The World of Cyber-Physical Systems

WE LIVE IN A WORLD in which the way we observe and control it is radically changing. Increasingly, we interact with physical objects through the filter of what computational systems embedded in them tell us, and we adjust them based on what those systems relate.

We do this on our phones, in our cars, in our homes, in our factories and, increasingly, in our cities. Physical objects are so interconnected that we simply take those connections for granted, as if being able to unlock your car by pushing a button on your key fob, unlocking it with your phone or even by walking toward it is the way car locks always worked.

This interconnectedness offers us capabilities that exponentially exceed the expectations of science fiction writers and futurists of past generations. But it also introduces disquieting possibilities. Those possibilities reach beyond cyberspace to threaten the physical world in which we live and – potentially – our own physical well-being.

To understand those threats, this book will take a deeper look at the cyber-enabled world in which we live. We'll assess the vulnerabilities that cyber-connectedness opens and how it forces us to rethink our current approaches to cybersecurity. We'll explore how those vulnerabilities can be – and, in some cases, already have been – used to inflict physical damage. Later in this book, we will also look at what we can do to reduce those risks and how to take proper actions to mitigate the impact of the attacks once they happen.

Cyber-Physical Systems

As we extend cyber technology into our physical world, we create cyber-physical systems (CPS). Such systems integrate computational devices with a single- or extremely limited-purpose scope into key areas of physical systems – whether mechanical or biological – to monitor and interact with them.

In the mechanical realm, think of a computer chip that monitors a valve in a factory, automatically opening or closing it as needed to maintain proper system pressure. In the biological realm, think of an automated insulin pump that constantly checks a diabetic's glucose levels and adjusts insulin levels with little or no input from the patient – before the patient would otherwise even recognize the problem.

Integrating computational components greatly expands what physical components could do when they depended solely on human interaction. Even a simple single- or limited-purpose computational component added to a mechanical or biological system can potentially monitor and adjust more reliably than a human could.

Computational components can be integrated at minute levels that humans would find difficult or tedious to monitor. Thus, CPS can gather more comprehensive data than humans – who are subject to distraction – could. They won't miss critical data that could affect decisions.

Components integrated at a minute level also surpass human ability in that they can network with computers that control larger parts of the overall process. This eliminates the indirect step of humans inputting collected data. In fact, CPSes offer an almost unlimited ability to network components incorporated at the most basic level to computers engaged in every level of the overall process – wherever in the world those computers may be – to offer real-time data on all components of the system and allow humans to intervene in the process only when necessary.

We might, therefore, define cyber-physical systems as any systems in which embedded computers monitor and control physical processes, with feedback loops where physical processes affect computation and vice versa.

One of the best definitions of the term cyber-physical systems was coined in 2006 by Dr. Helen Gill of the National Science Foundation. Dr. Gill defines CPS as "physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale. Computing is deeply embedded into every physical component, possibly even into materials. The computational core is an embedded system, usually demands real-time response, and is most often distributed.[1]"

CPS is a broad, umbrella term that encompasses many other, more familiar terms for technologies that connect our physical world with the cyber world. It encompasses Industrial Control Systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC). It also encompasses Internet of Things (IoT), Industry 4.0 and Industrial Internet of Things (IIoT), the Internet of Everything and 'Smart'-Everything, and the Fog (similar to the Cloud, but incorporating also the physical objects that can be connected to it). CPS is the broadest of these terms because it focuses on the fundamental intersection of computation, communications and physical processes without suggesting any particular implementation or application.

Even more relevant to the focus of this book, we may use the working definition developed by the Cyber-Physical Systems Security Institute (CPSSI) and used by its member companies: "Cyber-physical systems are physical or biological systems with an embedded computational core in which a cyberattack could adversely affect physical space, potentially impacting well-being, lives or the environment." This definition recognizes the cyber-kinetic threat of such cyberattacks – largely overlooked by many of those moving the field of CPS forward – and, along with how to address those threats, is the focus of this book.

Attacks That Mix the Cyber and Physical Realms

Several terms describe the mixing of cyber and physical realms for malicious purposes. It's important to understand the difference between them because the words used in them cause them to be easily confused. These terms are "physical-cyber attacks," "cyber-physical attacks" and "cyber-kinetic attacks." To classify the threats it is useful to characterize them based on the domain that is the origin of the threat, and the domain where the impact is felt.

Physical-cyber attack refers to an attack originating in the physical domain with the impact felt in the cyber domain. Commonly such an attack damages physical equipment, with the objective of disrupting cyberspace functions. For example, damaging the servers or network cables on which cyberspace operates would impair ability to access the cyber world. This could also involve physically compromising sensors so that they are incapable of sending accurate data. The key to this kind of attack is that physical equipment is damaged, with resultant impairment of cyberspace functions.

