The History of Cyber-Kinetic Attacks and Incidents

THE FACT THAT CYBER-KINETIC ATTACKS rarely appear on mainstream news doesn't mean they don't happen. They happen more frequently than you would think. Many, for various reasons, aren't even reported to agencies charged with combatting them.

This hinders security experts in understanding the full scope and recognizing the trends in this growing problem. We'll highlight examples of cyber-kinetic incidents and attacks in this chapter. Some were malfunctions that, nonetheless, demonstrated cyber-physical system vulnerabilities. Some were collateral damage from hacking or computer

viruses. The vulnerabilities these exposed inspired a growing number of targeted cyber-kinetic attacks in recent years.

The Beginning

The previous chapter mentioned how the concept of using cyber-physical systems to disrupt industrial processes appears to date back to the early 1980s. The U.S. Central Intelligence Agency supposedly introduced defects into oil pipeline software that the Soviets were trying to steal from Canada. The flawed hardware was claimed by a former CIA operative to have caused a catastrophic explosion in a Soviet natural gas pipeline. Thus, the concept of cyber-kinetic attacks likely existed well before most people even had an inkling of the cyber-enabled systems that industries and energy distribution systems were developing.

Early warnings of potential problems

Early problems with cyber systems involved simple malfunctions. These malfunctions, however, demonstrated the damage that improperly functioning cyber systems could inflict.

Software glitches turn deadly - malfunction

Between 1985 and 1987, six individuals either died or suffered serious injuries from radiation treatment by machines with flawed software. The **Therac-25 radiation therapy machines**, in rare situations, showed the

equipment operator that the machine was properly configured for the prescribed radiation dose when it actually was configured to deliver a potentially fatal dose.

Although the manufacturer upgraded hardware components after the first two accidents, it neglected to consider software flaws as a source. The result was disastrous.

Continued equipment use, combined with manufacturer insistence that their equipment was incapable of producing the overdoses, led to four deaths before the flaws were uncovered. Clearly, the entrance of computer-controlled equipment into safety-critical systems revealed a need for more stringent coding practices. A 1993 investigation on these accidents, reprinted from *IEEE Computer*, Vol. 26, No. 7,[1] stated:

> *The mistakes that were made are not unique to this manufacturer but are, unfortunately, fairly common in other safety-critical systems. As Frank Houston of the US Food and Drug Administration (FDA) said, "A significant amount of software for life-critical systems comes from small firms, especially in the medical device industry; firms that fit the profile of those resistant to or uninformed of the principles of either system safety or software engineering.[2]"*
>
> *Furthermore, these problems are not limited to the medical industry. It is still a common belief that any good engineer can build software, regardless of whether he or she is trained in state-of-the-art software-engineering procedures. Many companies building safety-critical software are not using proper procedures from a software-engineering and safety-engineering perspective.*

So, as software entered the realm of controlling safety-critical systems, its producers were slow to recognize the need for more strenuous efforts to ensure that then-new technology would not open the door to unexpected dangers. How similar the situation then was to now, when producers of cyber-physical systems are slow to recognize the need for more robust security as those systems become ever more cyber connected.

Integer overflow coding error destroys a rocket - malfunction

The 1996 maiden launch of the Ariane 5 rocket by the European Space Agency ended spectacularly with a malfunction causing it to explode 40 seconds after lift-off. It took the European Space Agency 10 years and $7 billion to produce its own heavy lift launch vehicle capable of delivering a pair of three-ton satellites into orbit. It took a single coding error seconds to bring it crashing down to earth.

Dividing by zero leaves a warship dead in the water - malfunction

Another early malfunction was the accidental disabling of a U.S. warship in 1997 as it increased its reliance on computer controls. The **U.S.S. Yorktown** was touted as a great advance in Smart Ship technology. Computers closely integrated with shipboard systems enabled a 10% reduction in crew. Yet the software was not equipped to deal with bad data that a $2.95 hand calculator could handle with ease.[3]

The software crashed, disabling the propulsion system, when it

encountered data that asked the software to divide a number by zero. The ship had to be towed into port and required two days of maintenance to get it running again.

The software problem was ultimately corrected. No further incidents of this scope have been reported. You can be sure, however, that hackers of all types – especially the government-trained hacker armies mentioned in chapter 1 – have been inspired to explore ways to accomplish such disruption of military systems ever since.

Careless programming practices kill three people - malfunction

Lives can be put at risk when overconfidence of system developers and administrators leads to carelessness. That's what led to the **1999 Bellingham, Washington, gas pipeline rupture** that claimed three lives.[4]

Although the rupture was not solely the result of computer malfunction, poor network practices were a key contributor to the disaster. It is believed that an administrator was programming new reports into the system database without having first tested them offline.

This caused the system to become unresponsive during the pressure build-up that led to the rupture. The consequent fireball killed three people, injured eight others and released a quarter-million gallon of gasoline into the environment.

The role that administrator carelessness played in this will never be fully determined. The improper assigning of a single admin login password to all computer operators and the deletion of key records from the system shortly after the incident has prevented investigators from

completing their investigation into this area of the incident.

