrid threats.
- When there is a lack of understanding of who is responsible for which data and processes relative to connected and integrated systems, it can thwart important aspects of planning that would otherwise help to bridge several functional areas.
- If different departments resist coordination for fear of losing power (turf wars), it can be impossible to reach cooperation on security issues.

It is well-established that criminals need motive, means, and opportunity. While connected systems provide motivated attackers the means to conduct hybrid attacks on critical infrastructure, it is siloed security functions that provides the opportunity: vulnerabilities and gaps in security emerge when physical and cybersecurity are managed in isolation from one another. Thus, there may be nothing more important for the security of the world's critical infrastructure than to evolve to a more systematic and comprehensive approach to asset prioritization and protection.



- Security siloes—in which aspects of security are managed in isolation—remain commonplace.
- Vulnerability often resides in the lack of coordination between the various owners of security.
- Addressing the risk of hybrid threats requires a dedicated effort to break down security siloes and overcoming barriers to coordination.





G. Benefits of Security Convergence

When a critical infrastructure owner manages security threats in isolation within specific enterprise functions—rather than addressing them from a comprehensive perspective—it can't:

- accurately set priorities,
- focus on risks most capable of doing harm,
- address vulnerabilities of connected physical-cyber systems, and
- it can't leverage full value from protection investments.

Strategic security convergence—approaching the whole of security tactically as opposed to a security posture merely being the sum of its parts—allows critical infrastructure to make smarter decisions about protection and risk mitigation. Rather than each function addressing risks on its own and hoping they align, a paradigm built on convergence gives infrastructure operators better insight into how countermeasures can combat threats. Because risks from an operational perspective are interdependent, security convergence, by eliminating those silos, is better able to address threats.

From an organizational perspective, a convergence approach to security risk yields significant value by placing different assessments of risk—physical site surveys, IT audits, and so on—into a common construct. It normalizes discussions of risk so senior executives can make decisions with a complete understanding of security risk. This is imperative, as the same level of protection, or the same level of security spending, can't be simultaneously maintained for each business unit, much less for every component within business units.

A convergence approach also encourages practitioners to recognize that protection in their domain is not the totality of the security challenge—that security in their function is just one part of the greater need to secure operations and ensure resiliency. It will always be important for functional executives to devise robust physical or IT protection strategies and ensure their departments effectively carry them out, but the move to have “security” encompass protection from all non-routine risk helps all those in different disciplines recognize the value in teamwork and inter-departmental cooperation.

Convergence of physical and cyber security strategy also helps to drive critical infrastructure to meet a goal broader than just security: that of ensuring operational resilience. Beyond the specific security risk-countermeasure paradigm, security is one element of many that is necessary to ensure uninterrupted operations. This recognition—that from operational perspective it is somewhat irrelevant whether harm is caused by terrorism or a tornado—can help drive cybersecurity and physical security into closer working relationships with other pieces in the resiliency puzzle: disaster response, crisis management, business recovery, health and safety, IT, and others.

Convergence success stories abound. Infrastructure firms are closing regulatory compliance gaps by integrating logical and physical access control; others

are saving tens of thousands annually by reducing duplicate database management; others are transforming countless unwatchable hours of video into data that is being shared and searched to improve operational processes; and others are deploying single solutions to similar problems and coordinating reporting and logging processes.

A joint physical-cyber security approach helps to cut costs by streamlining historically disparate security projects; improves productivity and speed of work by removing duplication; eliminates costly user support functions and reduces maintenance costs; eliminates inefficiencies, such as duplicative investigations conducted by HR, IT, and physical security, and increases the ability to demonstrate to those outside the organization that the organization meets mandates for physical security and cybersecurity.

Value of a converged security approach include:

- A security budget that reflects security priorities. One problem when security spending is within a siloed budgeting structure is that money for security falls in the hands of departments for whom security isn't a primary concern. A convergence approach ensures decisions about security spending remains in the hands of security leaders.
- Leveraging expertise. Specialized skills run in all directions, and a coordinated approach to security makes it easier to exploit and maximize the skills of different departments for the good of the common mission. Combining expertise during investigations, for example, makes them more efficient and effective.
- Regulatory assurance. Greater standardization in policies and procedures helps a critical infrastructure operator adhere to management standards to

facilitate regulatory compliance. A centralized security approach also provides accountability, which is a central element of most regulation. A converged security model puts the accountability for security all in one location.

- Personnel development and productivity. When a system is developed that in some way unifies everyone who performs security functions, career paths open for staff and it creates room for innovation, and to maximize people's skills.
- Better metrics. When security functions are embedded in the various activities of different departments, the goals and measures of security often only reflect the security needs of those individual departments. In a coordinated model, security metrics can help drive security improvements that benefit the entire operation and align with the goals of the entire organization—not its various units.

For better security, finances, and efficiency, operators of the world's critical infrastructure need to adopt a mechanism for achieving visibility into the full spectrum of threats they face and coordinating protection activities.



- **A joint physical-cyber security approach allows for strategic alignment of the two functions and reduces security risk.**
- **Other benefits often flow from security convergence, including enhanced productivity, efficiency, and regulatory compliance.**





H. Security Convergence Framework

Most organizations have a multitude of specialist functions designed to protect them. The challenge is to unify, align, and integrate the management of these myriad protection-related activities. For many operators of the world's critical infrastructure this requires leadership from a new perspective, one that serves to overcome the silos of security responsibility that can lead to unrecognized vulnerability.

An optimally efficient asset defense demands the blurring of physical and cyber security, but what is the model of this new security blend?

A collective defense approach requires recognition that security is truly a shared responsibility between many stakeholders, and several useful strategies

and frameworks have been developed that organizations can follow to help unify and coordinate their activities. A structured approach is important to enable communication across security functions; identify linked cyber-physical risks and vulnerabilities; align security policies, goals, and spending; and coordinate incident response.

Each organization must follow a process and adopt framework components that best suit the risks they face, the regulations to which they must adhere, and their unique business and operational goals. But while the “how” will vary among critical infrastructure organizations, the goal of improving coordination among security functions should be universal.

A serviceable convergence framework will function as a vehicle for coordinating the many facets of security risk management, which includes physical security and cybersecurity, and help organize and align disparate self-protection programs. Once a security convergence framework is adopted, the security activities that flow from it are more likely to recognize that critical infrastructure protection is like an ecosystem that requires defensive activities to work together to collectively defend the interests of all stakeholders.

Without a defined process for coalescing the many slices of the protection pie, gaps in the security shield are more likely to develop. By following a framework that drives security convergence, critical infrastructure can be more proactive about its security defense, rather than simply addressing whatever hole was most recently exposed. An effective security convergence framework will also:

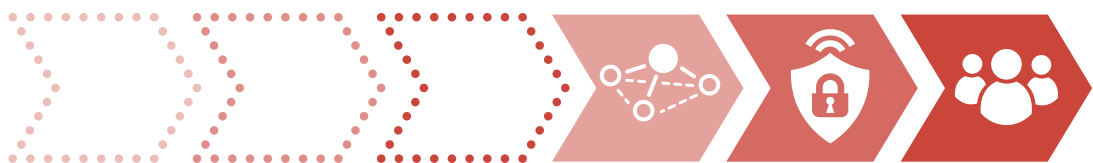
- Clarify responsibilities,
- encourage accountability,
- minimize turf wars,
- raise the profile of security issues within the organization, and
- serve as a tool to communicate to internal stakeholders about the “protection ecosystem” and its interdependencies.

For the benefits outlined above, it is useful for critical infrastructure operators to embrace a comprehensive approach to security and create a structure that will serve to unify protection activities.

Since systemic change can be daunting, some operators find it useful to jumpstart cyber-physical security alignment by focusing on specific benefits from improving coordination between protection activities—such as cross-training or eliminating duplication of effort. While this can provide an avenue into coordination, first steps must also include a willingness to conduct an honest self-assessment, according to Felipe Bayon, CEO of Ecopetrol Group, Colombia’s leading energy company which operates pipelines, refineries, and transmission lines across the Americas.

At Davos 2022, Bayon said they recently conducted such an exercise, taking a hard look at their security posture against the current risk environment. As a result, “we realized we needed to step it up and raise our game,” he said. For example, operators must assess whether they have the right skills, expertise, and capabilities to initiate a more coordinated approach to security.

