7.3 Cyber Attack and disruption

- Modern society is dependent on computer systems and the internet to maintain basic functions. They are increasingly used to run the infrastructure that supports dense, urban environments.
- Computer systems can face disruptions due to human error, intentional cyber-attacks, physical damage from secondary hazards, and electro-magnetic pulse (EMP).
- Cyber-attacks can take varying forms including amateur hacking, "hacktivism," ransomware attacks, cyber espionage, or sophisticated state-sponsored attacks. These attacks have the potential to cause internet or utility outages, leak or delete sensitive data and information, compromise critical infrastructure or services, or cause physical destruction.
- The City of Seattle faces daily threats of cyber-attack and disruption but has yet to experience a large-scale attack. The biggest concern is an attack on critical infrastructure such as the transportation, water, or power system. Manual backups still exist for these systems but would degrade overall service capabilities if it were required that these systems revert back to non-computerized technology.
- Cyber-attacks are becoming more frequent and sophisticated around the world. Despite improvements in security, the U.S. remains behind in mitigating the threat of cyber-attacks. Many experts believe that a major cyber-attack that will cause widespread harm to a nation's security and capacity to defend itself and its people by 2025.[377]
- Seattle faces a growing threat of cyber-attack as more of the city's infrastructure and basic functions are connecting to the internet. Traditionally non-computerized items (e.g. watches, thermostats, printers) are being connected to the internet and providing new avenues for hackers.
- While a catastrophic cyber-attack or disruption has not yet occurred in our world, the consequences of such attack in Seattle could severely harm the public and degrade or halt basic city functions and services.

7 3.1 Context

Today, the internet touches almost every aspect of our lives. The internet is a "network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless, and optical networking technologies." Seattle, like the rest of the world, has become incredibly dependent on the internet and digital systems to maintain basic city functions such as communications, public safety, critical utilities and services, transportation, business and commerce, and more. Cyber-attack and disruption is a hazardous threat arising from intentional or unintentional incidents that cause a breach in security, damage to digital devices and networks, or a network outage. Digital systems can be damaged by human errors, cyber-attacks, electro-magnetic pulse (natural or man-made), or physical damage as a secondary impact from another hazard. A prolonged outage to digital infrastructure could have catastrophic impacts for the community.

Many modern telecommunications systems rely on digital connections, including large components of Seattle's private and public communications networks. The City of Seattle's communications infrastructure is discussed in the Community Profile. While parts of the City's telecommunications still use analogue connections, many systems are moving towards Voice Over Internet Protocol (VOIP), or communications delivered over Internet Protocol networks. Disruptions to telecommunications are discussed here because of their strong tie to digital systems.

Causes

Electromagnetic Pulse (EMP)

Electromagnetic pulse is an intense burst of electromagnetic energy resulting from natural (e.g., solar storms) or man-made (e.g., nuclear and pulse-power device) sources. Both types can destroy or damage unshielded electrical and electronic equipment. Solar storms can induce extreme currents in wires, disrupting power lines, and causing wide-spread blackouts to the communication cables that support the internet.[378] There is still much we do not understand about how effective nuclear weapons are as EMP weapons, especially lower yield bombs that terrorists or small states would probably use. The scale and scope of damage caused by an EMP could vary considerably based on the type of device, and the altitude and latitude of the detonation. A nuclear device detonated at high altitudes (30-400 km) could generate an EMP with a radius of effects from hundreds to thousands of kilometers.[379] While it could disable electrical and electronic systems in general, it would pose the highest risk to electric power systems and long-haul communications.[380]

Physical Damage

Cyber disruptions can also happen as secondary effects from other kinds of hazards. Earthquakes, floods, and fires can destroy computer and network equipment. Most of the time the effects are limited due to the availability of back-up systems and the ability to route networks around problem sites. Nevertheless, if a significant network node goes down the effects could be wide-spread and possibly prolonged. Communications can be disrupted by physical damage to copper or fiber cables or radio equipment located on buildings. Damage to cables has accidentally occurred during construction or repaving projects, causing temporary internet and phone outages for thousands of customers.[381]