The careless practices that led to this disaster likely stemmed from overconfidence in the computer systems of that time to handle unexpected glitches. Our situation today is very similar. They pioneered computer-controlled systems. We are pioneering cyber-connected systems. We must be careful not to have the same overconfidence in systems' ability to compensate for the unexpected. Widespread cyber-connectedness today makes us vulnerable to even more devastating consequences if we fail to anticipate and act to prevent them.

The rise of hacking

Not all incidents in those early years were simple malfunctions. With growing access to systems on which critical systems depended provided by the internet, hacking surfaced as a threat.

These hacks, performed by young computer enthusiasts, usually were not intended to cause harm, but merely to demonstrate the hacker's skills. These hacks were far from harmless, though.

A young hacker disrupts a Boston airport – untargeted attack

A teen hacker in 1997 cut off communication systems in and around **Boston's Worcester airport**, including the control tower and crucial air-to-ground landing aids for over six hours.[5] Not only airport functions, but also the fire department and all emergency services in the area were

disrupted. This resulted in him becoming the first juvenile to be charged with computer crimes.

Authorities who charged him recognized that he did not anticipate that his hack would cause the harm that it did. The incident, however, was a clear indicator of the damage that a single hacker could inflict, and how vulnerable critical systems were to attack.

The first documented targeted attack

The **2000 Maroochy Shire wastewater attack** mentioned previously, on the other hand, was an intentional attack, designed by a disgruntled engineer to get revenge on the township that chose not to hire him. It showed the damage someone with knowledge of a critical system could accomplish, as he released more than 264,000 liters of raw sewage around the township, killing marine life and risking residents' health.

Slammer and the nuclear power plant - untargeted attack

A **2003 incident at the Davis-Besse nuclear power plant** in Ohio demonstrated another threat to cyber systems: worms and viruses that, although intentionally created, attacked randomly as they spread. In this case, the Slammer worm entered the nuclear power plant's system[6] through a T1 connection between a contractor's network and the plant's network.

This worm crashed several systems over the course of eight hours, including making core temperature monitoring systems unavailable for

more than five hours. Fortunately, the plant was shut down at that time for maintenance.

The frightening thing, though, is the damage this worm could have inflicted on a fully operational nuclear plant. Incidents like this showed the vulnerability of critical systems to malware, a now-common threat, as we will see later.

Also frightening is the fact that most Davis-Besse IT staff was unaware of the T1 connection through which contractors were connecting to the plant. Despite their best efforts to secure the plant, more entry points into the system existed than they knew.

With the complex web of cyber connections in today's world, the same potential exists for vulnerabilities to slip past IT professionals trained only in traditional security processes. The cyber-physical systems developing today have even more potential entry points to secure than the corporate networks at the time of Davis-Besse.

Trends in cyber-kinetic threats

With the exception of the Maroochy Shire wastewater attack, early incidents appear not to have specifically targeted their eventual victims. That changes as the 21st century unfolds. Now, a growing number of targeted attacks mix with accidental disruptions.

Oil and gas industry

Malfunctions in natural gas and oil pipelines

A **2010 San Bruno, California natural gas pipeline rupture**[7] occurred when deficiencies in the operating system allowed pressure to rise too high for a pipeline that was overdue to be replaced. This pipeline, running through a residential area, exploded in a fireball that killed eight people, injured 60 others and destroyed 37 homes. Although this was not a targeted attack, the blast shows how vulnerable pipelines can be to erroneous data in the SCADA systems that control the flow.

In another malfunction exacerbated by faulty SCADA systems, a **2010 oil line malfunction in Marshall, Michigan**[8] dumped 819,000 gallons of crude oil into the Kalamazoo River. SCADA deficiencies failed to trigger pressure alarms and delayed response to the spill, allowing the scope of the spill to far exceed what it would have been with a prompt response. Here again we see how SCADA systems not working as intended can cause massive damage.

Possible targeted pipeline attack

Malfunctions have not been the only cause of incidents in the oil and gas industry. A **2008 Turkish pipeline explosion**[9] may have been a targeted attack by Russian operators to cut off oil supply to Georgia at a time when geopolitical tensions were moving toward armed conflict between the two. The exact cause was not conclusively determined, but multiple vulnerabilities appear to have been exploited around the time of the

explosion. Lessons from this incident are important regardless of the actual cause of the explosion.

Confirmed targeted oil facilities attack

One incident known to have been a targeted attack was the **2008 attack on Pacific Energy Resources**[10] SCADA systems that monitored and controlled offshore drilling platforms and dams. As with the Maroochy Shire wastewater attack, a former consultant for Pacific Energy Resources sought revenge when the company turned him down for a permanent position. Using multiple user accounts he created without the company's knowledge, he transmitted programs, codes and commands to impair system functions. Fortunately, this attack did not cause major damage. The attacker's intent was more to annoy than to destroy. Had he wished, however, he was positioned to cause massive damage.

Water Utilities

Attacks on water supplies go back to ancient times and have always been an attractive target for making a statement. That remains true today, and automatic systems that control both water supplies and wastewater treatment offer new targets.