It also requires widespread buy-in. Forging an integrated approach to security is a significant undertaking involving many vendors, systems, stakeholders, and locations, so a firm must gather support for a project of that magnitude.



As noted, no one framework can be the right fit for all critical infrastructure operations, and companies are certain to approach the integration of resiliency functions in different ways. At some, the nexus of coordination may be risk management. At others, it may be business continuity, a combined physical-cyber security department, or some other discipline. Regardless of the particular structure, an effective paradigm will typically have several elements in common.

First, it is likely to be a top-down process, capable of exerting guidance and control over all aspects of security—regardless of which department it is embedded in. This helps to ensure that someone is accountable for all aspects of security, and that each is being carried out in accordance with company principles and its strategic goals for protection.

Part of convergence is to look at individuals and functions who carry out security activities and to combine ‘like work’ into a centralized model. Previously separate responsibilities will typically align under some sort of central security organization with budgetary and operational authority. Such a group can then consolidate and prioritize the organization’s security spending; find ways to extract full value from new technology; align policies and procedures; set goals and track progress through companywide security metrics; provide security oversight; and report to key stakeholders.

Another likely feature is a more significant role for security risk management to guide activities, one that focuses on proactively managing security risk in a preventative, organization-wide manner, while removing the fragmentation and inefficiencies of responding to individual security events as they occur.

Additional governance and oversight to security activities is another necessary component. While security management helps ensure that the functional aspects of security—policies, processes, and the like—are operating effectively, an added layer of governance helps an organization work together to create a culture of accountability, one that allows for effective security management throughout the company. Importantly, the framework will facilitate consistently effective security management—providing the foundation so that security risk can be addressed even as everything about it is changing. Evolving technology, the interdependence of technologies and risk, and changes in the relative value of corporate assets is creating a very dynamic threat environment.

An effective framework will also:

- Identify basic guiding principles—for inclusion, transparency, compliance, ethics, measurement and reporting, and risk management—to which everyone who manages elements of security risk knows they must adhere.
- Thoughtfully address the issues of roles and responsibilities and separation of duties. A process for assigning, evaluating, and ensuring that all aspects of security are addressed will prevent unaddressed gaps in protection.
- Be a platform upon which future coordination can be built. Thinking of security risk as having two components—physical and cyber—does not capture all the complexities of security risk and may sell its importance short. Convergence of physical and cyber security strategy can be part of a process that encourages an integrated approach to risk that is as comprehensive as the organization needs.

An integrated effort to mitigate security-related risk is foundational to a more strategic and robust approach to critical infrastructure security, providing a structure to prepare organizations to handle all aspects of security, regardless of what department has responsibility for it, the type of threat, or how they change. It recognizes that a more comprehensive, progressive, and proactive approach is now required to defend critical infrastructure in an era of connected systems, hybrid threats, and determined adversaries.



- **Critical infrastructure entities should adopt a framework to unify, align, and integrate physical and cybersecurity and facilitate better coordination with other resiliency functions.**
- **Understanding and assigning responsibilities, strategic alignment, and oversight are critical elements of an effective framework.**
- **An integrated effort to mitigate security-related risk is critical to protect critical infrastructure security in a world of interdependent risks.**

About the Author:

Garett Seivold is a career security journalist who writes for the International Security Ligue.

Section II.

Issues in Physical-Cyber Security





Prospective Analysis of the Private Security Industry

Challenges for the private security professions in the next ten years

The world of private security has evolved considerably, driven by the ever-increasing security threats and, on the other hand, by a proximity that is getting smaller every day with the internal security forces.

The evolution of the private security sector—and thus its ability to help protect the world's critical infrastructure— is characterized by two strong trends.

A widening of the field of competence

The first is an irreversible widening of the field of competence of private security companies at national level, with an adapted regulatory framework.

On a daily basis, security and health threats are growing and law enforcement agencies at national and local levels are obliged to refocus on a number of missions.

This means that private security will become increasingly present in the public space, and that certain missions, such as the recording of offences, thefts in shops, violence against people visiting shopping centers, could be entrusted to them.

This is already the case for rail transport, in the same way as it is already possible for security companies to carry out (in certain cases and with a specific authorization of the State representative) their security mission in the public space.

Even if it takes time, because of institutional brakes or corporatist reactions, the trend is confirmed.

The fact is that Private Security Companies (PSCs) already provide protection and security services to a wide range of public areas and buildings: shopping malls, restaurants, cinemas, stadiums, airports, trains, urban public transport, leisure centers, beach and mountain resorts, etc.

The growing emergence of technologies

The second trend is an increasingly strong technological mix.

While there has been much talk of the security guard of the future as an “augmented guard”, there is no doubt that they will be much better equipped. New technologies will facilitate their missions by allowing them to better understand their environment. **They will have access to real-time information and the integration of data will allow their operational management to free themselves from administrative tasks, so that they can be even more present in the field and closer to their clients.**

Artificial intelligence in the field of behavioral and facial recognition will complement the training currently provided to agents, as training will be a determining factor in the ability of security agents to evolve in a world protected by more effective security technologies. The detection of “risky or non-compliant” behavior will help avoid conflict or criminal situations. Sound detection (screams, cries,

specific noises) will also improve the speed and efficiency of interventions to make public spaces, such as shopping centers, safer and more pleasant.

In shopping centers, for example, the Security HQs will become real operations centers dedicated—even more than today—to supporting the agents deployed and to protecting the technical areas.

Private security companies will have to build a hybrid security offer (human-technology) for their clients, driven by digital hypervision platforms, capable of managing security operations and of providing significant added value in terms of incident or crisis management. By analyzing the information collected and the incidents dealt with, these tools provide a predictive capacity that makes it possible to anticipate the times and places where possible incidents may occur. The services are therefore programmed accordingly, and the security teams are deployed by managing human resources as accurately as possible.

Beyond these technical developments, the private security sector is also undergoing structural changes

The concentration of companies is increasing, and many of them are moving towards the integration of a diversified offer. **Private security companies must now cover a wider spectrum of the value chain, from business expertise to the integration of security systems, in addition to a traditional human security offer that is increasingly professional and efficient.**

Thus, in addition to the human skills expected by the clients, they must commit to a holistic approach to their security offer. They must position themselves vis-à-vis their clients in the same way as they apprehend their risks, be able to anticipate their security problems and work out appropriate solutions with them. Indeed, the security threat is three-dimensional and must be addressed as such.

A holistic approach, innovative partnerships

The holistic approach allows us to combine know-how in human security with the ability to integrate innovative technologies to meet the needs of the client, including the cybersecurity dimension. We are convinced that this evolution will result in the creation of shared value between security companies and clients, by offering clients a quality of service that goes beyond what is done today.

About the Author:

Jean-Philippe Bérillon is an experienced security expert with a deep experience in several regions of the world and sectors, including energy and private security. He is the Head of Security of the DPD Group and chairs the CoESS Committee on Critical Infrastructure Protection.





2.

Towards an Integrated Vision of the Cyber and Physical Governance of Organizations

Cybercrime costs are constantly increasing, and the simple analysis of attacks shows that all vectors are used to penetrate the defenses of companies or institutions, with a strong creativity.

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching \$10.5 trillion USD annually by 2025.

Administrative or industrial computer systems are still the growing targets for these criminals of the digital space, but electronic security systems are not spared. **In a world growing more interconnected than ever, organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats.**

The human target will remain the preferred one, whether (s)he is an employee, a consultant, or a company contractor, and for the same reasons private security companies have no other alternative today than to reinforce the training of their officers, to sensitize and prepare the operators of their SOC and their PC operations to cyber-attacks. The quality of the service thus offered will lead to better staff qualifications and therefore an upgraded security service.

And it is also why the journey towards more integration of security and surveillance technologies in the combined offer of private security, human-technology, is today the perfect expression of this.

Video surveillance systems, access control, surveillance robots and drones are, or will be, the next targets of cyber criminals.

All this shows the technical convergence between cyber security and physical security. But if we set apart the technical aspect and focus on the organizational aspect, we can see that organizations still operate in silos. However, it is the nature of cyber security as well as physical and human security to be transversal, as it impacts all aspects of a business, including strategy, production, business development, supply chain, staff and customer experience.