Indirect Effect

Other hazards or human error can have effects on digital networks and information. Power outages can create cyber disruptions. In 2006 many parts of Seattle lost power for days. Many individuals and small businesses had trouble powering computers and mobile devices. As computers become our primary tools for gathering information and communicating, their loss can endanger public safety and welfare. If the power goes out and fuel delivery to generator sites is impaired, bigger sites like communications hubs and data centers could go down causing disruption if they are not adequately backed up. Additionally, much of the City's communications equipment sits under high-powered sprinklers. If there was a fire in one of these buildings or a sprinkler head was knocked off, it could damage equipment and cause disruptions to City communications.[382] Human error can also play a role in cyber-related incidents. An unintentional release of sensitive digital information presents a potential threat to personal and financial security.[383]

Cyber Attack

The City of Seattle experiences attempted cyber-attacks on a daily basis but has avoided a major compromise so far. A cyber-attack is "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity."[384] Cyber-attacks are intentional and can be carried out by individuals, organizations, or government entities. They range from unsophisticated attempts made by amateur hackers using existing computer scripts, to sophisticated attempts sponsored or carried out by international governments. There are many types of attacks in between these extremes (see Table). "Hacktivists" are individuals or groups who use hacking to promote their social or political ideology. Additionally, threat agents may use ransomware, malicious software designed to restrict access to a system or data until a sum of money is paid.[385] Espionage and data theft could degrade public safety, expose the City to financial risk and the public to identity theft. In 2016,

Washington state victims of internet crimes lost over $24 million, mostly through fraud schemes.[386] Tactics used in cyber-attacks are always changing and becoming more sophisticated.

The U.S. Department of National Intelligence's 2018 Worldwide Threat Assessment states that multiple nation-state actors pose an increasing threat of cyber-attack to the United States in the next year.[387] The report goes on to say that while cyber-attack as a foreign policy tool has been mostly confined to low-level attacks, these state-sponsored actors have been testing more aggressive tactics in recent years. In 2016, the Department of Homeland Security stated that they were confident that Russia was responsible for hacking the Democratic National Committee (DNC) and leaking thousands of DNC emails during the presidential election.[388]

Table 7-1. Common Cyber Attacks and their Impacts

Type	Impact
Malware (ransomware, spyware, viruses, worms) Malicious software used by attackers to breach a network through a vulnerability, such as clicking a link, that automatically downloads the software to the computer.[389]	• Blocks legitimate access to components of the network • Installs additional harmful software • Obtains information by transmitting data from the hard drive • Disrupts components and makes the system inoperable
Phishing Fake communications (typically through email) appearing to be from a trustworthy source that allow hackers to obtain login information or install malware on a computer when someone interacts with their message.[390]	• Obtains a person's confidential information for financial gain • Obtains employee log-in credentials to attack a specific company • Installs malware onto a computer
Man-in-the-middle attack (MitM) Attackers insert themselves into a two-party transaction. Common points of entry include unsecure public Wi-Fi networks and computers affected with malware.[391]	• Interrupts a transaction to steal personal data
Denial-of-service attack (DoS) Attackers flood a site host or network with digital traffic until the target site/service cannot respond or crashes completely. A distributed denial of service attack (DDoS) is when multiple machines are used to attack a single target. Botnets, which are networks of devices that are infected with malware, are often used in DDoS attacks.[392]	• Legitimate users cannot access websites, online services, or devices • Slows down network performance
Structured Query Language (SQL) injection Attackers use malicious code on vulnerable servers to force the server to reveal	• Obtains contents of an entire database, including sensitive information • Allows attackers to modify and delete records in a database

information.[393] Can be done by submitting malicious code into vulnerable search boxes on websites.	
Zero-day exploit Attackers hack a network vulnerability before it is noticed and fixed by a patch or permanent solution.[394] Used by nation-state actors and sophisticated hackers.	• Allows attacker to plant malware into a system without the victim knowing

Computer Types and Threat Exposure

Computers permeate our society. Most of our financial and personal data is stored in networked computers systems along with our intellectual capital. They also control the machines that compose and maintain our infrastructure. Computers are increasingly being embedded into every day devices and products, such as phones, coffee makers, vehicles, home heating systems, and watches. Some of the networks connected to these computers are private, but most are connected to the Internet, the primary route for hackers.