Malfunction in dam system controls

The most significant SCADA malfunction in water utilities was the **2005 Taum Sauk Water Storage Dam catastrophic failure**.[11] Discrepancies

between pressure gauges at the dam, 100 miles south of Saint Louis, and at its remote monitoring facility led to the release of a billion gallons of water. This release destroyed 281 acres of a state park and caused $1 billion of damage. Fortunately, no fatalities occurred and only four people were injured. Although not a targeted attack, it demonstrates the vulnerability of SCADA systems to incorrect data.

Untargeted water filtration plant attack

A **2006 hack into a Harrisburg, Pennsylvania, water filtration plant**[12] did not cause damage – the foreign hacker apparently intended to use the network merely as a tool to distribute spam emails and pirateware – but it raises concern because the hacker hacked gained control of a system that controlled water treatment operations.[13] It is unknown whether the hacker realized the sensitivity of the hijacked system or what damage he could have inflicted if so inclined.

Targeted water distribution system attacks

2011 Springfield, Illinois, water distribution malfunction [14] that destroyed a pump responsible for piping water to thousands of homes was initially blamed on Russian hackers. Shortly after the Springfield malfunction was revealed, a hacker operating from an address in Romania posted screenshots as proof of his **control over a similar water facility outside Houston, Texas**.[15] The Romanian hacker claimed that the facility had such poor security that he was able to gain access to it in less than 10 minutes. He came forward with his claim to dispute U.S. authorities'

claims that the Springfield incident gave no reason for people to be concerned about the safety of critical systems. Although this hacker sought to prove a point rather than cause damage, the ease with which he penetrated critical systems is a cause for concern.

As troubling as these water facility incidents are, perhaps the most chilling is the **2016 attack on an unnamed water facility**.[16] A hacktivist group with ties to Syria took control of hundreds of PLCs that controlled toxic chemicals used in water treatment. If they had more knowledge of the processes and chemicals they controlled, they could have inflicted mass casualties. Verizon Security Solutions, the company that investigated this breach, chose not to release the name or location of the facility because the many vulnerabilities Verizon found in the facility's systems would attract more attacks if known to the hacker community.

Industry

Manufacturing facilities, too, have been hit with cyberattacks. While earlier ones appear to have been untargeted, the most recent documented attack raises serious concerns over hacker capabilities and worker safety.

Untargeted industrial facilities attack

A **2005 Zotob worm attack on 13 of Daimler-Chrysler's U.S. automobile manufacturing plants**[17] left workers idle for almost an hour while infected Windows systems were patched. Estimated cost of the incident was $14 million.[18] The worm also affected systems at heavy equipment manufacturer Caterpillar, aircraft manufacturer Boeing and

major U.S. news organizations.[19] As with other worm attacks discussed previously, the attacks were not specifically targeted against the affected companies, but demonstrate how malware introduced into computer systems can cripple companies – even if only briefly.

Targeted steel mill attack

Perhaps the most famous attack on an industrial facility was the **2014 targeted cyberattack on a German steel mill**[20] that caused massive damage to equipment. In contrast to the hacktivist attack on the unnamed water facility, hackers in the German attack appear to have had extensive knowledge of industrial control systems.

Once they penetrated the corporate system, they worked their way into production management software and took control of most of the plant's operations. They disabled sources of human intervention on the systems and targeted high value equipment, including a blast furnace whose shutdown controls they disabled, overheating it until it was ruined.

Neither the source of nor motive for the attack were ever determined, and the plant, like the unnamed water facility, has not been identified. The attack, however, shows how much damage skilled and knowledgeable hackers can inflict on an industrial operation.

Demonstrations of industrial vulnerabilities

Although the scope of the attack on the German steel mill is presently not common, the vulnerability of industrial devices is frighteningly real. A **2017 test of industrial robots by security consulting firm Trend Micro**

showed a shocking array of vulnerabilities. They reported:

> *In our comprehensive security analysis, we found that the software running on industrial robots is outdated; based on vulnerable OSs and libraries, sometimes relying on obsolete or cryptographic libraries; and have weak authentication systems with default, unchangeable credentials. Additionally, the Trend Micro FTR Team found tens of thousands industrial devices residing on public IP addresses, which could include exposed industrial robots, further increasing risks that an attacker can access and compromise them.*[21]

Trend Micro demonstrated multiple attack vectors open for hackers to exploit. These attack vectors could introduce defects into the products being manufactured, sabotage robots so they are ruined – or even cause injury or death to equipment operators.

My own experience with industrial robots confirm their conclusions. In fact, in certain industries and in certain geographies, covert access to industrial control systems is almost a regular practice. The long-standing practice of industrial espionage now commonly branches into industrial sabotage as companies introduce barely noticeable failures into their competitors' processes to gain a competitive advantage.

Transportation

Transportation systems have also been attractive targets for cyber-kinetic attacks. Although the 1997 disruption at the Worcester airport was more collateral damage than targeted attack, it demonstrated the damage that

such disruptions could cause. Similar incidents, whether accidental, targeted or the result of controlled testing, reinforce this fact.

Untargeted rail attack

A **2003 shutdown of CSX Transportation system**[22] brought commuter, passenger and freight rail service to a standstill for 12 hours because of a worm infecting the system. Dispatching and signaling systems were compromised along much of the U.S. East Coast., demonstrating the wide-ranging affect that a single attack can have.