The key role of the CSO

This means that the collaboration between Chief Information Officers (CIO), Chief Information Security Officers (CISO) and Chief Security Officers (CSO) is not adapted to the challenges of the cyber threat. The problem of the CISO being attached to the CIO, which is almost the norm today, may be seen as an inefficient organization. As the person in charge of controlling the security of systems, his/her independence from the CIO should be more natural, and a different reporting is to be preferred, such as to the CSO for example.

In addition, the CSOs are already in charge of the operational management of private security companies. They are also actors in the field of defining specifications for the physical security of the sites, the processes to be elaborated and set up, and identifying appropriate technologies for the protection of their sites.

In many cases, the CSO directs the calls for tender for the maintenance of electronic security systems, access control, and surveillance, towards a preference for security companies that can operate these systems as well as ensuring their maintenance and that have the capacity to integrate security technologies.

The choice to attach the CISO to the CSO is motivated by the greater transversality of the profession of CSO and because this transversality better integrates the difficult subject of human behavior approach, as human behavior is most of the time the weakest part of the defense line that organizations must build.

This would bring the collaboration between these two protection managers, the CIO and the CSO, closer together. Organizations no matter how big or small, critical, or not critical, can pursue convergence by developing an approach that is tailored to the organization's unique structure, priorities, and capability level.

Breaking the silos

More than just an observation, it is a real concern to continue dealing with the physical and cyber threats independently. It also shows the inability of organizations to rethink their model, and to review their governance in this area. **The fact is that one cannot provide good cybersecurity without robust building security, or if both the cybersecurity and physical security teams continue to be siloed.**

When it comes to critical infrastructures, the stakes are even higher. Not dealing with the threat with a homogeneous organization leaves room for vulnerabilities in the gaps that criminals or anyone who wants to attack the company can exploit to penetrate the sites or systems. These vulnerabilities are as much a matter of protecting industrial or management IT systems as they are of physical and electronic security devices.

Furthermore, attacks are becoming combined: insider threats, physical intrusion by neutralization of electronic security systems, cyber-attack. It is therefore necessary to have an approach capable of combining skills to ensure a global and converging approach to security, an organization based on a holistic approach to understand the threat.

It is this convergence that will enable organizations to be decompartmentalized and to give coherence and robustness to the protection systems that they need today.

It is therefore necessary for organizations to evolve towards a convergent construction of security with one single head. It is indeed an integrated governance of security that companies in general and critical infrastructures in particular need, i.e. security of people, industrial and administrative IT networks, and physical security of sites.

This model of mature organization, which integrates homogeneity and holistic approach, provides a greater reactivity and efficiency, which also translates into a stronger security culture of the organizations. We are firmly convinced that such organizations are better able to provide more effective defense and faster reaction to increasingly sophisticated and combined (physical-digital) attacks.

This vision of a Chief Security Officer sees a unique head in charge of this global area that will become a single point of contact for executive management, security agencies, or any other organization executive to have a quick call with when concerned by any transversal and urgent security question.

About the Author:

Jean-Philippe Bérillon is an experienced security expert with a deep experience in several regions of the world and sectors, including energy and private security. He is the Head of Security of the DPD Group and chairs the CoESS Committee on Critical Infrastructure Protection.



3.

Reimagining Public-Private Partnerships to Enhance Critical Infrastructure Resilience

The title of this chapter is slightly misleading, in that public-private partnerships are not (yet) areas that are very well defined. PPPs, in the context of this paper, are partnerships between an agency of the government and the private sector in the delivery of goods or services to the public. A recent CoESS comparison of the legal frameworks that govern private security in Europe shows that only 40% of the 30 European countries surveyed have such partnerships in place. These are generally local agreements, which are therefore limited and are not subject to clear frameworks or references.

In a White Paper on “The Security Continuum in the New Normal” published in 2019, CoESS calls for such frameworks to be created, and proposes guidelines and recommendations to build successful PPPs based on concrete cases.

The fact that, so far, PPPs do not benefit from a clear framework, gives the opportunity to build in the Cyber-Physical Systems (CPS) dimension from the outset and to recommend a holistic approach from scratch.

The CoESS recommendation for PPPs looks at various aspects from the private security companies' side, articulated around the 4 values of CoESS: safety, compliance, quality and trust.

Safety ⇒ Legitimate companies

- Licensed guards
- Working conditions & equipment
- Well selected
- Adequately trained for the job/environment

Compliance ⇒ with:

- Legislation in place
- Fiscal, social, administrative obligations, collective agreements
- Recognised standards and certifications

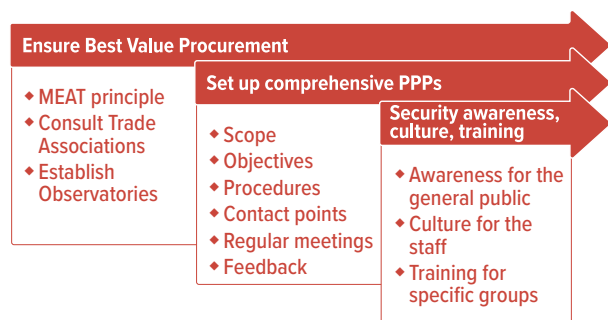
Quality ⇒ Following the Best Value procurement approach

- Select PS providers based on best value, not on lowest costs
- Quality > 50% and >60% in CI

Trust ⇒ Validation by a relevant and representative association/chamber

- Clear description and understanding of roles
- Communication
- Plan Do Check Act ⇒ feedback and improvement
- Security Chain Mindset
- Framework for the exchange of information

Once established, CoESS gives the following recommendations to ensure that the partnerships work:



Note: MEAT stands for Most Economically Advantageous Tender. It is a method of assessment that can be used as the selection procedure, allowing the contracting party to award the contract based on aspects of the tender submission other than just price.

For the sake of successful PPPs that enhance Cyber-physical security, the following points deserve special attention:

- Ensuring that the Private Security Company (PSC) is selected on quality criteria over price. CoESS advocates in favour of having at least 60% of the contract awarded on quality criteria for Critical Infrastructure, and has developed a tool to objectively measure them in a manual jointly developed with the Trade Union UNI Europa and with EU funds.
- The criteria to measure quality include compliance with legislation and relevant standards, such as the standard system for PSCs in CIP, EN 17483.
- Careful selection and training of the security officers is very important but will not be sufficient. It has been demonstrated that good management practices are the foundation on which a good security culture can be built, an important step to mitigate Insider Threats, which in turn are a significant vector of cyber-attacks. While disgruntled employees may intentionally carry out or support malicious attacks, accidental Insider Threats may result from insufficient training, and negligent Insider Threats

may be the consequence of low security culture.

- The roles and responsibilities of the public and private partners need to be well described and mutually understood to ensure the continuity and solidity of the security chain. **A common security chain mindset is essential, and this requires training in and awareness of cyber-physical threats.** A vast majority of cyber-attacks comes from human intervention, physical or otherwise, and can be avoided with simple measures and awareness campaigns.
- Determining the scope, procedures and processes of the partners is also very important to secure the chain and explaining the purpose of their existence will go a long way in ensuring that they are well implemented.

In the White Paper, CoESS also highlights that, too often, the “exchange” of information is a one-direction exercise.

In cyber-physical security cases, it is even more crucial that public authorities communicate to PSCs about any suspicion of malicious activities or heightened threat. Without divulging any secret information, it may be very helpful to send early warnings to PSCs about suspected physical breaches or cyber-attack attempts. As emphasized by CoESS on several occasions, the risk of not communicating is likely higher than the suspected risk of divulging information.

In conclusion, both parties in PPPs have a lot to win by adopting a common and shared cyber-physical security policy in the protection of Critical Infrastructure, and this will most certainly benefit both parties, as well as society as a whole.

About the Author:

Catherine Piana has been the Director General of CoESS since 2014 and of ASSA-i since 2016 and the Chairperson of the CEN's Technical Committee TC 439 “Private Security Services”.



4.

Convergence of Physical and IT Security in Critical Infrastructure, Great! But what about OT?

