The Internet of Things, Critical Infrastructure, and Terrorism

Wesley Street

Missouri State University

May 10, 2017

Introduction

The past 30 years has seen the growth of cyber technology in our daily lives. From desktop computers to laptops to mobile devices and finally connected appliances. All of these developments have increased processing speed while reducing the footprint of the associated technology. One of the more recent developments in this field is the increasing number of connected, or "smart," devices. These connected devices have increased the quality and efficiency of life while reducing costs.

The Internet of Things (IoT) will continue to expand with more and more connected devices. TVs now connect directly to the internet to use streaming media. People can lock or unlock their front door from their phone. Security cameras and baby monitors connect wirelessly to be accessible by the owners from anywhere. There was a website with tens of thousands of camera feeds streamed from the internet simply by the owners using default passwords (Smith, 2014). It seems like every day there is some sort of new fitness tracker or wearable device collecting biometric data. While these are a little more secure simply by the fact they are usually are paired through a mobile phone, it does not make them invulnerable to exploitation.

Connected devices have also developed a new threat vector to cybercriminals, terrorist groups, and state actors. The vulnerabilities and methods examined are not exclusive to terrorism. They are also employed by hackers, criminals, and state actors. The approach used and targets selected by terrorist verses the others, besides maybe state actors during a conflict, differentiates between the terrorist and the criminal. However, it can still be blurry trying to distinguish between a hacktivism, cybercrime, cyber espionage, and cyber warfare. A political

hacktivist group could inadvertently or on purpose become cyberterrorists based on the size and scope of the attack employed.

Defining Internet of Things and Critical Infrastructure

Before a in depth examination can be made of the threat, it is important to try to define the Internet of Things (IoT). Different experts have different opinions but also consistently have two of the same components: 1) internet connectivity and 2) some type of built in processing power. Many also include a sensor of some type and the ability to connect wirelessly. Essentially these processors are connected to a network, often the internet. Various experts will lump in laptops and mobile phones while others do not, citing that these devices have more robust defenses and possess the capability to defend against cyber threats (CIO, 2016, p. 1; Lewis, 2016, p. 1-2).

Infrastructure is typically thought of as physical assets like bridges, roads, utilities, and communications. Critical infrastructure would be physical and virtual facilities contributing to national defense, economic resilience, and the health and safety of the population (Simon, 2017, p. 2). The Department of Homeland Security (DHS) has identified 16 sectors of critical infrastructure, in which a disruption would be detrimental to national security. Many of these areas use connected sensors, whether it is a chemical plant producing the powder for fireworks, a dam monitoring water levels, a defense contractor assembling the newest military vehicle, the energy sector transferring electricity through connected switches, or automated processes within a cellphone tower. Many farms use connected devices to measure soil, moisture, and many other variables. Hacking one of these could lead to the destruction of a season of crops. While this

would be inconsequential at a micro level on a single farm, except maybe to the farmer, a wide spread attack against multiple vulnerable systems could lead to a food shortage.

History

Some of the original systems were originally known as ICS (industrial control systems). These originally were contained within proprietary networks without outside access. With the advent and popularity of the internet, a newer generation of devices we able to connect to it and allow access and visibility to a larger audience. What would have once required an offsite executive to call or visit a manufacturing plant was now available via local internet access. The collection and control of this information is typically called supervisory control and data acquisition (SCADA) with copious amounts of data being continually collected and warehoused (Simon, 2017, p. 2).

Because of the miniaturization of mobile technology and improvement in efficiency extending battery life, a whole new range of consumer electronics have been created. We now have refrigerators that are connected to the internet. With a person's mobile phone, he or she can sign in and look at what is in the refrigerator while out shopping. A house can have a smart thermostat installed and allow a home owner to adjust the thermostat remotely. People use wearable activity monitors which continually collect positional and biometric data about the wearer.

The medical field has also embraced these advances. Pacemakers can now be installed with Bluetooth or Wi-Fi connectivity. This would allow a patient's doctor to monitor his or her medical condition remotely. Connected insulin monitoring and pumps allow a parent to monitor

a child's blood sugar, and this real-time monitoring allows more accurate insulin delivery. Many other medical devices are becoming available with the ability to connect.

Infrastructure has also leveraged these advances to improve services while decreasing costs. SCADA still remains at the heart of infrastructure's IoT expansion. Electric utilities are using live SCADA information to look for lightning strikes on electrical transmission lines to improve response times and accuracy of crews dispatched. Homes are now equipped with "smart" thermostats which report usage data back to the utility and help companies analyze usage to run more efficiently. The State of California has mandated the use of these devices (Lewis, 2016, p. 9).