Targeted city transportation system attacks

We saw previously how the **2008 Lodz, Poland, takeover of a city tram system**[23] by a teen resulted in the first documented personal injuries. This, however, was not the first targeted takeover of a city transportation system.

Two years earlier, a **2006 hack of the Los Angeles city traffic system** disrupted traffic lights [24] at four of the city's most heavily used intersections for days. Two city employees caused traffic lights at those intersections to function in a way that snarled traffic in hopes of pressuring the city to give in to union demands in a labor negotiation. Here, again, we see how disgruntled insiders are capable of inflicting massive disruptions through a targeted cyberattack.

Demonstrations of transportation system vulnerabilities

Lest anyone dismiss such ancient (in terms of cyber time) threats as

having likely been eliminated, a **2014 test of the types of traffic systems used in many major cities** has shown how vulnerable those systems are not only to insiders, but to hackers, as well. Although traffic lights themselves appear to be secure, data from the sensors and control systems that determine how and when traffic lights change were found to be easy to intercept and replace with false data. Cesar Cerrudo, the security expert who conducted the tests stated:

> *[All] communication is performed in clear text without any encryption nor security mechanism. Sensor identification information (sensorid), commands, etc. could be observed being transmitted in clear text. Because of this, wireless communications to and from devices can be monitored and initiated by attackers, allowing them to send arbitrary commands, data and manipulating the devices.*[25]

Cerrudo was easily able to intercept data and gain enough information about the systems to reverse engineer them so that he could gain control of the data flow if he was within 1,500 feet of the targeted sensors. By use of a drone, he could then extend his distance from the intersection he was testing to the range of the drone.

Although newer versions of the sensors contain encryption, tens of thousands of vulnerable sensors remain embedded in intersections of cities around the globe, with no capability for upgrade other than ripping up the streets and replacing sensors with newer models.

Demonstrations of automobile vulnerabilities

Transportation vulnerabilities are not limited to transportation systems

and traffic controls. As vehicles we drive become increasingly able to recognize potential hazards and react to them, they also become more vulnerable to outside control.

Extensive research has gone into the **vulnerabilities of vehicles that have advanced safety features** that enable those vehicles to autonomously make safety decisions in place of drivers. At the forefront of this are **researchers Charlie Miller and Chris Valasek**, who have repeatedly demonstrated how automaker efforts to make autos as fully connected to the internet as smartphones comes with the threat of hackers taking control of everything from windshield wipers and radio to steering, brakes and even the ignition system.

Their **2015 remote hijacking of a Jeep Cherokee** made a big splash with the media and led Jeep to recall their vehicles to, with Miller and Valasek's help, patch the vulnerabilities. Although those particular vulnerabilities have been patched, Miller and Valasek warn that merely fixing one vulnerability is not enough to prevent determined hackers from taking control of onboard systems.

Miller and Valasek have since demonstrated even greater control that hackers could exert over a vehicle if they gained access to the onboard Controller Area Network (CAN) bus that coordinates communication between microcontrollers and devices in vehicles. Other researchers have suggested that a compromised smartphone or compromised plug-in monitor, like those provided by insurance companies, could facilitate remote access to the CAN bus for future vehicle hijackers.

In fact, such a CAN bus hack has already been accomplished. **Chinese researchers in 2016 took control of some functions on a Tesla S** when the vehicle's built-in web browser connected to a compromised

Wi-Fi network.

And, finally, in penetration testing in which my team was engaged, we were **able to gain partial control of multiple cars at the same time**. Unlike the Jeep or Tesla research that hacked a single vehicle, we could control multiple cars simultaneously.

Demonstration of drone vulnerability

In another penetration testing engagement, **my team overrode drones' geofencing system** (the system that enables government authorities to set up restricted airspaces to block drones from flying over airports, military bases, sensitive facilities and large public events). In a simulated test, we successfully bypassed geofencing protections and directed multiple drones straight toward previously restricted airspace. In other words, we demonstrated that safeguards to prevent drones from accessing restricted areas were not sufficient.

Demonstration of superyacht vulnerabilities

Another area of concern is with the growing development of superyachts for the very wealthy. Such vessels have moved from being floating luxury hotels for leisure activities to becoming floating business complexes from which owners direct their business operations. As such, the demand has skyrocketed for such vessels to possess cutting-edge communications technology.

In the rush to equip vessels with such technology, however, security has been almost wholly overlooked. A **2017 conference on superyachts** featured a sobering demonstration of how easily those poorly secured

systems can be compromised.[26]

Cybercrime expert Campbell Murray remotely took control of one superyacht, seizing control of navigation, satellite communication and the onboard Wi-Fi and telephone systems. He could do whatever he wanted with the ship and then wipe the system clean of any evidence of his hack.

His demonstration is not theoretical, either. Cybercriminals have already hacked superyacht communication systems to intercept owners' banking information and withdraw money from owners' bank accounts. They also have blackmailed owners by obtaining compromising photos or confidential information from shipboard computers. There have even been incidents of superyacht owners paying ransom to regain control of the hijacked navigation systems.

Demonstration of aircraft vulnerabilities

The holy grail of cyber-physical systems security research is remotely hacking a passenger jet. In terms of the impact to human lives as well as to the economy, a malicious hack of an aircraft could be one of the most impactful. Uncovering potential aircraft vulnerabilities and closing them before they are abused is therefore an active area of research of many governments in addition to the industry.