Introduction

Our contemporary society is increasingly digitalized. Over the years this has brought humankind lots of value, prosperity and wellbeing. The downside, or dark side as you will, is, however, also becoming more prominent. Digital incidents, resulting from both accidents and malicious intent, are in the news on a daily basis. Government cybersecurity agencies, institutions and cyber experts are warning of digital disruptions that endanger the continuity of organizations and society. Nowadays every process is depending on digital (IT) infrastructure and there are hardly analog alternatives if the digital systems fail. Even critical infrastructure itself is completely depending on the digital infrastructure.

The bright side is that all participants in society are becoming increasingly aware of the interdependence and risks. Private individuals, organizations and governments are extending their cyber defenses and are building up resilience.

The professional security domain, dealing with this ever-evolving new reality, is unfortunately still very siloed. Physical security professionals are primarily concerned with physical threats, IT security professionals deal with cyberthreats. These two domains share a common interest in security risk management and even share similar risk management processes. Nonetheless, they have a different background, specific threats and controls, and even a different language. In recent years these domains slowly reached out to each other and started to get familiar. Over the past decade hybrid threats, combinations of physical and cyber threats,

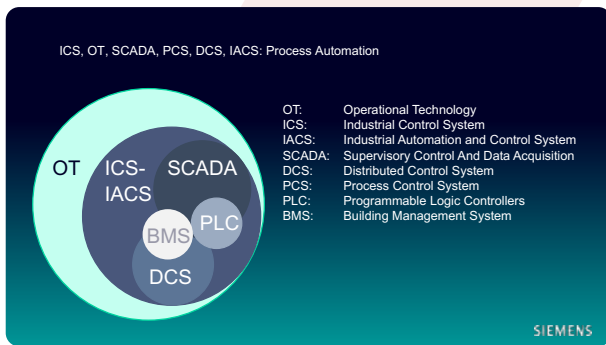
evolved, driving the convergence of these domains.

To complicate things, there is a third security domain that desperately needs attention: OT security. This paper will briefly introduce this domain and detail some specific characteristics of it. **OT security closely relates to both IT and physical security and a holistic security strategy cannot go without a proper understanding of it.**

OT, what is it?

OT is the abbreviation of Operational Technology. It is the twin sibling of Information Technology (IT). They both represent the digital world. IT, as the name indicates, focusses on the creation, processing, storage, security and exchange of all forms of information and electronic data. The primary goal of OT, on the other hand, is to control equipment influencing the real world. These systems are known as Industrial Control systems (ICS), SCADA systems, Industrial Control Systems (ICS), Industrial Automation and Control Systems (IACS), Building Management Systems (BMS) etc.

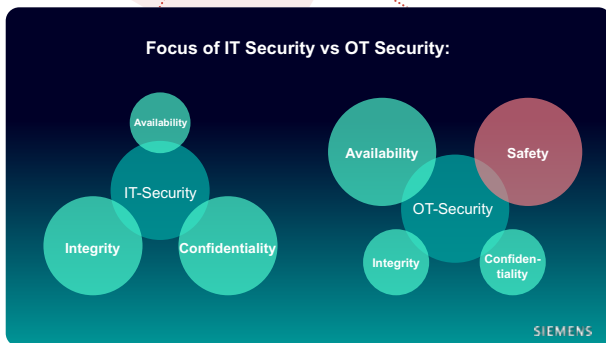
This domain ranges from (industrial) process automation, transportation systems, automation control systems all the way to smart grids and smart buildings. These systems are referred to as cyber-physical systems, they connect the digital world to physical sensors and actuators interacting with the physical environment. Physical security systems like video surveillance, intruder detection, access control and alike, are also part of the OT domain.



Most often, the convergence of physical and cyber security concentrates on the convergence of physical and IT security, forgetting the OT domain.

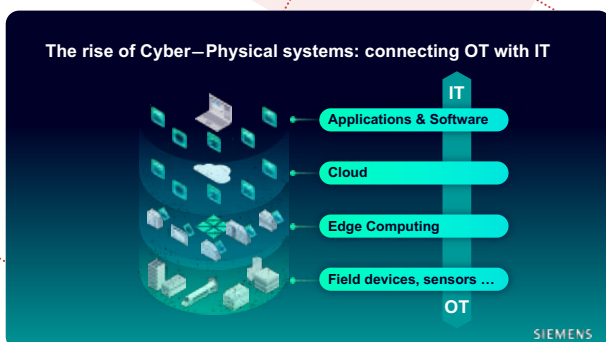
The OT domain is traditionally managed by the operational departments. They are responsible for keeping the organizational processes running. Their focus is system availability and to reduce (unplanned) downtime. As their processes are physical by nature, keeping people and the environment safe is a prime concern. Real-time interaction is essential for OT systems, for example: pushing an emergency stop button needs these systems to respond instantaneously. Delays and latency are not acceptable.

IT vs OT: what's different?



The IT domain, with its focus on information and data, is primarily concerned with the confidentiality and integrity of information. Availability of information is most often less critical and latency and even short downtime is acceptable. In the IT domain safety is usually not a topic of concern. In corporate environments, the IT department is usually concerned with the office IT. They are usually unaware of any OT systems in their network or they simply create a separated 'technical network segment' for it, so they will not be bothered with OT. Most of the time, OT is not considered the responsibility of an IT department.

The OT professionals originally managed automation systems that were not connected to the outside world (back in the days IT and the internet did not exist yet). They are still of the opinion they are running a powerplant/production process/bridge/building and it never crosses their mind they actually are running OT systems that are interlinked with, and even partly consist of, IT equipment.



The fortunately growing number of IT professionals that are confronted with OT systems do not understand or do not accept that OT systems have some peculiar characteristics to deal with. IT professionals, for example, are used to keeping their systems up to date and upgrading and patching their software on a regular and very structured way. Upgrading software of OT systems is, of course, possible and recommendable; it might however, implicate that the entire OT system needs to be tested end-to-end to make sure all safety features are not affected by the upgrade and function as needed. Migrating the process automation software of, for example, a powerplant thus might be not possible (it cannot be shut down) or very costly due to extensive testing. **A growing number of organizations, especially in critical infrastructure, are merging IT and OT departments to get them to cooperate.**

So, what about physical security?

Nowadays organisations and their higher management are increasingly aware of the importance of IT systems, data and information. Protecting these systems and their content has a high priority. Physically protecting IT systems is a no-brainer and usually focusses on the physical protection of datacenters, IT equipment rooms and network components. For IT systems, the physical components are concentrated in specific rooms and buildings and, thus, are easier to protect. Physical security is an integral part of IT security standards and norms. Physical security managers can easily incorporate these standards and guidelines in their security policies. Physical security systems are also prescribed and detailed in these guidelines. In this sense, physical security is an inseparable part of, and belonging to, IT security. As IT or cybersecurity nowadays is a boardroom topic (and physical security often is not) it makes sense for physical security professionals to jump on the bandwagon of IT security to put their profession in the spotlights and give it the priority it deserves.

OT systems are hidden in the operation of many organisations. They are of the utmost importance for specific operational departments and a part of their daily operation. They usually are not a topic of concern on their own. The physical set up of these systems differs completely from IT systems. The physical components of OT systems are controlling physical processes and their components are distributed all over the site. These components are not or only partly centralized and installed in less secured environments. Take for example a video surveillance system, the cameras are installed all around and even on the unsecure outside perimeter of sites, bringing network connections to the OT systems core literally outside your first line of defense. Physically securing these systems is a challenge due to their omnipresent components. The operational departments, generally responsible for OT systems, lack security awareness and standards and guidelines are less developed and implemented. The OT domain, specifically, needs a physical security perspective to get the security up to date.

To conclude....

Most often physical security is not a topic that is on top of mind in organisations and their board. Cybersecurity, in practice limited to IT security, however is. Highlighting the inseparable connection between physical and IT security can increase the relevance of the physical security domain. **Physical security of OT systems is still in its infancy, and this is an area of opportunity, particularly for critical infrastructure.** In our contemporary society, security is of vital importance, let's team up physical, IT and OT security to build a perfect place.

About the Author:

Johan de Wit is on the faculty at Delft University of Technology in the Netherlands and works at Siemens Building Technologies on future product development and security system design.



5.