Vulnerabilities

There are many security vulnerabilities within the scope of the Internet of Things. The first and most pervasive is the human factor. People want rapid and easy access to their creature comforts. This means a majority of people not knowing or caring to change the passwords for the default values. For example, if a connected refrigerator was sold to 10% of new housing construction with the default values being "admin" for both username and password and 90% of owners changed these, it presents a substantial number of newly vulnerable points. The US Census Bureau reported 819,000 single family housing completions in March 2017 and using the numbers above leaves 8,190 unsecure points. When extrapolated over the course of a year would mean over 98,000 in a year just from this single point of origin.

Another problem is hardware and software weaknesses. The size of the devices make built in firewalls and malware defenses difficult to employ. IoT devices are produced with weak

or non-existent encryption protocols. This can be especially complicated in battery powered devices, such as a pacemaker, because this encryption reduces battery life. Once a company sells a device, there is no requirement for them to produce firmware upgrades to patch issues or even continue to support a product like computer and software manufactures do. There is also the problem of where many of these devices are made. Items can be counterfeited or subverted to have spying software or hardware installed, this is called Provenance (CIO, 2016, p. 1,4).

Lastly, it is becoming more common for users to not have the ability to change security settings or passwords even if they were inclined to do so. This could mean that if a vendor goes out of business, support disappears without the owner knowing. It would also mean that patching and updates would also cease (CIO, 2016, p. 4). In the case of the "smart" thermostats in California, the utility company can take control of the thermostat and make adjustments while locking the user from altering these changes.

The U.S. Government does not have a single federal agency overseeing security of IoT devices. Instead it has several separate agencies regulating their small slice of the pie. The Federal Communications Commission regulates the electromagnetic spectrum used by devices to communicate. The Federal Trade Commission monitors and regulates consumer electronics, including privacy and security. DHS coordinates security between sectors of critical infrastructure (Fisher, 2015, 8-9). The European Union is also examining the security and privacy issues and how to regulate them. It wants to ensure interoperability of these devices while protecting users (Davies, 2015).

Methods of Attack

While there are many ways to exploit a vulnerability, the two most applicable to terrorism would be the ability to take over, or hijack a device, and either use the devices for nefarious purposes or attack the device itself. When hijacking a device, the hacker exploits a vulnerability and loads malware giving control to the hacker. This can give the hijacker access to the information collected. While the data is not always relevant in itself, the conglomeration and analysis of big data can provide intelligence information to a terrorist cell. If a specific device is able to be accessed, it could provide targeting and location information. These hijacked devices can also be used inside of a Botnet. This is a system of hundreds, thousands, or even millions of nodes with which to launch a denial of service (DoS) or directed-denial of service (DDoS) attack.

Vulnerabilities can also be exploited to allow devices to be attacked directly within a network. A sophisticated attack would destroy or damage the device in question while spoofing the SCADA stream making everything appear to be ok until it is too late. Verizon reported numerous intrusions in to a water utility's SCADA system due to it using an IMB AS/400 system which was introduced in 1988. There are several companies within the oil and gas industry that either still use AS/400 or have recently transitioned away from it. A 2015 Dell report showed that attacks against SCADA systems had increased 400% between 2013 and 2014 (Simon, 2017, p. 5).

Past Attacks

There have been several notable attacks on IoT devices or by IoT devices. While not directly related to terrorism, they should serve as examples of methods a sophisticated enemy could employ against the U.S. The Stuxnet worm caused the closure of an Iranian nuclear plant. It caused permanent damage to centrifuges being to enrich uranium for the Iranian nuclear program. It was able to accomplish this by spinning the centrifuges out of control while reporting the system was functioning normally. This system was actually not connected to the internet but was most likely infected with a USB thumb drive (Simon, 2017, 4, 7, 8; Fisher, 2015, p. 15).

In September 2016, a major DoS attack using IoT devices occurred against Dyn. The attack prevented users from being able to access popular websites like Twitter and Netflix. Level 3 Communications (L3) monitored this attack with 150,000 IoT devices being exploited generating 500 gigabits per second of traffic. This consumed a significant amount of globes internet bandwidth. It is also notable that this used just a fraction of the total available node to perform this attack (Drew, 2016, p. 3; Walden, 2016, p. 1; Schneier, 2016, p. 1-4).