Cyber-physical attack refers to the exact opposite. Such attacks involve actions that originate in cyberspace but impact the physical characteristics of a system by impairing the ability of cyber-physical systems to monitor and control physical processes. An example of this term in its broadest form is hackers impairing performance of a CPS through a Denial of Service (DOS) attack or breaching it to demonstrate their ability to compromise it, then extorting the system owner into paying a ransom. Attacking smart meters to reduce electricity bills is also an example of a cyber-physical attack. Other possible goals under this broad definition could be industrial or political espionage, where hackers seek a strategic advantage over competitors, or hacktivism, where hackers seek to hamstring their targets to force them to comply with the hacktivists' goals. Thus, the term cyber-physical attack serves as an umbrella term. Its three key elements are that the attack 1) uses systems in cyberspace as the channel for the attack, 2) targets cyber-physical systems, and 3) impacts the physical world.

Cyber-kinetic attack falls under the umbrella of cyber-physical attacks, but is more specific in its goal. It, too, uses cyberspace as the channel for an attack. It, too, targets cyber-physical systems. But its goal is more specific. That goal is to cause tangible, physical damage. For example, state-cyber-warriors or cyber-terrorists hacking into a power plant and causing generators to fail could leave millions of people and businesses without power, with not only massive inconvenience, but also significant economic damage. Other examples include cyber-terrorists attacking connected or autonomous vehicles to cause a crash; cyber-terrorists, cyber-warriors or cyber-spies assassinating people by attacking embedded medical devices; a company changing competitors' automated manufacturing processes to damage competitors' product quality or volume; or – the holy grail of cyber-terrorism – causing explosions and/or environmental damage by remotely attacking nuclear power plants, chemical or gas installations, oil pipelines or other physical targets whose failure could cause catastrophic physical damage. Cyber-kinetic attacks thus cause direct or indirect physical damage, injury or death, or environmental impact solely though the exploitation of vulnerable information systems and processes. It is on these attacks that this book will primarily focus.

Although cyber-kinetic attack is a relatively new term, an apocryphal story[2] suggests that the concept of such an attack was conceived as far back as the 1980s. The story goes that the U.S. Central Intelligence Agency learned in 1982 of Soviet efforts to steal natural gas pipeline control software from a Canadian company. In response, the CIA supposedly introduced defects into the software so that the version the Soviets stole would cause pipeline pressure to build until pipes ruptured. According to the story, this eventually occurred in a Siberian pipeline in an explosion so massive that it could be seen from space. Although the story has never been confirmed by any other source, it shows that the concept of cyber-kinetic attacks was understood long before our world became so ubiquitously cyber-connected.

How Cyber-Physical Systems Work

Perhaps the easiest way to understand CPS is to look at some of its larger-scale installations – the type found in factories, power distribution systems or buildings – commonly referred to as Industrial Control Systems (ICS). These typically consist of electronic processors attached to key control points, such as valves and switches. The processors monitor the status of those control points, as well as pressure, temperature, flow or whatever other conditions impact the proper functioning of the system. The processors may report this data to human operators for manual intervention. More often, though, they automatically adjust the equipment as necessary to keep it functioning as intended. Readings and adjustments occur continuously without human intervention.

Large-scale systems have a pyramidal hierarchy. A large number of processors interact with minute components at the base level. An aggregation of those processors may then be monitored and controlled at a slightly higher level. This next level might monitor an entire piece of equipment, the level above that multiple pieces of equipment engaged in the same process. A decreasing number of interfaces monitor broader groups of functions the higher up the pyramid you go, until you reach a corporate headquarters level. There, at the top of the pyramid, they receive real-time high-level data from multiple plants spread around the globe.

Interfaces for human interaction are designed into appropriate places in this pyramid. This enables manual overrides in unanticipated situations. Such interventions may come from changes in equipment, or the need to increase or decrease production for changes in demand. Other interfaces forward data to automated systems that archive it – both automatic and override – as permanent records for future diagnostic needs, and to analyze efficiency and trends.

Programming of processors and human interfaces that operate at the most basic level generally are simplistic. This enables human operators to easily program them even if those operators don't have more than basic programming training.

The Growing Presence of Cyber-Physical Systems

The transportation, utilities, city services and industries infrastructure that surrounds us follow the industrial control systems model described above. Cyber-physical systems are everywhere. Surprisingly, sometimes they even monitor dirt, as you'll soon see!

Beyond the ICS process described above, manufacturers increasingly use sensors to take the guesswork – and the element of surprise – out of equipment maintenance. Sensors monitor equipment for degradation[3] so maintenance can be scheduled in advance instead of interrupting workflow. This gains efficiency. It reduces the need for preventative maintenance and its increased downtime, because companies can run equipment until just before its failure point without running the risk of unexpected breakdowns that require emergency juggling of workflows. In addition, sensors also allow manufacturers to analyze and identify equipment and process improvements that will increase efficiency and productivity.