Overcoming Barriers Between IT and Physical Security

Cyber and physical security are often treated in isolation, which raises questions of:

- Why is something so clearly beneficial as better coordination so uncommon?
- What can organizations do to help overcome barriers to better alignment?

There can be structural and technical barriers to getting cyber and physical security to work more closely together, but the greatest obstacle is oftentimes cultural. Any effort at collaboration is likely to bring together entities with distinct cultures and perspectives on their missions, and this can be especially true with security practitioners. IT security tend to come from a world in which innovation is most admired and a libertarian value system often prevails. Physical security may be comprised of specialists from law enforcement or military background and lean towards an authoritarian command structure.

Although leaders in both departments share the goal of conducting operations securely, convergence can be accompanied by a clash of visions, cultures, and expertise. The various entities performing security-related functions within companies all have “different points of view, different cultures, different career paths, different education, and even different vocabularies,” said a security leader at a port authority in the US.

Time has helped address some concerns, because while progress is slow, there is also a sense of inevitability around the removal

of security silos. Technology has also helped to bridge the gap somewhat, as it has become the heart of many enterprise security management processes and has fundamentally changed and united the way all groups do business.

Still, some operators of critical infrastructure may find it impossible to bridge the divide between security functions without specific, targeted efforts to encourage these distinct cultures to work together more effectively.

Creating common terminology for both physical and cybersecurity to use is one simple but popular strategy. By using a common glossary of risk management terms, operational and cybersecurity executives can communicate more effectively, and it may help improve collaboration in stubborn areas of coordination such as information-sharing.

As organizations identify the changes that are needed for developing an integrated security strategy, a potential clash of cultures should be an issue of consideration. When the city of Vancouver (Canada) took on the ultimate strategy integration—the merging of IT security and physical security into a single unit—the head of the combined department explained that understanding the different cultures that exist between the groups was the most critical factor for success. “During a consolidation effort, it is crucial to be cognizant that there are two groups of people who may or may not have an understanding of the other group’s functions, goals, or capabilities. It is critical to communicate to both groups and

explain to each how the two groups fit together, their similarities, and the benefits of consolidation.”

According to critical infrastructure operations that have fully embraced security convergence—and combined physical and cybersecurity operations to coordinate strategy—the most important management activities for implementing change are (in order):

- leadership alignment,
- communication strategy and execution,
- and organization design, including job and role profiling.

The issue of job design is particularly important for several reasons, including the fact that it is necessary to first understand how security responsibilities are managed before it is possible to implement effective change or develop an integrated strategy.

Successful convergence demands a baseline of understanding regarding who does what: for example, who oversees on-site crisis response? Facilities or security? How about policies and standards? Security or HR? What role does line management or legal counsel have in information security or investigations? While convergence is recognized as a way to improve security, the fact is that many organizations lack a clear understanding on exactly what role different departments already play in various security functions—an important precursor to improvement.

The issue of job design is also thorny because functional staff within traditional and information security specialties are often protective of their current roles, responsibilities, and intellectual property. Some may fear that efforts at integration may result in the loss of jobs or authority. Existing silos of security enjoy differing levels of prestige and authority within an infrastructure company; implementing change with those in mind may help to identify strategies that can minimize staff concerns and improve buy-in.

Hiring offers critical infrastructure with another opportunity to forge a more cohesive security operation, by selecting job candidates that have expertise in their specific domains but also demonstrate a capacity to appreciate security more broadly. For example, technology can help unite different protection disciplines, but only if staff has enough technological savvy to thoughtfully engage in discussions about how to make strategic, enterprise use of new technology to address common risks. Critical infrastructure should look to hire leaders who possess the skills and background to help serve the goal of enterprise security in addition to expertise in their respective domains.

Finally, while the road to security convergence may be long and challenging, there are approaches that may help jumpstart the process of better coordination:

- **Accept differences.** Information integration among all security stakeholders is important, but progress toward it can be incremental. **Instead of immediately dismantling silos and establishing new chains of command, companies can first emphasize building a comprehensive “situational awareness” capability,** in which executives from different groups can compare high-level information and look for trends. This is a useful way to build momentum for strategic convergence.
- **Build coordination around emergency planning.** Many critical infrastructure organizations do not have an oversight or umbrella unit that oversees all security risk. In its absence, however, there remain avenues to improve coordination; for example, via existing committees that deal with emergency response and business continuity. While these coordinating committees often owe their initiation to the need to manage a specific crisis, organizations increasingly use them as an essential tool for maintaining day-to-day preparedness.



➤ Socialize risk management tools and concepts throughout the enterprise. As noted, Human Resources, Information Technology, Information Security, Physical Security, and other security stakeholders may all speak a unique ‘language,’ but risk management may offer universal terminology (the ‘Esperanto’) that can help cross the cultural divide. It offers a set of concepts that can be applied to both physical and cybersecurity and uses tools that are relevant to the protection of physical assets, information assets, and operations. Importantly, risk management relates security to financial management, which helps senior executives to measure the value from security spending in relation to its benefits.

➤ Consider developing a single dashboard tool into which all functions that deal with security risk provide input regarding performance measurement. Such a tool can help organize security’s various parts into a greater whole and provides senior management with a high-level snapshot of the current security status for the entire organization.

Any critical infrastructure operation is likely to encounter barriers as they forge greater coordination between security functions. Identifying these likely obstacles, and developing strategies to overcome them, should be part of the plan for converging traditional and information security functions into a cohesive framework.

About the Author:

Garett Seivold is a career security journalist who writes for the International Security Ligue.



6.

Joint Risks Assessments and Penetration Tests

Risk assessments play a particularly important role in shaping a protection posture, as it is these examinations of threats, vulnerability, and potential consequence—against the existence of critical assets—that inform an organization what amount of risk mitigation is warranted and what level of risk it makes sense to accept. Many organizations have come to recognize the importance of security risk assessments and understand that if they are to effectively serve as the foundation for all security mitigation and prevention efforts, they must be accurate, detailed, frequently updated, and, critically, inclusive.

There are numerous risk assessment methodologies available to organizations, as well as tools to measure and assess different components of risk, and there is no single approach to measuring risk that is right for everyone. However, one important common feature is for risk assessments to bridge the false divide between cybersecurity and physical security.

Critical infrastructure operators can improve resilience by being systematic in their approach to physical security and cybersecurity risk and embracing common, formal risk assessment methodologies for both. Some of the benefits:

- Sharing risk assessment techniques helps to create consistency in calculating the impact of risks on the enterprise.
- Functional leaders can prioritize and support their specific recommendations in similar ways and uniformly communicate those risks to executive leadership.

- Senior management can have all operational risk presented in similar fashion for review, allowing for more informed and effective decision making.
- Organizations can forge a holistic understanding of risk and correctly prioritize protection measures.

Not all security risk assessments support a holistic approach to infrastructure security management, however. For example, risk assessments that only consider the direct impact of security events—and ignore their potential cascading effects—can obscure potential consequences and result in a lack of necessary security investment. Security risk assessments should examine both the direct consequence of a security breach or event and its possible downstream impacts to forge a coordinated approach to security risk management.

Case in point: A physical building intrusion should not be viewed merely as a weakness in building access control but also in network security if the unauthorized entry could have potentially led to a breach of data systems. This perspective acknowledges that individual security incidents, such as data theft by an employee, can have cascading effects and lead to compliance violations, monetary fines, unfavorable media reports, loss of public trust, lost business, and other harmful consequences.

Risk communication is an important aspect of making security risk assessments more broadly applicable. Specifically, while security risk assessments are often conducted to guide the decisions

by, and recommendations of, security professionals, communication with other stakeholders should be part of the risk assessment cycle. The outcomes of risk identification, assessment, and response should be conveyed to end users and operation process owners; for example, relevant results from a security risk assessment could be shared with power plant floor managers, to make them more security-aware, have them understand the range of threats they face, and to help them understand the interdependencies of security vulnerabilities and countermeasures.

A basic element in effective companywide security risk assessment is a comprehensive asset survey at each location. Without it, it can be impossible to effectively prioritize protection. A facility asset survey and impact assessment should ask detailed questions to get at what is truly vital at each infrastructure site to the overall operation, and what the consequences of a breach would be for different assets. Surveys should ask: What critical activities and operations take place at this location at this time? What critical assets are located at this facility? How much did it cost to develop the asset? Is the asset still valuable if it is compromised?