General Purpose Computers

These are computers that built to handle many tasks. They include personal computers, most servers, tablets, and smartphones. They house most of our financial, organizational, and personal data as well as our intellectual capital. They are built from standard commercial off-the-shelf components like the Windows, iOS, or Linux operating systems. Being general purpose gives these computers great flexibility but also creates many openings for hostile actors to exploit. Being built from commercial components reduces cost but also means that the same hostile actors can achieve economies of scale when writing malware.

Specific Purpose Computers and the 'Internet-of-Things'

Specific purpose computers are systems with dedicated functions. A computer that assists in the control of a car or controls industrial machinery is a specific purpose computer. Many of these computers are embedded systems that are integrated into a mechanical or electronic device. It is estimated there are over 10 billion embedded systems world-wide.[395] They have a wide range of applications from consumer electronics, industry, transportation, medicine, facility management to defense. Miniaturization is pushing their integration into smaller and smaller devices. Where previously these devices were often isolated from the internet, more are now being connected. Everyday items, from printers to baby monitors, make up a growing body of objects connected to the internet, a term has been coined "the internet of things" (IoT). While this merging of the physical and digital world promotes greater efficiency and convenience, it also poses greater security risks. The scale of the interconnectedness of these devices and their information sharing is being taken advantage of by hackers. They attempt to infect large segments of devices at a time to access data, cause an internet outage, or attack other computers.[396] In 2016, two apartment buildings in Finland had their heating system attacked, leaving them without heat or hot water for over a week.[397] These devices also pose a greater management challenge for IT security departments. IT departments do not always know when a personal device, which can be more vulnerable to hacking, is connected to sensitive servers or databases.[398] Some identified vulnerabilities of these devices include opportunities to hijack communication channels, to access sensitive information, to disrupt vital services, and to alter signals and data for malicious purposes.[399]

Supervisory Control and Data Acquisition (SCADA) Systems

SCADA is a class of industrial control systems (SCADA can also be referred to as ICS – industrial control system, or OT - operational technology) that can include embedded systems, general purpose computers, and communications equipment. There are many specific types of SCADA systems. They provide real time data flow between sensors, workstations, and other networked devices in a system, as well as allow for monitoring and control.[400] They support both human-to-machine and machine-to-machine interfaces. They are used in power generation, transmission, and distribution; traffic control; water treatment, distribution, drainage, and waste; oil and gas transmission; dams; transportation monitoring; manufacturing; and communications. Many systems incorporate sensors to monitor infrastructure activity (e.g., water flow), a computer system that executes programs to control devices (e.g., a valve) based on sensed information, a database, and a human-machine interface to allow people to program them. Most are now linked on private networks to allow whole systems to be controlled. For example, all the devices in a water distribution system are linked to allow individual sites to behave appropriately given the status of the whole system.

SCADA systems are mainly vulnerable to attack because of issues in design, human interactions, and configuration.[401] Most systems are aging, and were not designed with cyber security in mind, but rather for processing efficiency. Older systems often relied on the "security by obscurity" principal - that the system would be secure as long as its design remained secret. Many now lack security features needed in our increasingly interconnected and sophisticated digital world. While many SCADA functions are machine-to-machine interactions, humans still interact with these systems on some level and can unintentionally provide access to an attack. Weak configuration of operational technology can make a SCADA system vulnerable, especially when it is connected to the internet for convenience. For this reason, many SCADA operators do not allow their networks to connect to the internet. Despite the prevalence of this policy there is pressure to connect and it is easy for staff to mistakenly do so. According to Shodan, a search engine that catalogues online devices, the U.S. has over 57,000 SCADA systems connected to the internet, more than any other country.[402]