Unlike some of the other industries mentioned, aircraft manufacturers and airlines take the threat of cyber-kinetic attacks seriously and have been careful and deliberate in their adoption of digital technologies despite the multiple opportunities IoT offers to improve operational efficiency, increase personalisation to passengers and even introduce new business models.

That, however, didn't stop the researchers. In November 2017 an official from the U.S. Department of Homeland Security (DHS) announced that one year earlier a team of government, industry and academic researchers were successful in remotely hacking a passenger jet controls in a non-laboratory setting while parked on a runway.[27]

Ransomware attack on a major transit system

This last use of hacking a system to extort ransom is an example of a disturbing new trend: ransomware attacks. Ransomware is a recent strategy in which hackers take control of computer systems and demand money before they will release them to the rightful authorities.

A **2016 ransomware attack on the San Francisco municipal rail system** (Muni)[28] resulted in free rides for commuters, but no physical damage and little other effect on the system. The criminals behind the ransomware demanded 100 bitcoin (approximately US $73,000 at the time) to provide the encryption key to unlock the compromised system. The attack apparently was the result of random, automated scanning of web by the criminals behind the attack and Muni was fully operational within a day after the attack became known. Muni has released little information about the attack, but it appears that they were able to recover full use of their systems without paying the ransom.

Security experts found evidence that the cybercriminal behind the Muni attack had previously succeeded in extorting ransom from multiple manufacturing companies.[29] If this becomes an M.O. for cybercriminals, it won't be long before they start causing kinetic impacts to get their victims' attention and compliance.

Other ransomware attacks

Although Muni appears to have escaped their ransomware attack unscathed, others have not. Ransomware is becoming a booming business. The 10 ransomware programs known in January 2016 had grown to many hundreds by January 2017.[30] And the number and the use of them keep growing.

On a city library system

A **2017 ransomware attack on the St. Louis library system**[31] left all its libraries unable to provide services to patrons. Books could not be checked out or returned. Like Muni, the library system refused to pay for the encryption key. Unlike Muni, however, they were not as well prepared to recover from the attack. It took them nearly two weeks to wipe the entire computer system and rebuild it from backups.

On a resort

Not all victims have refused to pay. A **2017 ransomware attack on an Austrian ski resort** compromised the "smart lock" system at the resort.[32] Guests' key cards failed to unlock their rooms and the resort was not able to create usable new key cards for them. This attack hit at the beginning of the ski season, when all rooms were booked. The resort paid a demand of 1,500 Euros in bitcoin to enable guests to access their rooms again.

Foreseeing the future of ransomware attacks

Ransomware attacks to date do not appear to have been highly targeted. Most of them likely were similar to the Muni attack, where automated scanning software sought specific vulnerabilities it could exploit. As a result, targets so far have been random, either being well enough prepared to restore operations without paying the ransom, such as Muni and the St. Louis library system, or capable of providing only a modest payout, such as the Austrian resort.

Where the cybercriminals behind ransomware attacks have found the most profit is in manufacturing companies, such as the ones from which the Muni attacker was found to have successfully extorted ransom. Even with those, though, the data compromised were usually corporate data. The real threat from ransomware attacks lies in the eventual targeting of critical systems.

Researchers have already demonstrated possible attack vectors that ransomware criminals could use to seize control of ICS devices. One such attack vector was revealed at a 2017 ICS Cyber Security Conference:

> *[An] ICS security consultant, Alexandru Ariciu demonstrated ransomware attacks, which he called "Scythe," were able to target inconspicuous and less risky SCADA devices. The names of the targets are not revealed but he describes the affected devices as several types of I/O systems which stand between OPC servers and field devices. The devices run a web server and are powered by an embedded operating system. He says that a large number of these systems are unprotected and easily accessible online, which allows crooks to hijack them by replacing their firmware with a malicious code.*[33]

Being able to demand ransom not just for corporate records, but for a company's entire manufacturing capability will make ransomware a devastating threat for companies that fail to secure vulnerabilities in their SCADA systems and the IoT connections to them.

The massive May 2017 "WannaCry" ransomware attack on tens of thousands of hospitals, government agencies and businesses as large as Fedex and PetroChina across the globe[34] brought ransomware to wide media attention. It, however, is only the tip of the iceberg regarding the threat that ransomware poses.

A growing ransomware threat against hospitals

Most chilling are the ransomware attacks targeting hospitals. At least 19 hospitals were compromised by ransomware attacks in 2016[35] and 48 hospital trusts in the UK[36] alone – nearly 20% of UK hospital trusts – were documented from the May 2017 "WannaCry" attack, not to mention many others around the world. These ransomware attacks caused tens of thousands of cancellations of appointments[37] and even operations in some cases, and temporary hospital shutdowns in others.

Radiotherapy machines, oncology equipment, MRI scanners and other diagnostic equipment have been rendered useless when connected to hospital networks infected by ransomware. Critical care was delayed and the possibility of clinical mistakes multiplied. Some critical equipment required weeks to get it functioning properly again after an attack.