To be comprehensive, all assets—including people, equipment/material, information, facilities, and activities and operations—must go through this level of scrutiny to identify its criticality.

Penetration testing

In addition to cybersecurity's technical aspects, a holistic approach requires attention to what systems do, all ways they could be compromised, and what the consequences would be if they were. The cybersecurity of critical infrastructure cannot be assured unless physical security is equally robust.

Once acknowledged, this should catalyze operators of critical infrastructure to consider physical vulnerabilities as part of

network penetration testing. Penetration tests that do not account for blended or hybrid threats cannot offer real assurance of network system security. It is necessary to conduct active penetration exercises that attack the points of intersection between physical and cybersecurity and go beyond the automated vulnerability scanning of network systems.

Joint penetration testing is also a valuable way to forge alliances and enhance communication between practitioners in both disciplines, and to improve the coordination of protective strategies.

For example, results might point to the need to position surveillance cameras so they can aid in forensic examinations of network breaches (cameras can help provide proof in cases when an employee launches an insider attack on the network from someone else's workstation). Or it can suggest the need to use intelligent video systems to help protect company networks by analyzing the behavior of employees and others who have building access, such as service personnel, and alerting when someone is lingering in a room for too long, for example.

Many researchers who conduct network penetration exercises at critical infrastructure say that operators often have an inflated opinion of the security of their networks because they overlook physical access issues and often warn that exploiting business networks through unauthorized physical access is typically easy. Many discover during penetration testing that anyone with the time, desire, and some know-how can infiltrate systems, observe network traffic from industrial systems, and even gain control over them.

Critical infrastructure must take a regular temperature of how well physical security is doing to deny access to technology and network systems, especially those identified as critical. Network vulnerability can be reduced by conducting active penetration exercises to assess if infiltrating a facility could result in data theft and if vulnerabilities in connected systems might

allow physical harm to result from network intrusions.

The results of real-world penetration tests show the need for them.

- In testing at one corporation, a pen test team member said he only needed a few employee names and a confident attitude, and he was soon in a room of workstations with dozens of logged-on but unattended computers from which he could have gained access to critical data systems.
- In another test, a utility company wanted to assess the vulnerability of its physical systems to a network attack, so his team dug into distribution lists to get the email addresses for employees with access to its supervisory, control and data acquisition (SCADA) networks. His penetration team then sent them emails about a potential cut in employee benefits, and several clicked on a Web site link that promised additional information about it. When they did, malware downloaded onto the user's machine that gave testers control of them. In less than one day, the penetration team had the ability to disrupt the utility company's power production and distribution.
- Another penetration consultant said companies typically assume that if they have a badge system that their data center is secure. But badge systems don't typically sound an alert when a picture is changed, he explained, so in red team tests, he may infiltrate a client's computer network to change an employee's photo to the picture of a member of his red team. Then, when that individual goes to the company and 'his badge' doesn't work, staff will look him up in the directory and see his picture is in the system, and they will typically let him in with a temporary badge. Additionally, because access systems rarely alert when a person's level of access privilege changes, he

can remotely grant the members of his team access into any part of a building he wants. Such easy intrusions are highly likely to work, say experts, who note that basic infiltrations are often effective, such as 'popping' electronically secured doors with just some copper wire, or tripping request-to-exit system sensors by pushing a heat generating device under a door and holding it next to the door panel.

Good coordination between IT security and physical security is necessary to learn whether converged attacks are occurring, how they are happening, and how to respond and investigate. Coordination between physical security and IT security is also a necessary foundation for many successful countermeasures, such as common user provisioning and de-provisioning for both IT and physical systems; a single identity management process; automated log-off processes; segmenting networks so a breach from the Internet can't reach control systems; providing tougher access controls to all equipment; and improving detection of unusual behavior and activity.



Joint physical-cyber risks assessments, the use of similar risk assessment methodologies for both disciplines, and conducting penetration tests that address hybrid threats are strategies that may help critical infrastructure operators improve coordination between physical and cybersecurity.

About the Author:

Garett Seivold is a career security journalist who writes for the International Security Ligue.



Using Metrics and Other Activities to Bridge Physical and Cybersecurity Strategy

As operators of critical infrastructure acknowledge the critical interdependencies that exist between different security activities, it should become clear that there is enormous value in an integrated approach to security, in which the strategies for protecting physical and information assets aren't created in isolation but are instead developed holistically.

But the road for getting there can seem long and difficult. The silos of security that exist may have deep roots and crafting a course correction can seem like a monumental task. Some organizations may believe that strategies often used to achieve alignment are disruptive or too far-reaching, such as combining physical and cybersecurity into one department, appointing a single executive to oversee both functions, or creating a new, comprehensive risk or oversight committee.

Indeed, achieving strategic security convergence is not a simple matter. Security risk is imbedded throughout a critical infrastructure's processes, yet the owners of those processes may rarely consult with one another. Operating cultural differences may provide a formidable barrier to forging a coordinated security strategy, including between physical and information security. Or departments performing security functions may work together but occasionally be at cross-purposes. For example, in hiring, security and human resources may both be involved, but security tends to be concerned with conducting detailed background investigations while HR may be concerned with reducing time-to-hire.

Absent a structured departmental merger that creates integration, it's not easy for everyone to get on the same security page. However, not every avenue to better coordination must flow through restructuring the organization's physical and IT security functions.

There are specific activities that may help critical infrastructure to align the many disparate functions that have a role to play in protection, which can push the organization in the direction of a more integrated security strategy. Possibilities include:

- Identify in the security master plan all protection activities that the organization conducts, and which department and individuals are responsible for each.
- Share risk assessment techniques to create consistency in judging risk.
- Develop standardized processes and tools for identifying, collecting, and reporting security risks and incidents.
- Implement clear channels for reporting and sharing information about security risks.
- Join representatives from different parts of the company in committees to discuss security challenges and solutions.
- Implement technology that drives enterprise security solutions.
- Formalize intelligence sharing and collaborative decision-making between all functions that hold security responsibilities and impact security operations.

Some groups promote a SIMPLE acronym as an easy way to communicate the benefits of a converged approach to security risk management. An integrated security strategy affords critical infrastructure:

- Strategic view of organizational risk across all departments, resulting in fewer policies, less room for error, and more streamlined processes and reporting mechanisms.
- Improved communications by allocation of appropriate resources, resulting in improved business continuity planning and effective change management to create a more security focused organizational culture.
- Mitigation of risk, as intelligence, investigation, and disaster recovery techniques are better integrated, reducing exposure and increasing agility to conditions.
- Process alignment and increased efficiency, resulting in fewer meetings and a reduction in overlapping processes and procedures.
- Legislation and compliance assurance, resulting in a simplified compliance process and an improved legal and regulatory position.
- Effective evaluation of corporate audit procedures, with improvements enabling a better understanding of attack targets and methods and reducing vulnerabilities.

The metrics bridge

An integrated and strategic view of security necessarily asks broad questions such as:

- What is security costing me?
- What do I get for my money?
- Does it work?
- Can it be enhanced?
- Can it be done at less cost?

These basic questions—ones that senior management must answer to properly prioritize and budget for protection—cannot be answered without a thoughtful, well-planned security metrics program. Security executives should be an ally in this process—by demonstrating willingness to share information, integrate processes, and concede that other risk priorities may at times take precedence.

Security executives must also move beyond vague goals for their department and be willing to be held accountable on specific measures of performance so that there is widespread visibility into the company's vulnerabilities. Often, security objectives are identified too broadly to direct improvement activities; the goal of security, for example, may be seen as a general objective to provide a safe and secure environment. This can be problematic, as **a lack of clear indicators of security performance and objectives for what it is trying to achieve can result in excess discretion at the operational level**. The result can be that what senior company managers want from security is not reflected in where practitioners choose to focus their time, attention, and resources.

The actions of security personnel should match what the organization believes is necessary to maximize protection—something that formal security metrics can help to ensure. Converged security metrics, where appropriate, can improve alignment even further. It is a way for an organization to holistically analyze and address critical threats and to truly inform the organization about its progress.