ICS plays an increasing role in smart city technologies that centralize monitoring and control of vital systems for greater efficiencies. Through automated monitoring of traffic patterns and densities, traffic lights can be optimized to minimize gridlock.[4] Pollution control, street lights, building management, emergency services and security, too, increasingly fall under the umbrella of smart city technologies.[5] And in the most advanced public transportation systems, prospective users can receive real-time information about when and where to access them to achieve the fastest travel time, based on GPS information from user smartphones and user-chosen parameters.

Power companies and water companies electronically monitor distribution[6] to detect problems – and the exact location of each problem – before the first consumer notices them. Waste management companies can monitor collection containers and empty them only when they are nearly full.[7] Oil companies and railroads use ICS to keep operations flowing smoothly. The list of users goes on and on. And, as mentioned earlier, ICS technology is even used to monitor dirt! Agricultural operations are increasing yields by using soil sensors to determine optimal times to water crops and what nutrients to add to the soil.[8]

Converging Technologies

The growing world of CPS doesn't end with large-scale networks of ICS, though. As mentioned previously, it also contains the rapidly expanding world of IoT, the smart devices ubiquitous in our lives. Although the two are often treated as totally different because of differences in their original technologies, those differences are rapidly evaporating.

Industrial control systems originally were designed as closed systems isolated from the cyberworld. They operated with specialized protocols not compatible with internet protocols. That model is fast becoming history, though. ICSes increasingly connect with company networks to enable more company personnel to access information and to take advantage of analytical tools on company networks. Thus, they increasingly use internet protocols and connections.[9]

IoT devices are increasingly taking over as components in ICS,[10] due to their superior ability to interact with more of a company's information systems. That increased ability, though, also makes them vulnerable to outside attack. Thus, throughout this book, we will not differentiate between ICS and IoT. Their risks and the approaches to risk reduction for both are increasingly similar.

One example of an IoT system – or, perhaps more accurately, collection of systems – is found in the newest automobiles. Processors monitor internal sensors throughout the vehicle to bring drivers on-demand diagnostics of engine operation and alert drivers when service is needed – anticipating breakdowns before they happen. Clearly, this interrelationship between sensors, monitors and interface fit the ICS model.

Other processors connect to outside cyber-services to offer drivers an unprecedented ability to access driving directions and almost any type of entertainment they desire. Such in-car information systems can be accessed and controlled on a handy touch-screen, or projected on the windshield and controlled by the driver's voice to ensure the driver keeps eyes on the road. It's easy to see the ICS model of sensors, processors and human interfaces in these systems, as well as the interconnectivity of IoT, showing the convergence of the two.

This convergence is even clearer when we view safety and emergency systems. Computer-enriched cameras and radars monitor traffic around the vehicle and warn of vehicles in the driver's blind spots, either passing alongside the car or crossing the car's path when in reverse. They also can take over deceleration and braking functions, cutting power to the engine and applying brakes automatically, when the driver doesn't act to avoid a potential collision.

Sensors throughout the car connect to remote emergency personnel in the event of an accident. Processors send detailed information from internal sensors about the type and severity of the crash to help emergency personnel be fully prepared to take needed action when they arrive – even if the accident renders the driver unable to contact or communicate with them.

CPS is so integrated in autos that totally self-driving cars, where the car sets its own course, monitors and adjusts to traffic and responds automatically to potential emergency situations – even faster than a driver could – are inch daily toward acceptance on public highways.

Our phones, too, serve as points of interface with our cars, enabling us to lock or unlock them, start the engine or check diagnostics wherever and whenever we want. They may connect us with our homes, allowing us to control lights and heat, or even lock and unlock doors from anywhere in the world. Or, they can program lights, heat, doors, appliances and more to operate according to a specific schedule or to activate or deactivate depending on where people are in the house.

CPS finds applications in our appliances, in our health care, and even in our bodies. In medical treatment, implanted heart monitors allow medical personnel to monitor a patient's heart no matter where the patient is. These devices can alert doctors of a dangerous condition even before the patient is aware of it. Implanted blood monitors continuously monitor insulin levels and alert the patient to what action to take to return levels to normal. Current experimentation even has us on the verge of creating 3-D printed synthetic human organs[11] to replace or enhance the ones in human bodies.

There is no question that our physical world is fully blanketed in the cyber world. The only question is whether that mix of physical and cyber is secure.

The Unspoken Problem in Cyber-Physical Systems

Using CPS to monitor and control devices and equipment that affect our physical environment introduces new problems. The potential for malicious use of those CPSes exposes our physical environment to cyber-kinetic attacks.

This can include damage to physical property, such as the 2009 Stuxnet[12] worm that caused Iranian uranium-enriching centrifuges to malfunction and be ruined. It can extend even to causing injury or death to people, such as the potential, demonstrated in laboratory tests, of hacking a person's implanted pacemaker or defibrillator and sabotaging it[13] so it kills the person. Although no case of hacking an implanted heart monitor or defibrillator has been documented, potential for it was enough to lead doctors for then-U.S. Vice President Dick Cheney to disable the wireless functionality of his implanted defibrillator[14] in 2007 as a precaution against assassination attempts.