As hackers increasingly find monetizing their abilities appealing,

fears grow that the demonstrated vulnerabilities of medical devices will also become an avenue through which hackers seek to obtain ransoms. We'll look at that shortly.

Medical

Aside from the ransomware attacks on hospitals, most medical threats remain unfulfilled. We'll look at one incident of people with a medical condition being specifically targeted over the internet, and then look more closely at the growing threat of hackers targeting implanted medical devices.

An attack on epilepsy patients

In a **2008 hack of the nonprofit Epilepsy Foundation website**, the hacktivist group Anonymous flooded the Epilepsy Foundation's forum with brightly flashing graphics and redirects designed to trigger migraines or seizures in the epilepsy patients who frequented the forum.

No motivation has been found for this attack other than that it was intended as a sick and malicious joke. It shows, however, the damage that can be inflicted, under certain circumstances, purely through the internet.

Demonstrations of hacking implanted medical devices

We discussed in Chapter 1 the tests of pacemakers and defibrillators that led to then-U.S. Vice President Dick Cheney having the wireless functionality of his implanted defibrillator disabled in 2007 as a precaution against potential assassination attempts. Additional

demonstrations of vulnerable medical devices since then have raised awareness further.

A **2011 demonstration by Jerome Radcliffe on insulin monitors and pumps**[38] showed multiple ways to cause harm to insulin patients. He showed that signals from insulin monitors could be intercepted and overridden so that they displayed inaccurate data. As a result, patients relying on those readings would be at risk. Even more alarming, he found that insulin pumps themselves could be reprogrammed to respond to a hacker's remote, who could, conceivably, administer a fatal dose.

Not long after, another researcher, **Barnaby Jack, demonstrated even more advanced insulin pump hacks**.[39] While Radcliffe's attack vector was protected somewhat by the need for the hacker to first obtain the targeted device's serial number, Jack's approach enabled him to locate and control any insulin pump within 300 feet without the serial number.

This opens the potential for a new and terrifying form of attack. Many critical medical devices are listed on Shodan, a specialty search engine of internet-connected devices, **raising fears**[40] **that criminals could seize control of those systems and extort money** to keep patients alive.

Although Shodan is not yet known to have been used for any such attacks, it has already been misused as a tool to discover a wide variety of unprotected or poorly protected control systems.[41] It is only a matter of time before critical medical devices come into play for hackers.

Other attacks on physical well-being

Attacking medical devices or targeting medical conditions is not the only way to affect people's well-being. We could consider the **2016**

Lappeenranta, Finland, attack that shut down heating and hot water in two apartment buildings[42] mentioned previously an attack on well-being as well.

The same could be said about the **2017 unauthorized activation of emergency alert sirens in Dallas, Texas**.[43] All 156 sirens in the system were triggered at 11:45 p.m., Dallas time, through its wireless system. They were rendered unresponsive to shutoff codes, sounding for 95 minutes until workers deactivated the entire system.

Other than the inconvenience the sirens caused residents, no physical damage occurred from this attack, although the city's 911 system was flooded with more than 4,000 calls during the attack disrupting genuine calls. Under different conditions, an attack such as this could have caused mass panic.

Most likely, this attack was from young hackers challenging themselves to see how big of a "splash" they could make with their hacking skills. Whatever their motivation might have been, however, this incident raises concerns about another threat that cyber vulnerabilities present.

The threat of physical damage from hacks of poorly secured cyber-physical systems comes not just from hardened cybercriminals and highly trained cyberwarfare-trained agents of other countries. It comes also from curious kids who might cause kinetic impacts inadvertently by trying things out.

Power Grids

The effect of the Lappeenranta, Finland, attack may have been small, but

potential for attacks that affect vast swaths of people are real. Power grids that provide essential services to large populations are vulnerable.

Demonstration of generator vulnerability

The threat to power grids was dramatically demonstrated in the **2007 Aurora Generator Test**.[44] The test used a computer program to rapidly open and close circuits of a diesel generator out of phase. The generator exploded in less than three minutes.

The generator used was typical of most generators used in power grids, operating on protocols that were designed without security in mind. Failure of such a generator in an actual power grid could have caused widespread outages, or even the type of cascade failure experienced in the 2003 US Northeast blackout.

Targeted revenge attack

A less damaging – but still concerning – attack occurred two years later at a **2009 hack of a Texas power company**.[45] A fired employee of the company used his not-yet revoked authorization to cripple an energy use forecasting system, leaving the company unable to sell their excess capacity to other energy companies.

The unauthorized access targeted company profits rather than consumer access to energy. The situation, however, could have played out much worse. The fired employee had access to critical power generation systems and could have wreaked widespread damage to the power grid if he had chosen.

Targeted attacks on power grids in Ukraine

Real-life disruptions of power grids have occurred, with the **2015 BlackEnergy attacks on Ukrainian power grids**[46] being the first. These attacks, believed to have been conducted by Russian government-sponsored hackers, left more than 80,000 people without power.

Former U.S. National Security Director Michael Hayden said of the attack, "There is a darkening sky. This is another data point in an arc that we've long predicted."