In 2014, the German government released an annual report in which they note a malicious actor had attacked a steel mill. By using a phishing email, the actor compromised the corporate network and then the mills network. The actor was then able to cause multiple components to fail and cause permanent physical damage. A 2008 explosion at a pipeline in Turkey was the result of a cyberattack while Russian based hackers caused blackouts in Ukraine by taking control of SCADA systems (Simon, 2017, p. 1, 8).

Terrorist Applications Toward Critical Infrastructure

There are multiple uses for terrorists exploiting IoT devices depending on goals, resources, and level of sophistication. On a small scale, control of a localized botnet would have regional impacts. Returning to the use of a "smart" thermostat, if a terrorist could control a considerable number throughout a county or large municipality and activate all the air conditioning units at once, it could cause regional brownouts and blackouts. While there may not be a loss of life during this event, it could certainly cause panic. It would be a significant propaganda tool for the terrorists and be psychologically detrimental to the target. It would be the terrorist version of the U.S.'s "Shock and Awe" campaign against Iraq.

Many natural gas utilities use IoT devices for monitoring and regulating flow of gas. If these were to become compromised, significant localized damage could be inflicted. Once again, the loss of life could be minimal but the fear and propaganda value would be significant. An attack on the manufacturing, chemical, or communication sectors could also have, mostly localized, effects.

Many of the options available to terrorists would be a DoS attack. Without a way to directly access connected devices, a group could still have an impact by denying that access to others. It could create a DoS attack against a utility with possibly the same results at taking over utility devices themselves. It could also be used in conjunction with a terrorist attack. What if the Boston Bombers were sophisticated enough to have engineered a DoS attack against local police, fire, and medical services at the same time? They should have increased the number of casualties by slowing the response and possibly they would have had more time to try to elude police custody.

Two main examples used when considering cyberterrorism attacks on infrastructure is attacks against dams and nuclear power plants. The dams sector includes dams, levees, navigational locks, and other water control systems. A DoS could be used to prevent navigational locks from operating causing financial damage from goods not being able to be transported and possibly physical damage to the system. It could be used to prevent control stations from being able to communicate with dams. A more sophisticated and subtle attack would prevent dam spillways from operating as designed, causing permanent damage and possibly a catastrophic failure, leading to loss of life and property.

While the Stuxnet worm served as an example of an attack against nuclear and defense infrastructure in Iran, a similar attack could be launched against U.S. facilities (Fisher, 2015, p. 15). U.S. nuclear facilities must incorporate robust physical and electronic countermeasures; however, as in the Iranian case, it still relies on humans which are fallible. At the same time, the U.S. nuclear infrastructure ages and becomes more susceptible to the newest threat vectors.

A sophisticated terrorist could also use directed IoT vulnerabilities in directed attacks and assassinations. Accessing a "smart" electric meter of thermostat could remote monitoring if someone was at home. There is ever increasing autonomy in automobiles. If a bad actor were to hack in to a self-driving car, they could create a deadly auto accident or divert the vehicle to a specified location to abduct the individual.

Other problems

In Managing Risk for the Internet of things, Lewis argues that when weighing the advantages of IoT against disadvantages, the advantages outweigh any negatives. For example,

Lewis states that the inherent safety of interconnected and self-driving cars outweighs any lives lost due to malicious activity when compared to all the lives currently lost due to automobile accidents. While on the surface, this general assumption seems logical, it fails to account that these deaths caused would be purposeful at the hand of a bad actor. According to the National Highway Traffic Safety Administration (NHTSA), 23,695 people were killed in automobiles and 2,230,000 injured in 2015 (NHTSA, 2016, p. i). Would society accept a nominal zero-accident rate if they knew that 1,000 people were dying because their cars were hacked? I think this statistic, even though you are safer, would cause a panic and lack of faith in the system. This type of widespread fear is exactly the type of thing a terrorist group would want to exploit (Lewis, 2015, p. 4).

Lewis continues his thesis that there is little chance that a malicious attack on an IoT device would produce mass casualties or major economic damage like 9/11 did. These attacks amount to pranks with little physical consequences. While this is probably true about the scale of the attacks, it does not make it unlikely that at least an attempt would be made. Lewis seems to think that terrorists only understand inciting terror through violent actions while at the same time acknowledging that the repeatability of an IoT attack would also determine its psychological. When Lewis wrote his paper, he stated that as of February 2016, there had be no IoT incidents (Lewis, 2016, p. 4-10). It would be interesting to revisit this in light of the Dyn attack. Terrorist groups are increasingly successful in recruiting technologically sophisticated members as demonstrated by Deash's successful public online presence. It should be expected that the group has also been developing more clandestine means as well.