For example, if data theft is a problem, a converged security metrics program can be developed to address it, one that identifies goals and performance measures for each group in service of the collective mission. For physical security, for example, it might be important to enhance the security culture and improve adherence to access control policies, so metrics may

be designed to measure and improve employee attitudes. For IT, weak passwords may be seen as contributing to data theft, and metrics may be designed to measure progress toward better password policy enforcement. In this way, the organization can measure progress toward better data security while ensuring that both cyber and physical security are part of the solution.

It is important to devise security performance measures, but these can reinforce security silos if goals and performance measures only reflect the security needs of individual departments and units. Security metrics should also be crafted to act as a bridge—enabling organizations to consider threats and risks across departments and aligning performance measures with organizational goals.

When a collective metrics approach is taken, security metrics help to unify security missions across departments and allow senior management to appreciate security from a strategic perspective rather than a risk/fix or incident/countermeasure model.



Integrated security metrics is one way that critical infrastructure can help align security functions without a fundamental restructuring, alongside communication, reporting, data collection, and technology strategies.

About the Author:

Garett Seivold is a career security journalist who writes for the International Security Ligue.





A New Security Paradigm in the Threatening Cyber Era—from Physical to Converged Security Information Management

It was 2005 when James I Chong coined the PSIM acronym, after setting up VidSys company. A PSIM is a kind of software that collects data from all security applications (burglar alarm, CCTV, access control, fire alarm ...), enabling control for all of them through a unified interface, helping Alarm Receiving Centre, Control Room, Command Center personnel to be aware of the situation, make decisions and react even before a security breach occurs. To make it clearer, PSIM is not just an integration platform, but rather an intelligent software that converts massive amounts of data into meaningful and actionable information. This is done by filtering and correlating the data based on time, location, duration, frequency, and type, using sophisticated algorithms, which could include cutting edge technology, such as Big Data and Artificial Intelligence.

As PSIM is constantly evolving based on customer and business process needs, it already started in the last decade to naturally shift towards what has been identified as Converged Security and Information Management (CSIM, once again a new acronym from Mr Chong). The concept behind this evolution can be easily rooted into the fact that all security applications are now IP converged. As a result, since anti-tampering is inherent to all security systems features, cybersecurity and cyber resilience have been taken into account by manufacturers of security systems and, as a consequence, implemented in PSIM, now CSIM.

But in an era when physical and cyber security are merging to better respond to combined attacks, it's time to broaden the PSIM/CSIM scope to include awareness within security of what are becoming—or already are—the most crucial assets of any public or private infrastructure: IT and data. In fact, several studies¹ show how a holistic approach is required to evolve towards a full understanding of the ever-developing risks facing cyber-physical systems.

CSIM, where correctly designed and implemented, extends software abilities beyond physical security by capturing and correlating data from multiple IT-security systems and information management systems. With capabilities for large-scale, widely dispersed assets or customers, this advanced kind of platform can be effectively leveraged to support providing Private Security Services (PSS) in a variety of use-cases such as Critical Infrastructure Protection, supply-chain security, crowd and event security, building and plant management, and so on.

As the transition from PSIM to CSIM continues, an improved cooperation—if not a merger—between previously contrasting functions like Physical security and IT security is envisaged and necessary. Organisations involved in this process are pushed towards an organisational and operational convergence, which requires to merge functions. Private Security providers, offering comprehensive solutions in this scenario and adopting CSIM technology,

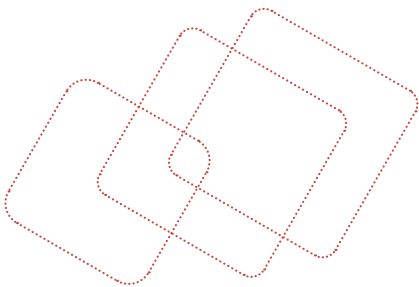
¹e.g. the one conducted by [Newsweek Vantage](#)

have to broaden their competences and skills as well, adding IT security to the company's knowledge base. They also have to integrate it in their company culture, consistently implementing the above-mentioned holistic approach. The most innovative security companies around the world already started this process, and we can already see several cutting-edge providers and success stories, confirming that the holistic approach is the way to go. These private security companies are now able to support the customers facing new, combined, threats, Cyber and Physical, understanding their needs starting from the risk analysis stage.



A CASE HISTORY ...

... in which the use of a CSIM could have helped. This case involved a famous brand operating several plants globally. In one of those plants, located in the Czech Republic, criminals launched a cyber-attack to a server intended to manage pick-up orders. Thanks to IT measures that were in place, commonly supported by an Intrusion Detection System (IDS), the attack was detected within minutes, brought to the attention of the relevant IT teams and fixed. But due to the lack of convergence between Cyber and Physical security and, as a consequence, IT security not being implemented within the tool adopted to manage Physical security (a PSIM), within such a short time frame, criminals were able to give clearance to a fake logistics player for a fictitious pickup. PSIM was fed by fake data to grant access to this fake “operator” and a full cargo was stolen. Security officers couldn't block this fraud because, from an overall security perspective, an important piece of the picture, i.e. the one describing the cyber-attack, was missing. With a CSIM in place, this crucial piece of information would have been shared between IT AND Security teams, the latter would have been able to postpone hauling operations until the server was up and running again and give to relevant Law Enforcement Agencies the right information to identify and arrest criminals, within a well-established Public Private Partnership (PPP).



About the Author:

Antonello Villa is an entrepreneur and expert in Alarm Receiving Centre and Monitoring sector in general. He's also Vice President of Confedersicurezza, the Italian association representing Private Security Companies. Within CoESS he chaired the Monitoring and Remote Surveillance Committee for many years and was a member of the Board of Directors.



9.

Cyber-Physical Security: Can EU Legislation and/or Standards Help?

In recent years, the European Union has been at the forefront of producing legislation in the digital domain, which has had an impact and has influenced legislators far beyond the Union's scope.

This has been the case, for example, of the General Data Protection Regulation (GDPR), which came into force in 2018. We can, therefore, expect that other legislation, existing or in progress, might also inspire legislators in other regions.

Several EU Directives and Regulations are relevant to the topic of this White Paper:

- Under the heading of Critical Infrastructure Protection:
 - ◆ On the Cyber side, the so-called NIS1 (Network and Information Security) Directive, to be updated shortly by NIS2, entailing more stringent rules
 - ◆ On the Physical side, the Directive on the Resilience of Critical Entities (CER), to replace the Critical Infrastructure Protection Directive 2008/114.
- Under the heading of cybersecurity requirements for manufacturers and users of connected products and services:
 - ◆ The EU Cybersecurity Act
 - ◆ The EU Cyber Resilience Act (in progress)
 - ◆ The Radio Equipment Directive (so-called RED)
 - ◆ The EU Artificial Intelligence Act (in progress)

One observation can be made when looking at this complex web of Directives and Regulations in the context of cyber-physical security: **in the same way as cybersecurity and physical security are handled separately in enterprises, they are also handled in silos in legislation.**

When the proposals for the CER and NIS2 Directives were being prepared, this is the first observations that CoESS made to the relevant European Commission Services. While it was indicated in the proposals that these two areas needed to be handled in parallel, the legislator did not go so far as addressing them in one and the same text. Is this a lost opportunity or just a sign that the situation was not mature enough?

Granted, the two directives had a fair share of cross-referencing and parallel requirements, but CoESS didn't think this went far enough. The one positive aspect of the situation was that it offered the opportunity to ask for useful provisions in the NIS2 proposal to be mirrored in the CER proposal, among others on the reference to standards. The adopted CER Directive does recommend to the Member States to use standards to verify the quality of security providers. However, the fact that the two Directives originated from different services in the European Commission, and followed different paths in the European Parliament, was not an ideal situation.

What the two texts do have in common:

- To a certain extent, the sectors identified as "critical entities", referred to in NIS as "essential services" are similar, even if not entirely the same;

- These essential services/critical entities are obliged to carry out risk assessments and take the appropriate measure to protect the entities and ensure they are resilient;
- Operators of such services/entities must report disruptive incidents to the relevant authorities.

Although they should be coming into force broadly around the same time –around 2024–further to the recent sabotage actions in the Baltic sea against underwater pipelines, the Council has recently invited the Member States to speed up the transposition of the CER Directive. The Commission has highlighted that energy and transport infrastructure should require particular attention and undergo stress tests.