Many SCADA operators are not patching systems (a patch is temporary software to address bugs and security vulnerabilities) for concern that it will cause system outages, that a bug in the patch itself will crash the system, that it is not needed because systems are not directly connected to the internet, and that the equipment is so old that there are no patches available. Some organizations simply lack the capacity and resources to keep up with patching.[403] Even if SCADA systems remain disconnected from the internet, past attacks have demonstrated that it is possible to deploy malicious code to computers that are not connected to the internet, as with the Stuxnet virus that was spread through infected flash drives. The U.S. Department of Homeland Security received 295 reports of SCADA-hacking incidents in fiscal year 2015, a 20% increase from the previous year.[404] Additionally, the U.S. Department of Defense has stated that while progress is being made towards more resilient infrastructure, these improvements are not on pace to achieve an acceptable level of risk within the next decade.[405]

7 3.2 History

2008 marked a cyber-attack turning point when the U.S. and Israel deployed a computer worm, Stuxnet, that destroyed Iranian centrifuges that are a key component of Iran's nuclear program. The event was the first documented of offensive cyber warfare that destroyed physical objects. It demonstrated that cyber-attacks can cripple critical, well defended infrastructure.

The following timeline comprises state, national, and international events that show the consequences of cyber-attack and disruptions.

2003. A power company representative unintentionally executed malware resulting in power outages for the Northeastern U.S. and part of Canada. The malware disrupted power grids across multiple states.

2008. Hackers disabled alarms, communications, and caused a crude oil refinery on the Turkish pipeline to explode, destroying operations and facilities.

2009 (Local). An electrical fire took Fisher Plaza data centers offline, bringing down several eCommerce sites including a credit card validation service. It was the third time Fisher had experienced downtime.

2014 (Local). Most of Washington State experienced a 6-hour 9-1-1 phone system outage due to human error. Around 4,500 calls went unanswered.

2015. The Deputy National Security Advisor confirmed that Russian hackers compromised a non-classified system over a several month-period to obtain information about the President's activities.

2015. As many as 22.1 million government employees, contractors, and other personnel records stored within the U.S. Office of Personal Management were compromised by a cyber-attack traced back to the Chinese government.

2017. A ransomware virus called WannaCry effected over 230,000 computers throughout the globe.[406] It did not require any user interaction to spread, but rather took advantage of vulnerable public-facing Server Message Block (SMB) ports. Boeing was attacked with the virus, but the vulnerability was small and there was no interruption to business.[407] It affected the UK's National Health Service, causing system outages at hospitals and forcing ambulances to be rerouted. It was the first time the UK convened its emergency committee due to a cyber-attack.[408]

2018. The City of Atlanta, Georgia and the Colorado Department of Transportation were hit with ransomware called SamSam. In Atlanta, attackers requested $51,000 in cryptocurrency to restore the city's data. It also caused a multi-week outage to Atlanta's website, hindering utility payments, business licensing, ticket processing, and court functions.[409] The attack also erased Atlanta Police Department's dashcam archives.[410] Colorado faced multiple attacks in the span of weeks, with the ransomware mainly affecting employee computers and not critical transportation systems.

2018. A borough in Anchorage, Alaska and the City of Valdez, Alaska suffered a ransomware attack that remained dormant in their computer systems for weeks before doing any damage.[411] Over 650 computers were compromised, and phone and email systems were inoperable. The borough manager in Anchorage declared the attack as an emergency.