Little is said publicly, though, about the potential for cyber-kinetic attacks. Those who have a stake in expanding cyber-connectedness have been quick to downplay such threats. The rush is on to cash in on industry's quest for the increased efficiency and greater profits that CPS and ICS offer – not to mention consumers' hunger to control ever more of their lives from the convenience of their smartphones. Conferences on

CPS focus almost exclusively on enhancing and extending the technologies, with little to no discussion on security [15] of those technologies.

Yet the potential is real. Not only the defibrillator experiment mentioned above, but also attacks on power plants and remotely taking control of crucial systems on automobiles, have been demonstrated as doable[16] in laboratory tests. Cyber-kinetic attacks have been carried out in scattered acts of sabotage (such as the Stuxnet worm), espionage and criminal activity. The fact that past incidents have been, so far, of a small scale does not excuse dismissing their potential as unrealistic or alarmist. Attacks may indeed be happening, but not detected. Results from experiments on hacking cars or medical implants suggest that such attacks would be so hard to detect[17] and so foreign to investigators of transportation or medical fatalities that they likely would overlook the scant evidence left behind and rule the deaths accidental.

As our physical world grows exponentially more connected to the cyber-world, potential for attacks grows with it. The security community must increase its efforts to shore up the vulnerabilities that presently are being placed on the back burner in the rush to introduce ever more cyber-connected technologies.

Where We Are and How We Got There

On the surface, the wide variety of protocols still used in some ICS leads to an illusion of security, commonly referred to as “security by obscurity.” Because no protocol is used widely, engineers consider them unlikely to be targeted.

Security by obscurity, though, is illusory. The security of each protocol is only as good as what the manufacturer has built in. It is not the result of time-tested best practices. And the possibility of a breach is only increased the more exposed a system is via its cyber connections.

In many cases, security on ICS systems is weak. Early systems were thought to be of interest only to those who worked with them. Thus, they were built to facilitate easy access for anyone who needed to monitor or intervene with their operation. Little to no thought was given to securing them from outsiders. As long as commands that the device received were in the proper format and syntax, it accepted the instructions. That left them vulnerable.

Current Vulnerabilities

Even devices that received security patches are not fully secure. Adding patches offers more protection than leaving devices without any, but that option still is not ideal. Incorporating security into devices and systems at the manufacturing phase is far more comprehensive. Software can more easily accommodate multiple layers of safeguards when it is designed with those layers right from the start. The same goes for hardware. When built in at the start, it can incorporate failsafe functionalities that serve as a final line of defence against attempts to compromise the system or device. Such robust security safeguards are far more difficult to compromise than security patches that are later applied as an afterthought.

With unprotected, or inadequately protected devices, communication between sensors, monitoring devices and actuators is vulnerable. Hackers could either introduce false data to trick actuators into taking detrimental actions, or actually take control of the system and command a disruptive event. Although most literature on the subject talks about the latter, hackers could accomplish the same result by the former, as well.

For example, a hacker could unleash a pipeline explosion by disabling alarms and/or fail-safe functions and taking control of the monitoring element that maintains the proper pressure in the pipeline. This would require a hack into the element and wresting control of it away from its intended function. On the other hand, the hacker could also intercept data sent from the sensors and replace it with false data that suggests that pressure is too low. The monitoring system – or humans interfacing with it – would believe that the pressure needed to be raised and unknowingly raise it to a point where the pipeline fails. Thus, not only the system monitors and actuators, but also the communication stream between sensors and them must be safeguarded.

Industrial systems are not the only potential targets of malicious activity. Medical devices are vulnerable, too. Although medical devices are rigorously tested, they typically are tested only for adherence to manufacturer safety standards. These standards ensure that the devices do not pose a direct threat to life. Devices are not tested, though, for security against unauthorized access. In other words, they are tested to ensure that they do not pose a direct threat to life via faulty design or construction, but not to ensure that they do not pose an indirect threat to life via unauthorized access.[18]

That is not to say that implantable devices are the only cause for medical concern. Hacking of other medical technology, such as sending overdoses to drug pumps or increasing the level of radiation output of CT scanners could jeopardize lives, too.

Additional Challenges of CPS Security

Systems that maintain life or other critical physical services defy testing approaches used on business information systems. Penetration testing simulates the behavior of cyber-attackers to find weaknesses in a system and see how it can be made to fail. But how can you do this with a system that cannot afford to fail?

The conundrum is intense. Penetration testing on a system that provides critical functions could reduce performance. It could cause critical components to fail. It might alter data sent from the sensors. It might even cause unintended changes to the physical system, open a door for unauthorized access or damage whatever elements of our physical world the system is designed to support. No matter how experienced the testers or how carefully testing methodology is planned, such risks can never be completely eliminated.

An alternative is to compartmentalize testing, testing only cyber elements of the system or only physical elements, each apart from the other. Doing this, however, prevents us from discovering issues at their interface. Testing, to be truly effective, needs to comprehensively assess both parts of the system, as well as the way they interact. To accomplish that, new and innovative testing methodologies that test comprehensively without risking disruption will need to be developed.