Ever-present malware awaiting activation

In reality, the question is not so much *have* foreign hackers compromised power grids in their target countries, but *how much* of power grids are compromised. Researchers have uncovered **massive breaches that have given foreign hackers critical details of U.S. power grid infrastructure** from New York to California.[47]

Authorities believe that the means to strike U.S. power grids at will are already in place. This accords with my team's own observations. We regularly see malware in critical infrastructure systems, not doing anything presently, but just waiting on commands from their controllers wherever there is a bit of geopolitical tension.

Nuclear Power Plants

Perhaps people's greatest nightmare is the possibility of cyberattacks compromising a nuclear power facility. Chillingly, such systems have proven vulnerable to damage, either from simple malfunction or direct

attack.

ICS failures cause nuclear plant shutdowns

Failures within devices and software connected to plant ICS systems caused plant shutdowns[48] in the **2006 Browns Ferry shutdown** and **2008 Hatch nuclear power plant shutdown**. In the case of the Browns Ferry, Alabama, plant, excessive traffic on the control system network caused two circulation pumps to fail. An attempted software update at the Hatch Nuclear Power Plant near Baxley, Georgia, encountered a glitch that resulted in erroneous readings of water level that triggered an automatic shutdown.

In both cases, no widespread harm occurred. But both, again, demonstrate the vulnerability of critical industrial control systems to potential attacks that attempt to overload or insert false data into industrial control systems.

Targeted attack on Iranian uranium enrichment facilities

The **2009 targeted Stuxnet attack on Iranian centrifuges used to enrich uranium**[49] stands as the most damaging cyberattack known to-date. The attack, believed to have been launched by the U.S. CIA and Israeli government to cripple Iranian nuclear weapons development, may have destroyed as many as 10% of illegally obtained and operated uranium enrichment centrifuges at Iran's Natanz Nuclear Power Plant.

The plant, although isolated from the internet, was breached by targeting plant personnel with the Stuxnet worm, which then entered the

plant's network when personnel connected their infected computers to it. The Stuxnet worm appears to have been specifically tailored for the Iranian centrifuges.

The worm, however, by its very nature, could not achieve the surgical strike its attackers hoped. The need for it to spread widely in order to find access points through which it could attack led it to spread beyond its target. From there, it has been captured by hackers and modified to strike other targets. We'll look at that development shortly.

Unidentified targeted attack of nuclear facility

Finally, as with power grids, at least **one documented disruption of an unnamed nuclear power facility**[50] occurred in a two- or three-year period leading up to 2016. This is according to a high-ranking official at the International Atomic Energy Agency, who admitted that a cyberattack had disrupted a nuclear energy facility in that timespan. The location of the plant was not revealed.

Precautionary measures were launched to mitigate the attack, and no plant shutdown was required. No further details were divulged.

Growing threats

To the public, Stuxnet may seem like ancient history in the quickly changing cyberworld. Unfortunately, it is not ancient history to security experts. Its legacy remains a looming threat.

In many ways, the creation of Stuxnet to hamper the threat of Iranian nuclear ambitions opened Pandora's box. Stuxnet demonstrated

the feasibility of attacking vital systems through malware.

Furthermore, Stuxnet has not faded into history. It remains in the cyberworld as an ongoing threat to industrial control systems. Although it was specifically targeted for Iranian centrifuges, it has served as a model from which malware developers have created software that targets other SCADA systems.[51]

Stuxnet, however, is only one part of the growing body of threats. 2017 testing demonstrated the growing threat of ransomware targeting critical infrastructure.

David Formby, a PhD student in the Georgia Tech School of Electrical and Computer Engineering, and his faculty advisor, Raheem Beyah, the Motorola Foundation Professor and associate chair in the School of Electrical and Computer Engineering, designed a proof-of-concept ransomware that could take control of PLCs at water treatment plants, locking out authorized users and enabling them to introduce poisonous levels of chlorine into the water supply.[52]

And the massive May 2017 "WannaCry" ransomware attack on targets around the world only emphasizes the vulnerabilities present in our cyber-connected world. Ralph Langner, founder of German security consultancy Langner, said in light of the "WannaCry" attack: "For a competent attacker it would be possible to use the encryption vector specifically against industrial targets and force a production halt. We haven't seen that on a large scale yet but I predict it's coming, with ransom demands in the six and seven digits.[53]"

My own research confirms this degree of vulnerability. I have done a significant number of investigations of critical infrastructure providers,

such as energy, gas and water, in parts of the world where geopolitical tensions were escalating. My team almost always found malware present in their infrastructure.

The malware was not doing anything malicious. It was just there to provide a foothold for the attacker in case one day they decide to impact the service.

Based on the location, access rights and capabilities of the malware, we confirmed that the attackers indeed could have damaged the critical infrastructure if they wanted to.

Although we could eliminate the risks we found for our clients, identifying the attacker behind the malware is a different matter. It is always hard to determine the attackers with certainty. The best guess is always an adversary nation-state.

Takeaways

If nothing else, the attacks described in this chapter demonstrate that the threat of cyberattacks on critical systems are not hypothetical. They occur increasingly.

These malfunctions, attacks and research demonstrations are only a sampling of *known* incidents. Far more have been documented. Far more than those that have been documented have gone unreported or have only been hinted at by those charged with combatting them.

Many industries or organizations fear that releasing too much information about attacks will result in loss of public trust in them. Many fear that admitting to having been successfully compromised with make

them targets of further attacks.