Coming to standards, while researching existing standards that might point us to the direction of cyber-physical security, we found an IEC standard, EN IEC 62443 a Cyber Security Standard for Operational Technology. While this was not exactly the same as protecting Cyber Physical Systems (CPS), the approach could be used as a model to address them, as Operational Technologies (OTs) are CPS.

IEC 62443 is a series of standards being developed by two groups within IEC, in consultation with other standards groups within ISO, among others.

The approach is risk-based, and it is applied across a wide range of sectors, including:

- ◆ Utility grids and systems
- ◆ Hydropower facilities
- ◆ Offshore wind
- ◆ Railway, shipping and aviation
- ◆ Building control
- ◆ Industrial automation and IIoT

A more detailed analysis should be made in order to determine how the principles in IEC 62443 can be transposed to CPS in security.

On the physical side, CEN TC 439 “Private Security Services”, of which CoESS is a very active player, is developing a whole standard system to define quality criteria for security services providers active in Critical Infrastructure Protection:

- EN 17483-1:2021 “Private Security Services—CIP—General Requirements”: as indicated, this provides the general requirements for the security companies offering services in any type of Critical Infrastructure. It includes criteria covering the need to protect clients’ data but doesn’t implicitly refer to CPS holistic protection.
- prEN17483-2 (adoption planned in Q2 2023) “Private Security Services—CIP—Airport and Aviation Security”: this is the update from former EN 16082:2011 “Airport and Aviation Security Services”
- prEN17483-3 (adoption planned in Q2 2023) “Private Security Services—CIP—Maritime and Port Security”: this is the update from former EN 16747:2015
- future EN17483-4 “Private Security Services—CIP Energy Production and Transmission”
- Further standards will be developed, most probably on healthcare and hospitals, water treatment facilities and other CI that require it.

So what's next?

In the future, these standards will need to include a provision drawing attention to the need to adopt a holistic approach to cyber-physical systems but this will only be efficient if the CI operators have the same approach.

More than ever before, the security chain must ensure that each link is as robust as the next, and in addition it needs to have a holistic approach and multi-disciplinary teams in which the physical security and the cybersecurity specialists work together towards the same goal.

About the Author:

Catherine Piana has been the Director General of CoESS since 2014 and of ASSA-i since 2016 and the Chairperson of the CEN's Technical Committee TC 439 "Private Security Services".



10.

Table of EU Legislation Relevant to Cyber-Physical Security

	Data Protection Requirements	Requirements for Critical Infrastructure Protection (Physical & Cyber)	
	General Data Protection Regulation (GDPR)	Network and Information Security 1&2 (NIS 1&2) Directive	Directive on the Resilience of Critical Entities (CER)
Objective	Protection of personal data of EU citizens and new data privacy rights.	High level of cybersecurity of Critical Entities across the EU—NIS 1 has been updated by more stringent rules in NIS 2.	High level of physical protection of Critical Entities across the EU—repeals EU Directive 2008/114 on the definition of European Critical Infrastructure.
Scope	The GDPR imposes data protection obligations onto all organisations that collect and/or process data of EU citizens.	Operators of “Critical Entities” in the following sectors: NIS 1 (current): healthcare, transport, financial market, energy, water supply, digital infrastructure and service providers. NIS 2 (update): electronic communication networks, social networks, data centres, space, waste management, chemical sector, postal services, manufacturing of critical products, food, public administration, research. Article 2 of NIS 2 and the Annexes provide an overview of the type of critical entities in these sectors that are covered by the Directive.	Operators of “Critical Entities” in the following sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space. A methodology is established to identify the critical entities that are covered by the Directive.
Relevant provisions (non-exhaustive)	- data processing is subject to protection and accountability principles, based on data subject consent (with exemption in law enforcement activities) - data must be handled by the data controller in a secure manner based on certain technical and organisational measures - data protection by design and default in any new product or business activity/service	- enhanced cybersecurity capabilities of national authorities, incl. enforcement powers against operators - Operators have to adopt risk management practices and notify incidents to their authorities. - NIS 2 provides more specified security requirements, incl. on incident handling, business continuity, cybersecurity along the supply chain, vulnerability handling and disclosure, cybersecurity hygiene and training, human resource security, access control policies and asset management.	- Member States are obliged to have a strategy in place to ensure the resilience of critical entities, carry out a national risk assessment and identify critical entities. - Critical entities are required to carry out risk assessments, take appropriate technical, security and organisational measures to boost resilience, and report disruptive incidents to national authorities. - Technical, security and operational measures include the designation of critical personnel, including among external service providers, and the quality control of such personnel in terms of qualification and training. - Other measures include adequate physical protection of sensitive areas such as fencing, barriers, perimeter monitoring, detection equipment, access controls, employee security management and business continuity measures.
Applicable	Since 2018.	NIS 1: since 2018. NIS 2: as of 2024.	As of 2024.



	Cybersecurity requirements for manufacturers and users of connected products and services			
	EU Cybersecurity Act	EU Cyber Resilience Act	Radio Equipment Directive (RED)	EU Artificial Intelligence Act
Objective	Among others, the Cybersecurity Act strengthens trust in ICT products by establishing a cybersecurity certification framework for products and services.	Minimum cybersecurity standards for all connected hard- and software products to better protect users against cybersecurity threats.	Ensure that radio equipment is sufficiently secure. A Delegated Act in 2021 updated the Directive from 2014 to improve the cybersecurity of covered products.	Regulation of the use of high-risk AI systems.
Scope	Manufacturers and users of ICT-based products and services.	Manufacturers of all connected hard- and software products	Manufacturers and users of electrical and electronic equipment that can use the radio spectrum for communication and/or radio determination purposes—including internet-connected radio equipment, machines, sensors, networks and IoT.	Manufacturers and users of high-risk AI systems identified in the Annex of the EU AI Act—including biometric identification technologies and systems.
Relevant provisions (non-exhaustive)	◆ The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures for ICT-based products and services. ◆ It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements. ◆ Use of certified products can be made mandatory by Member States or the EU as per the NIS 2 Directive.	◆ General provisions: Products must meet specific requirements set out in the Act—to be documented by an EU declaration of conformity. All covered products shall bear the CE marking. ◆ Conformity assessment: For a specific number of “critical products”, a third party should be involved in the conformity assessment. ◆ Cybersecurity Updates: Manufacturers must ensure cybersecurity through consistent, free-of-charge security updates through automatic updates and the notification of available updates to users for the expected product lifetime or for five years.	◆ Article 3 of the RED in relation to health and safety, and more. The Delegated Act further provides that ◆ network operators and service providers should ensure that their systems and platforms are secure. ◆ manufacturers of equipment should ensure that it is designed taking into account security principles. ◆ users should be aware of risks performing certain operations and of the need of performing the necessary updates of the equipment they use.	High-risk AI technologies and systems, including their use, must comply with multiple provisions, including on data governance, human oversight and cybersecurity.
Applicable	Work is ongoing on different certification frameworks, e.g. cloud services.	Currently negotiated at EU-level.	RED applies since 2016. Updated cybersecurity requirements are effective as of 2025.	Currently negotiated at EU-level, effectively applies most likely not before 2025.



Publishers

Armin Berchtold
General Secretariat of
the International Security Ligue
c/o Securitas AG
Alpenstrasse 20
CH-3052 Zollikofen
infoliga@security-ligue.org
www.security-ligue.org

Catherine Piana
Director General
CoESS aisbl
56 Avenue des Arts
1000 Brussels
Belgium
catherine@coess.eu
www.coess.eu

Disclaimer:

Our Liability—to the fullest extent possible at law we (and all our sister, parent, subsidiary and member companies and organisations) exclude all liability for any loss or damage (including direct, indirect, economic, or consequential loss or damage) suffered by you because of using the contents of this document.

Design and graphics:
www.acapella.be

Photo credits:
© iStock: 1127637966 peshkov, 1091449668 Gugai, 1156760867 Natali_Mis, 836124870 WangAnQi,
1159763302 & 1355657113 gorodenkoff, 483074908 artJazz, 994789462 metamorworks,
1171066236 Blue Planet Studio, 1186996701 ismagilov
© depositphotos: 18398501 agsandrew