Another challenge is that testing one time, at initial installation, is not sufficient. Cyber elements of CPS are designed to outlive many physical components. That means that each time physical equipment is upgraded, testing must be redone, to ensure compatibility and to identify and eliminate any vulnerabilities that the new interface introduces.

The new world of CPS introduces challenges for how to approach authorized access, too. Where critical systems are concerned, authorized personnel must have quick and easy access to adjust CPS components. Yet security must be robust enough to prevent unauthorized access. Preventing an unauthorized party from tampering with a patient's implanted defibrillator could be accomplished by designing a comprehensive multi-layer security approach. Yet such robust security could delay life-saving intervention by doctors if the patient experiences a medical emergency. A workable balance must be weighed and maintained.

We must rethink well-established practices for physical security, as well. The fact that the physical location of a system is secured (such as a data center or a power facility being locked and physically guarded) does not mean that the system is secure. A remote interface – or even a seemingly benign IoT device that interacts with the system – could give someone with malicious intent an entry point, as we'll see shortly in some documented real-life attacks.

When it comes to CPS, we must rethink how to conduct nearly all practices used in information system security. Even such simple practices as routine patching require new approaches, to avoid the risk of the patch inadvertently impairing critical systems. For example, if installing a patch on a business information system encounters unexpected problems, the worst consequence is temporary loss of system access. If installing a patch on a CPS that controls an artificial organ encounters unexpected problems, a patient could die. These challenges to all aspects of security and maintenance of CPS must be addressed as our cyber world and physical world become ever more entwined.

Rethinking the CIA Triad

CPS security may require rethinking many established elements of cybersecurity, including the basic CIA triad paradigm that has traditionally driven them. This triad, which stands for Confidentiality, Integrity and Availability, has guided the practice of cybersecurity for decades.

Confidentiality refers to the need to keep data from falling into unauthorized hands, Integrity to the need to ensure that data is not tampered with and Availability to the need to keep the system functioning so that authorized personnel have access to its data whenever they need it.

We can indeed compare CPS against these concepts, and we will likely find our primary concerns largely lie in the areas of integrity and availability, as opposed to confidentiality – the traditional focus of enterprise security. If we are not able to maintain information integrity in sensor readouts or integrity of commands sent to actuators, this is clearly problematic. Let's look at some examples:

- Confidentiality breach of the mentioned automated insulin pump would give the attacker information about the patient's glucose levels. On the other hand, an information integrity breach could cause unauthorized alteration of insulin dosages, leading to hypoglycemia and potentially death.

- Breaching confidentiality of an autonomous drone would expose information about the drone's location and battery status. Compromising integrity of the drone's geofencing system information could force the drone into restricted airspace above an airport.
- Hacking into a traffic light system could provide information about the normal traffic light cycle and, in some cases, details about the traffic. Compromising the integrity of a traffic light system and altering the normal cycle could lead to massive pileups.
- Stealing information about the fuel consumption of a connected vehicle or driving habits of its driver is not a particularly exciting outcome for a cyber-attacker. However, altering the integrity of sensor readouts or the commands that flow between various systems within a vehicle could alter the vehicle's direction, disable the brakes, or cause other distractions that could lead to an accident.

Maintaining only the three elements of the CIA triad falls short of the needs of CPS, though. While they remain crucial to CPS security – especially Integrity and Availability – additional concerns arise when dealing with systems that interact or control elements of our physical world.

To address these additional concerns, a different paradigm might be needed. One to consider is the Parkerian Hexad. This paradigm expands the areas of concern from three to six, adding Possession/Control, Authenticity and Utility[19] to the three concerns addressed in the CIA triad.

Possession/Control recognizes the need to protect CPS from outright takeover by an unauthorized party. For example, you would not want a third party to take control of steering and braking systems on your cyber-connected car while you are driving it.

Authenticity recognizes the need to protect CPSes from data that comes from an unauthorized source. For example, if you were huddled down in your home on a cold winter night, you would not want someone to send false data that told the system that the house's temperature was so high that the system activated the air conditioner instead of the furnace.

Utility recognizes the need to balance security concerns against maintaining the intended usefulness of devices to authorized personnel. This was described above in the needed balance between robust security of medical implants and physicians' need for immediate access during medical emergencies.

Rethinking Other Familiar Paradigms

Other familiar concepts and solutions might have to be rethought in the cyber-physical world as well.

Threat, vulnerability and risk assessment of CPS, as well as threat modelling, should combine traditional cybersecurity skills with the safety and hazard assessment skillset of the physical world while keeping in mind the oft-forgotten cyber-physical interconnection.

Porous IT firewalls that have been the mainstay of enterprise security for over 25 years might have to be reconsidered in favor of much more restrictive hardware-enforced unidirectional gateways, FLIP products and other solutions more suitable for cyber-physical systems.