7 3.3 *Likelihood of Future Occurrences*

The World Economic Forum predicts that the number of devices connected to the internet will grow from 8.4 billion in 2017 to 20.4 billion in 2020, greatly increasing the risk of cyber-attack.[412] Many experts believe that a cyber-attack on critical infrastructure will happen in the future. In 2014, the Pew Research Center asked 1,642 experts in internet evolution and technology if they think by 2025, a major cyber-attack will have caused widespread harm to a nation's security and capacity to defend itself and its people (widespread harm being defined as significant loss of life or property losses, damage, or theft at the level of tens of billions of dollars).[413] Sixty-one percent of experts said yes, citing the increase in sophisticated tactics in recent years, the history of successful attacks on infrastructure (Stuxnet), and the fact that security was not the main priority in designing the internet. The major uncertainty that remains is how widespread an attack would be. Smaller attacks have already occurred that display the potential for major harm. San Francisco and Sacramento have both faced ransomware viruses on their metro systems. Additionally, an undisclosed municipal water system was hacked and had its levels of treatment chemicals changed, affecting 2.5 million customers.[414]

The City of Seattle is constantly facing attempted cyber-attacks on its digital systems. Most are minor and unsophisticated, but it is only a matter of time before a more sophisticated attempt is successful. The type of attack and extent of the damage is very difficult to predict. The recent ransomware attacks on Atlanta, Colorado, and Anchorage could signal that state and municipal governments are increasingly

becoming a target for ransomware. Many government agencies face limited cyber-security budgets and capacity, which could make them an attractive target to the attacker. However, limited fiscal resources also make them less attractive in terms of potential monetary gain.

Seattle is a world leader in the technology and software industries. The city will continue to be on the cutting edge of implementing new technologies and devices that are connected to the internet. If cyber-security does not improve at the same pace, Seattle will face an increasing likelihood of cyber-attack.

7 3.4 Vulnerability

The density and interconnectedness of Seattle and its service network make it especially vulnerable to cyber-attack and disruption. Seattle routinely ranks high on Government Technology's Digital Cities Survey, which recognizes cities using technology to improve citizen services. In 2017, Seattle ranked 6th for cities with populations over 500,000, slightly down from 4th in 2016.[415] Critical facilities such as hospitals, fire stations, emergency medical services (EMS), and 9-1-1 centers are all increasingly relying on new technologies, which also makes them vulnerable to attack. If their functions were to be disrupted or compromised by hackers, it could threaten the safety and survival of people. Most of these emergency service facilities have back-up generators or battery backups that would allow them to operate during an outage but remain vulnerable to other types of attacks that would limit or interfere with their service capabilities.

Seattle relies on SCADA systems for many of its basic functions including maintaining and monitoring the water and power systems. In 2015, Seattle City Light (SCL) began implementing a new Energy Management System, that modernizes their SCADA system from the 1980s. The new system allows SCL to utilize more "smart grid technologies," such as wireless meters that automatically track wattage and transmit data.[416] Seattle Public Utilities (SPU) also underwent a major upgrade to their SCADA system in 2015.[417] Seattle's water transmission and distribution systems are mostly gravity feed which means that pumps are less important that in many other regions. Less reliance on pumps reduces the water system's vulnerability to cyber disruption. However, if control of the water or sewer system is compromised there could still be public health and environmental consequences. Despite these upgrades, the SCADA systems that the city relies on are still vulnerable to an attack that could disrupt essential water, sewer, power, and heating services.

The City of Seattle began working on "smart city" initiatives in 2015. The initiatives focus on implementing new digital technology to improve city functions, such as traffic lights that can adapt to traffic levels and sensors around the city to provide real time environment and activity data.[418] While these initiatives will bring important information and convenience to the city, they also make Seattle more vulnerable. Increasing the amount of infrastructure that relies on computing technology and the ability to connect to the internet also increases the number of avenues hackers have for an attack.

The "smart" city vulnerability is particularly salient for transportation. As more and more of our transportation systems become "smart" we incur a greater the risk that cyber-attacks and malfunctions will cause disruptions to our transportation system or worse: harmful or fatal accidents. All modes of transport: roads, rail, air, and marine all have major computerized components. These computers run signals, communications, controls and vehicle subsystems. An attack that gains control of these systems could cause major vehicle collisions. One study found that it is possible to hack semi-trucks to take over acceleration functions and remove breaking capabilities when the vehicle is at speeds under 30 mph.[419] The same study concludes that these types of attacks are not just limited to the software on semi-trucks, but most other vehicles as well.