Lewis does make an excellent point that most research and discussion in IoT security is vulnerability and the need to harden IoT devices. Just the mere vulnerability of a device does not

mean that it will be hacked. Most devices would not be useful to a terrorist or any other type of bad actor. Just because this device does have poor security does not mean it would be targeted. Upgraded security would need to be measured against the need for speed and efficiency. IoT security upgrades should first be targeted at vulnerable systems (Lewis, 2016, p. 15-16). He does not discuss botnets because he removed this from discussion earlier, stating that DoS defenses will become stronger, so the threat of a botnet is no longer a relevant one (Lewis, 2016 p. 8).

Case Studies by the Department of Defense

The Department of Defense (DoD) policy paper contains several case studies outlining positive aspects of using IoT devices, some of their vulnerabilities, and recommendations to prevent vulnerabilities from being exploited. First is a DoD fuel depot using IoT devices to monitor take levels, inventory, system conditions, and security sensors. This would enable operators to track conditions without being physically present. The threat would be a bad actor hacking into this system and changing reported conditions. If the tanks were empty but reporting as full, a military unit arriving to refuel would be unable to. This could cause a sever hindrance in operations. It could also be possible for this bad actor to damage the system in such a way to create a fire or explosion. Next is a smart building. It uses a network of sensors to increase efficiency and reduce waste in utilities. It would also aid in finding the location of employees, fire and smoke, or even assigning conference rooms and parking. This would allow a bad actor to monitor the presence of who and what organizations were working. It could potentially enable monitor sensitive conversations.

The third case study involves an attack on an executive vehicle. Many cars already have the ability to be disabled or unlocked remotely with services like On-Star, or if an automobile collision, the system automatically contacts On-Star to dispatch emergency services to the location. If a bad actor was able to hack into this system, he could listen to conversations or disable a vehicle in a designated area and unlock the doors to enable an abduction of a senior government official. The last vignette is battlefield situational awareness: connected communications between soldiers, air power, and commanders. This greatly increases the speed of reactions while reducing fratricide and collateral damage. This comes at a cost of letting traditional skills atrophy. A bad actor hacking the system to interject bad information could derail operations or give him the ability to monitor and track those fighting him.

All of these case studies revolve around prioritizing and addressing the highest risk vulnerabilities. They all involve the need for simple but robust encryption and maintaining up to date protocols and standards in which all users can participate. The idea of using IoT devices at the tank farm requires these devices to reach a certain level of security to be attained on its own. Also important is ensuring that devices are not tampered with during the procurement process. While none of these would lead to devastating terrorist events like 9/11, it would enable attacks against the U.S. to be more successful. It could also lead to more battlefield successes for Daesh against the coalition forces fighting them in Iraq and Syria.

Examples in Fiction

The use of IoT devices is also found in fiction. In the James Bond movie *Tomorrow Never Dies,* an arguably terrorist organization steals a GPS encoder device. It is used to alter

GPS coordinates and a Royal Navy destroyer sunk because of it. While this is a fanciful movie plot, a bad actor figuring out how to spoof a GPS signal could be a major disruption to infrastructure. When considering the reliance that people place on positional location on their phones, in their cars, and in the air traffic control system, it could quickly become a major issue. It could have catastrophic impact on IoT devices within critical infrastructure that rely on positional data.

In the Mark Greaney's most recent Tom Clancy novel, True Faith and Allegiance, a shadowy private company is providing terrorists with information about people based on a compromise of the form government employees fill out when applying for a security clearance, the SF-86. The information about friends and family on this form is then used to search social networks and other open-source information to build targeting packages for the terrorists. Once again, while a work of fiction, it does demonstrate a vulnerability in which data collected from IoT devices would be useful.

SF-86 information could also be used to attack the networks of critical infrastructure. Most passwords used by humans are something easily remembered; for example, a cat's name. The terrorist selects an electrical utility to try to get a worm into the system and picks a target that used to have a security clearance. From the form, the terrorist learns that the target had a roommate 10 years ago. The terrorist then examines the roommate's sister's Facebook page, which is set to public, and sees a picture of when she stayed at her brother's apartment 10 years before. In this picture, there is a cat sitting in the sister's lap and she comments about how fun of a cat Fluffy was. The target has a password reminder asking for the name of his first cat. From here the terrorist is able to insert a worm to control IoT devices controlling the electrical grid and causes permanent damage to a generating station.