IT-centric intrusion detection and prevention solutions that traditionally must tolerate the operation of "noisy" host-based security solutions and approaches such as anti-virus, automated patching across the stack, proprietary application-level protocols and others should be locked down in a cyber-physical environment where most of the CPSes don't have the capacity and/or the risk tolerance for traditional host-based protections and automated patching.

Conventional IP hopping and address space randomization approaches designed to frustrate attackers by introducing a level of obscurity are being replaced by new, comprehensive moving-target defense techniques that can dynamically alter the attack surface of cyber-physical systems and potentially improve the CPS security.

Blockchain, the technology behind the cryptocurrency Bitcoin, could become the technical solution for ensuring integrity of information used by CPSes.

We will explore these and other approaches in the coming chapters.

Real-Life Attacks

The "attack that brought down the internet" – Companies seeking technological advantages over competitors often prioritize speed to market over security, and unknowingly create vulnerabilities. This has resulted in significant damage. Western media dubbed a significant slowdown of the internet in much of the U.S. in October 2016 as the attack that "brought down the internet." That attack, which paralyzed Twitter, Spotify, PayPal and other major sites, was traced to security flaws in consumer electronics[20] manufactured by a single company.

Hackers targeted these flaws and took control of nearly half a million DVRs and smart cameras. They used those devices' internet-connected functions to unleash a massive Distributed Denial of Service (DDoS) attack in which those devices contacted popular websites in such volume that the sites were overloaded and internet service slowed to a crawl in affected areas.

Although this attack didn't cause any kinetic impacts, it became the the attack that thrust IoT vulnerabilities into the limelight.

An attack that shut down heat in Finland – Weeks later in Lappeenranta, Finland, a city of about 60,000, a much smaller DDoS attack[21] occurred that demonstrates even more dramatically the threat to physical well-being in a world tightly connected to cyberspace. This attack compromised the heating and hot water systems in two apartment buildings, locking them into an endless reboot loop that paralyzed the systems and forced residents out of the buildings while technicians puzzled over how to get the systems running again.

That event may have been an isolated incident committed by an individual seeking nothing more than to embarrass the building management. Or, it may have been a trial run of an attack strategy for future, larger, attacks on life-preserving systems.

A wastewater engineer's revenge – A previous cyber-kinetic attack by one man in Maroochy Shire in Queensland, Australia, in 2000 did much wider damage.[22] The man had helped, as a contractor, to design and install their wastewater systems, and had hoped to be hired permanently to maintain them. When that didn't happen, he launched months of sabotage. He hacked the system at random times to release more than 264,000 liters of raw sewage at locations all over town, killing marine life and threatening the health of residents before he was caught.

A prank that injured innocent people – A 2008 attack in Lodz, Poland, was accomplished by a bored 14-year-old boy. He reprogrammed a television remote to interact with switch junctions in the city tram system. He then used the remote to reroute trams [23] for his entertainment. His prank eventually ended with an unintended collision that injured a dozen people.

A Growing Population of Attackers

Those with the skills to carry out cyber-attacks – including cyber-kinetic attacks – are legion. A growing cybercrime community gladly exploits vulnerabilities that appear in internet-connected devices.

Most people think of hackers as computer hobbyists who honed their skills through seeking ever-greater challenges. Their thirst for knowledge is indeed raising the risk of cyber-kinetic attacks as they are increasingly testing the limits in the new cyber-physical world. This, however, is only the tip of the iceberg of the cyber-attacker community.

They could also include[24]:

- Cyber-terrorists or cyber-warriors who have been trained by their governments or by terrorist groups on how to engage in cyber-attacks as a form of warfare, or to use their skills in more covert ways in pursuit of their country's strategic goals.

- Cyber-spies, again trained by their governments or employed by private corporations to steal classified or proprietary information used by rival governments or business competitors to gain a strategic, security, financial, or political advantage.
- Cyber-thieves who engage in cyber-attacks for monetary gain.
- Cyber-hacktivists who perform cyber-attacks for nonmonetary reasons, such as to test their skills for their own entertainment, or to try to enforce their philosophical beliefs on countries, industries or businesses that act contrary to those beliefs.

The potential for cyber-kinetic attacks from cyber-terrorists or cyber-warriors is sobering. They have already trained in ways to disrupt vital systems as part of cyber-war strategies and actively explore channels that would be vulnerable to attack.

Cyber-spies, while not actively exploring channels for cyber-kinetic attacks, are probing sensitive systems for confidential information. It would not take much effort for them, if provided with motivation to turn from covert to overt acts, to do so.

Another threat from those government-trained cyber-terrorists, cyber-warriors and cyber-spies comes when they recognize that dutifully serving those who trained them is not nearly as lucrative as putting their skills out on the open market. A growing network exists of cybercriminals who gained their training as members of cyber armies before turning their efforts toward cybertheft – or even serving as cyber-mercenaries, offering their expertise to the highest bidders.

Such rogue former state agents also proliferate hacking tools and strategies to eager learners on the underground internet. Advanced techniques and tools they learned are available to whoever has the money to buy them.