As communication networks move towards using VOIP services, they are becoming vulnerable to attack and other digital disruptions. Many critical services, like EMS and utilities have their own radio networks

or satellite phone capabilities to ensure they can still communicate in the event of an attack or natural disaster that disables their VOIP systems.

The Seattle region is home to many large companies that support the local economy such as Amazon, Boeing, and Microsoft, among others. A significant attack on one of these companies that either compromises consumer information or halts business operations would have negative economic implications for regional business. Seattle is also very trade-dependent. The large amount of products and money that move through the port makes the city's trade and business operations a target for cyber-attack.[420]

7 3.5 Consequences

Washington State estimates that a successful breach of critical networks could "severely diminish or destroy basic public utilities, fuel, health care systems, EMS, communications, and governance to at least 50% of the state's population."[421] An extended, local network outage would similarly halt most city functions. It would also harm the local economy, as many businesses would not be able to function. A City data breach that compromises consumer information could cause damage to the City's reputation and trust of its citizens.

The consequences of an attack on city infrastructure would depend on the systems affected and the problem's severity. The worst failures would affect SCADA systems that control critical transportation, power, water, health care, public safety, sewer, finance, and communications systems. While manual workarounds can be implemented, they greatly degrade overall system performance. In most cases the damage from computer failure will be temporary, but in some cases, it could cause physical damage. For a cyber-attack on infrastructure to be most effective, most experts conclude that physical attacks and sabotage would also be involved.

The loss of control over the water SCADA system could force Seattle to rely on manual backup systems that would reduce overall efficiency, and potentially cause a temporary water shortage. Experiments have demonstrated that it is possible to destroy electrical generators by sending them instructions that cause them to overheat.[422] Attacks or accidents could also damage turbines in power generation facilities. Losing generation facilities would reduce Seattle's power capacity and could lead to brownouts especially if an attack on the power system occurred during peak demand (during the winter in the Pacific Northwest).

Physical attacks on infrastructure could also lead to cyber disruptions. The City of Seattle has built two data centers outside of the city, one in Spokane and one in Tukwila, to provide for continuity of operations in the event that local infrastructure is damaged. Terrorist groups and individuals who seek to harm the U.S. and Seattle may turn to cyber-attacks. There are cases of state-sponsored cyber-attacks that have damaged and destroyed critical infrastructure.[423] It is also possible that a conventional attack could be aided by cyber-attacks that disrupt a target's ability to respond. It is even more likely that terrorists would use cyber-espionage to collect intelligence on a target before a physical attack in order to make the attack more successful.

Some of Seattle's natural hazards such as flooding, or earthquakes can cause physical damage that triggers cyber disruption. The cyber disruption could feed back into the consequences of the primary hazard. Having good business continuity plans (BCP) or continuity of operations plans (COOPS) in place will greatly reduce the risk of cyber disruption following natural disasters.

7 3.6 Conclusions

Institutions in the Seattle area face hacking attempts every day. The vast majority of these are not successful, but it only takes one success to cause a major compromise. Moreover, due to the interconnected nature of modern society, Seattle's public and its institutions are dependent on

organizations scattered world-wide. A compromise anywhere in the world could have major consequences for Seattle. Even though computer compromises and data theft pose a significant threat, the world has not yet seen a major disaster precipitated by cyber disruption whether accidental or intentional. Our perception of the severity of cyber-attacks seems to be changing. What once would have been considered a major attack, such as the 2016 WannaCry ransomware virus, is now becoming more commonplace in our computer-dependent world.[424] It is likely we will see an increasing number of cyber disruption incidents and attacks, but the severity of the direct or indirect effects on Seattle are still unclear.