Add those fears to the scattered patchwork of incident reporting channels and it becomes clear that it is almost impossible for security experts to see the true scope of the problem or to trace its underlying trends. Increased vigilance in protecting systems from cyberattack is essential to the safe use of the cyber-enabled systems on which we increasingly rely.

In coming chapters, we'll look at some of the specific threats, beginning with Stuxnet, and how they have been able to compromise systems. Ultimately, we will look at strategies for defending against threats and securing cyber-physical systems for a safer future.

---

[1] http://courses.cs.vt.edu/~cs3604/lib/Therac_25/Therac_1.html

[2] F. Houston, "What Do the Simple Folk Do?: Software Safety in the Cottage Industry," IEEE Computers in Medicine Conf., 1985.

[3] https://gcn.com/Articles/1998/07/13/Software-glitches-leave-Navy-Smart-Ship-dead-in-the-water.aspx

[4] https://pdfs.semanticscholar.org/3921/4bc7f02e067c6ac40cc3bf1eff1aaa4cc02d.pdf

[5] http://www.irational.org/APD/CCIPS/juvenilepld.htm

[6] http://www.securityfocus.com/news/6767

[7] National Transportation Safety Board (NTSB), *Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California*, September 9, 2010, NTSB/PAR-11/01, August 30, 2011, pp. 5-12.

[8] National Transportation Safety Board (NTSB). *Enbridge, Inc. Hazardous Liquid Pipeline Rupture*, Board meeting summary, July 25, 2010.

[9] https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf

[10] http://www.theregister.co.uk/2009/09/24/scada_tampering_guilty_plea/

[11] http://damfailures.org/case-study/taum-sauk-dam-missouri-2005/

[12] http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html

[13] http://www.gao.gov/assets/270/268137.pdf, pp. 16-17.

[14] http://www.bbc.com/news/technology-15817335

[15] http://www.itworld.com/article/2734691/security/illinois--texas-hacks-show-it-s-easy-to-take-over-u-s--water-systems.html

[16] https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

[17] http://www.eweek.com/security/zotob-pnp-worms-slam-13-daimlerchrysler-plants

[18] https://www.tofinosecurity.com/why/Case-Profile-Daimler-Chrysler

[19] http://www.gao.gov/assets/270/268137.pdf, pp. 16.

[20] https://www.sentryo.net/cyberattack-on-a-german-steel-mill/; https://www.wired.com/2015/01/german-steel-mill-hack-destruction/; http://www.bbc.com/news/technology-30575104

[21] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security

[22] CSX Transportation, "Computer virus strikes CSX transportation computers—Freight and commuter service affected (press release),"Aug 2003.

[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] http://articles.latimes.com/2007/jan/09/local/me-trafficlights9

[25] https://www.wired.com/2014/04/traffic-lights-hacking

[26] https://www.theguardian.com/world/2017/may/05/cybercrime-billionaires-superyacht-owners-hacking

[27] http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/

[28] http://www.securityweek.com/ransomware-attack-disrupts-san-francisco-rail-system

[29] https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/

[30] http://www.dailymail.co.uk/health/article-4149266/Chilling-menace-HACKERS-holding-NHS-ransom.html

[31] https://www.theguardian.com/books/2017/jan/23/ransomware-attack-paralyses-st-louis-libraries-as-hackers-demand-bitcoins

[32] http://fortune.com/2017/01/29/hackers-hijack-hotels-smart-locks/

[33] https://cyware.com/news/vulnerabilities-in-scada-enable-ransomware-attacks-16356dfb

[34] http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html

[35] http://www.dailymail.co.uk/news/article-3925240/Hackers-cripple-NHS-hospital-machines-demand-ransom-cash.html

[36] https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#595a136d425c

[37] http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-chaos-hits-thousands-patients/

[38] http://www.cbsnews.com/news/black-hat-hacker-can-remotely-attack-insulin-pumps-and-kill-people/

[39] https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack

[40] http://www.dailymail.co.uk/health/article-4149266/Chilling-menace-HACKERS-holding-NHS-ransom.html

[41] http://money.cnn.com/2013/04/08/technology/security/shodan/index.html

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

[43] https://www.wired.com/2017/04/dallas-siren-hack-wasnt-novel-just-really-loud/

[44] https://en.wikipedia.org/wiki/Aurora_Generator_Test

[45] http://www.theregister.co.uk/2009/06/01/texas_power_plant_hack/

[46] http://www.ibtimes.com/us-confirms-blackenergy-malware-used-ukrainian-power-plant-hack-2263008

[47] http://www.cbc.ca/news/technology/hackers-infrastructure-1.3376342

[48] http://www.safetyinengineering.com/FileUploads/Nuclear%20cyber%20security%20incidents_1349551766_2.pdf

[49] 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

[50] http://www.reuters.com/article/us-nuclear-cyber-idUSKCN12A1OC

[51] Eric Byres, "Next Generation Cyber Attacks Target Oil and Gas SCADA," Pipeline & Gas Journal, February 2012

[52] https://www.scmagazineuk.com/rsa-2017-researchers-create-ransomware-for-industrial-control-systems/article/638130/

[53] https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#595a136d425c