Thus, the cybercriminal underground is large, varied and highly capable of compromising vulnerable systems if motivated to do so. So far, it is thought that lack of motivation among hackers is the only thing holding back widespread attacks on vulnerable infrastructure. Counting on a continued lack of motivation among those with the requisite skills, however, is not a wise strategy for securing infrastructure from potential cyber-kinetic attacks.

So far, cyber-kinetic attacks have largely been discussed solely in the context of cyberwar. The increased convergence of cyberspace with our physical world, however, makes cyber-kinetic attacks increasingly within the reach not only of nation states, but also of extortionists, terrorists, hacktivists and criminals. Not only that, but there is also increased risk that cyber-kinetic attacks will follow the same pattern that spawned traditional hacking – kids like the teen in Lodz, Poland, testing their hacking skills on cyber-physical systems and inadvertently causing kinetic impacts.

Recognizing the Threat

Governments increasingly recognize that cyber-kinetic attacks pose a significant threat to their national security, their economy and public welfare and safety. Not only are critical infrastructures at risk but, as the technologies for smart cities, smart buildings, connected or self-driving cars, transit systems and drones advance, vulnerabilities expand exponentially. The damage from a major attack would have an effect that extends far beyond its immediate damage. The panic it could launch on the public would cause damage far beyond the immediate attack.

Former U.S. President Barak Obama declared in 2009 that cyber threats were among "the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber-security.[25]" In January 2012, the U.S. Director of National Intelligence testified before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, that "cyber-threats pose a critical national and economic security concern.[26]"

Former U.S. Secretary of Defence Leon Panetta in 2012 described the magnitude of potential threats on U.S. critical infrastructure as a "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life.[27]" A 2013 report issued by the U.S. Government Accountability Office (GAO) warns that cybersecurity threats to systems that support critical infrastructure and federal information systems are evolving and growing.[28]

Governments around the world echo this concern, as well. Israel enacted a centralized civilian Critical Infrastructure Protection (CIP) regulation in 2002 to address cyber-physical risk.[29] The European Union's Joint Research Centre (JRC) has been developing the Experimental Platform for Internet Contingencies (EPIC), a network test-bed designed to enable testing of cybersecurity scenarios in a safe and controlled experimental environment, since 2009. Its 2011 test[30] that combined simulated physical systems with real cyber-systems demonstrated the magnitude of the cyber-kinetic threat. It reported that "today's heavily interconnected power grids would hardly withstand sophisticated cyber-attacks without coordinated actions of grid operators in case of crises."

The European Parliament, in 2016, passed a network information security (NIS) directive[31] that requires minimum security standards for critical infrastructures, such as energy, transport, health, banking and drinking water, and places stricter reporting standards for cloud services and search engines. Parliament's rapporteur Andreas Schwab, MEP for Germany, described the threat this directive addresses and explained Parliament's goal: "Fragmentary cyber-security protection makes us all vulnerable and poses a big security risk for Europe as a whole. This directive will establish a common level of network and information security and enhance cooperation among EU member states, which will help prevent cyberattacks on Europe's important interconnected infrastructures in the future."

China, too, has expressed concern about its vulnerability to cyber-attack. Despite – or perhaps because of – China's intense focus on securing government cybernetworks and pursuing cyberwarfare capabilities, cybersecurity of China's infrastructure has lagged other major nations,[32] according to Qin An, director of China Institute of Cyberspace Strategy, in a 2016 call for cybersecurity upgrades to protect Chinese infrastructure from cyberattacks, cybercrimes and cyberterrorism.

Takeaways

Both lab research and actual attacks reveal the vulnerabilities that CPS presents for cyber-kinetic attacks on our world. Governments increasingly recognize those vulnerabilties. The threat is real.

As the digital world increasingly connects devices that impact people's health and welfare, effective security for CPS is crucial. Rethinking traditional cybersecurity to include the additional challenges of CPS is long overdue.

We need to model security for CPS more broadly, test more extensively, anticipate more strategies attackers might use to compromise systems and recognize where our traditional security practices may prove less effective or not work at all. Interfaces between cyber and physical realms will only increase – and likely will increase exponentially. We must secure these systems properly to protect lives, well-being and the environment.

[1] Radhakisan Baheti and Helen Gill, *Cyber-Physical Systems*, The Impact of Control Technology, IEEE, pp. 161-166, 2011.

[2] T. Reed, *At the Abyss: An Insider's History of the Cold War*, 2005, Presidio Press.