While to some this may seem like an imaginary situation, the Office of Personnel Management (OPM) was hacked and SF-86 information compromised. Considering social media like Facebook and Twitter, a massive amount of data is in the public domain. It doesn't necessarily even have to be that complicated with successive revelations about hacks in to Yahoo and other ISPs that include compromised passwords since many people use the same password for everything. While most likely Yahoo and others were hacked by cybercriminals seeking to use information to profit from the hack, nothing would prevent them from selling the information to a terrorist organization.

Conclusion

The IoT will continue to grow and connect more and more devices. It has the ability to dramatically improve people's quality of life while at the same time bringing down costs through efficiency and micromanagement. Estimates place between 26 and 50 billion connected devices by 2020. Cities will become "smart" with advanced IoT devices controlling traffic, sanitation services, electricity, dissemination of information (Butler, 2016, p. 4). More will be used in critical infrastructure to optimize production and improve delivery of services.

Securing IoT will involve partnership between both public and private entities. DHS has published strategic principles for this. It emphasizes using best practices throughout the industry and that security and updates should be incorporated in to initial designs and not added as an afterthought. As with the case studies from DoD, security should be prioritized based on the potential impact of malicious activity. Transparency within the community will allow all partners in creating IoT devices to recognize vulnerabilities in other areas. Lastly is to let users

and consumers control how and when to connect. Does an industrial device always have to be connected or would it be just as appropriate for it to connect once an hour or once a day (DHS, 2016, p. 5-12)?

While all devices connected to the internet can fall victim to terrorist attack, at present IoT devices are especially vulnerable. The scale of these attacks would not be comparable to 9/11 but an enemy using complex methods could still exploit this. Being able to repeatedly, successfully attack a network would shake confidence and instill fear, even without the loss of life or property. Terrorist organizations continue to evolve and embrace technology. Cyber terrorism is a low overhead attack that could potentially even the odds against a large state actor.

Resources cited:

Butler, R. J., & Lachow, I. (2016, October). Smart City Partnerships, Smart Cities and the Internet of Things: Benefits, Risks, and Options (Publication). Retrieved March 24, 2017, from New America Foundation website: https://na-production.s3.amazonaws.com/documents/SmartCityPartnerships10.18.pdf

Critical Infrastructure Sectors. (December 2016) Retrieved from: https://www.dhs.gov/critical-infrastructure-sectors

Davies, R. (2015, May). Internet of Things: Opportunities and Challenges (Eurpoean Parliment, European Parliamentary Research Service). Retrieved March 12, 2017, from http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

Department of Defense. (2016). DoD Policy Recommendations for The Internet of Things (IoT). Washington, D.C: Chief Information Officer. Retrieved March 23, 2017 from http://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440

Department of Homeland Security (DHS). (2016, November 15). Strategic Principles for Securing the Internet of Thing. Retrieved March 21, 2017, from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Fisher, E. A. (2015). The Internet of Things: Frequently Asked Questions (CRS Report for Congress, R44227). Washington, D.C.: Congressional Research Service. Retrieved March 23, 2017 from https://fas.org/sgp/crs/misc/R44227.pdf

Lewis, J. A. (2016). Managing Risk for the Internet of Things (Rep.). Washington, D.C.: Center for Strategic and International Studies . Retrieved March 15, 2017 from https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160217_Lewis_ManagingRiskIoT_Web_Redated.pdf

National Highway Traffic Saftey Administration. (2016). TRAFFIC SAFETY FACTS 2015. U.S. Department of Transportation. Washington, D.C. Retrieved from: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384

Simon, T. (2017). Critical Infrastructure and the Internet of Things (Global Commission on I Internet Governance Paper Series, Working paper No. 46). Waterloo, Ontario: Centre for International Governance Innovation. Retrieved March 15, 2017 from: https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf

Smith. (November 2014). Peeping into 73,000 unsecured security cameras thanks to default passwords. Retreived from: http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html

Understanding the Role of Connected Devices in Recent Cyber Attacks, Hearing Before the Subcommittee on Communications and Technology of the Committee on Energy and Commerce, U.S. House of Representatives, 114th Congress. 2, (2016). (testimony of Dale Drew, Kevin Fu, Bruce Scheiner) Retrieved March 23, 2017 from http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=105418

Voas, J., Feldman, L., & Whitte, G. (2016). Demystifying the Internet of Things. Computer,49(6), 80-83. doi:10.1109/mc.2016.162