[3] National Research Council; Division on Engineering and Physical Sciences; Commission on Engineering and Technical Systems; National Materials Advisory Board; Committee on New Sensor Technologies: Materials and Applications, *Expanding the Vision of Sensor Materials,* 1995, Available: https://www.nap.edu/read/4782/chapter/8

[4] Hasan Omar Al-Sakran, *Intelligent Traffic Information System Based on Integration of Internet of Things and Agent Technology Management* | Information Systems Department, King Saud University, Riyadh, Saudi Arabia, 2015, http://thesai.org/Downloads/Volume6No2/Paper_6-Intelligent_Traffic_Information_System_Based.pdf

[5] Venkat Pothamsetty, Is IoT the new OT? 2014, Available: http://id.lockheedmartin.com/blog/is-iot-the-new-ot

[6] Courtney Won, *Smart Grid*, Electrical and Computer Engineering Design Handbook, 2015, Available: https://sites.tufts.edu/eeseniordesignhandbook/2015/smart-grid/

[7] Mike Kavis, *Don't Underestimate the Impact Of The Internet Of Things,* 2016, Available: http://www.forbes.com/sites/mikekavis/2014/07/21/dont-underestimate-the-impact-of-the-internet-of-things/2/

[8] *IoT Agriculture Use Cases & Apps To Plant Seeds For Your Ideas*, 2016, Available: https://www.link-labs.com/blog/iot-agriculture

[9] Chris Johnson, *Securing Safety-Critical SCADA in the Internet of Things* | School of Computing Science, University of Glasgow, Glasgow Available: http://www.dcs.gla.ac.uk/~johnson/papers/IET2016/SCADA_IoT.pdf

[10] Ovidiu Vermesan and Peter Friess, ed., *Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems*, 2013, Available: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf

[11] Heidi Ledford, *The Printed Organs Coming to a Body Near You*, 2015, Available: http://www.nature.com/news/the-printed-organs-coming-to-a-body-near-you-1.17320

[12] Avag R. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* | Institute for Science and International Security. 2010; Available: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant

[13] B. Grubb, "Fatal risk at heart of lax security," The Sydney Morning Herald, Sydney, Australia, 06-Nov-2012

[14] Sanjay Gupta, *Dick Cheney's Heart*, CBS News, 2013, Available: http://www.cbsnews.com/news/dick-cheneys-heart/

[15] Scott D. Applegate, *The Dawn of Kinetic Cyber*, Center for Secure Information Systems, George Mason University, 2013, Available: https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf

[16] Applegate, ibid.

[17] Tarun Wadhwa, *Yes, You Can Hack a Pacemaker (And Other Medical Devices Too)*, 2012, Available: http://www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/#1ecbcb13e05d

[18] Mark Ward, Warning Over Medical Implant Attacks, BBC News, 2012, Available: http://www.bbc.com/news/technology-17623948

[19] Parker DB. *Fighting Computer Crime [Internet]*. Scribner Book Company; 1983. Available: http://books.google.com/books/about/Fighting_Computer_Crime.html?hl=&id=BVxsAAAAIAAJ

[20] Michael Kan, *Chinese Firm Admits Its Hacked DVRs, Cameras Were Behind Friday's Massive DDOS Attack*, 2016, http://www.pcworld.com/article/3134039/hacking/chinese-firm-admits-its-hacked-products-were-behind-fridays-massive-ddos-attack.html

[21] Mohit Kumar, DDoS Attack Takes Down Central Heating System Amidst Winter in Finland, 2016, http://thehackernews.com/2016/11/heating-system-hacked.html

[22] Tony Smith, *Hacker Jailed for Revenge Sewage Attacks*, *The Guardian*, 2001, Available: http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

[23] Graeme Baker, *Schoolboy Hacks into City's Tram System*, 2008, Available: http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

[24] Fischer, E. A., Liu, E. C., Rollins, J., & Theohary, C. A. (2013, March 1). The 2013 cybersecurity executive order: Overview and considerations for congress. Available: https://fas.org/sgp/crs/misc/R42984.pdf

[25] Obama, B. (2009, May 29) Remarks by the President on Securing Our Nation's Cyber Infrastructure, Washington, D.C.

[26] Clapper, J. R. (2012, January 31). Director of National Intelligence. Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence.

[27] Panetta, L. E. (2012, October 11). Secretary of Defence, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.

[28] United States Government Accountability Office (GAO). (2013 February). Cybersecurity national strategy, roles, and responsibilities need to be better defined and more effectively implemented, GAO-13-187.

[29] Robert M. Clark and Simon Hakim (eds.), *Cyber-Physical Security Protecting Critical Infrastructure*, 3, DOI 10.1007/ 978-3-319-32824-9_10 (2017) Springer International Publishing Switzerland

[30] The EU Science Hub, Cybersecurity, 2016, Available: https://ec.europa.eu/jrc/en/research-topic/cybersecurity

[31] Tom Reeve, *New EU Directive Requires Critical Infrastructure to Improve Cyber-Security*, 2016. Available: https://www.scmagazineuk.com/updated-new-eu-directive-requires-critical-infrastructure-to-improve-cyber-security/article/530778/

[32] Catherine Wong, China Will Boost Cyber Deterrence Powers, Vows President Xi Jinping, 2016. Available: http://www.scmp.com/news/china/policies-politics/article/1937224/china-will-boost-cyber-deterrence-powers-vows-president