

Research Question: How will future applications of internet based technology affect society?

Vincent Lopez

SPA: Dusty Grannis

2/23/2021

Abstract:

Computers are the backbone of the developed world, and the internet is the web that connects them. Understanding the relationship between the internet and society is critical to understanding both ourselves and our future. In this paper, I research the large scale changes brought on by the internet, the psychological effects of internet-connected devices on people, and what I believe the future of the internet will look like. I will attempt to determine the pros and cons of internet technology, specifically how we can benefit from it while maintaining control and security. The scale of the technology I will be highlighting cannot be understated. Behind nearly every logistical or analytical problem, lies the potential for an internet based solution. However, we must be careful in developing these solutions, for each one further intertwines the human race with a technology that may never be perfectly secure. Is becoming dependent on internet technology worth the countless benefits it can offer?

Pt I : Introduction

As you walk out of your house in the morning, the door locks behind you and the heater turns off to save energy. Your car is warm and already knows where to go. It even orders your coffee from the local cafe. You get to your job, where your phone clocks you in as you walk through the door and you get a notification for each of your daily objectives and reminders for all of your meetings. The elevator is ready for you with your favorite music playing. You begin to realize: the whole building is connected. Your car is connected. Your house is connected. This is the Internet of Things; as futuristic as it all sounds, it's digging its roots into every corner of society and human interaction.

What makes a device 'smart' is its ability to send and receive data from a worldwide network of other devices. This means access to basically limitless information that we wouldn't otherwise have available, at just a touch. This is true for most smart objects, which *Gartner.com* predicted would total 20 Billion devices by last year (2020). Some of these you might come to expect, or even own such as: a smart-printer, smart-coffee maker, or smart-television. These items are considered luxury, unnecessary, but still cool and convenient. Internet connected devices like these will be referred to as 'IoT' (short for Internet of Things) and will, as a whole, have far greater implications than that of just a coffee machine.

Let's start with what's in your pocket, which is "81%" likely to be a smartphone.(Pew) The smartphone shocked the world by offering limitless information, products, apps and a camera at the tips of our fingers. Information, communication, and interaction are rapidly changing because of it.

One of the biggest forces that drives the modern economy is competition. Basically,

businesses compete to have the best product for the lowest cost, and this constant competition drives innovation. Reducing costs with mass automation and data collection will play a huge role in the global economy and workforce.

IoT has one huge weakness however, and that is security. With massive amounts of data in constant transfer from one object to another and more devices capable of internet access, security is a challenge. Security will need to be designed into the IoT rather than be something tacked onto the finished product. We need to seriously consider what degrees of IoT integration are worth depending so heavily on.

Altogether, the IoT is shifting the world as we know it. As more things become internet connected, the convenience of data and automation will fundamentally change how we utilize and interact with technology and each other by affecting our brains, evolving to our environment, and becoming integrated into society on a global scale.

Pt II : Background Knowledge

| A History of the Internet |

The modern internet is a collection of instructions for certain tasks that are consistent between connected devices. These instructions let devices talk to each other. As an article from *ugs.edu* describes it, “The Web is one of several ways to retrieve information from the Internet. These different types of Internet connections are known as protocols.”(ugs par.2) Originally, they included instructions that computers used to send and receive files. More modernly, people use protocols that live stream video and audio to communicate with each other live over great distances, especially in the wake of Covid-19.

Internet protocols have been around since the '60s, but not how you might think. According to an accompanying article, “A Brief History of the Internet”, “The Internet started in the 1960s as a way for government researchers to share information. Computers in the '60s were large and immobile and in order to make use of information stored in any one computer, one had to either travel to the site of the computer or have magnetic computer tapes sent through the conventional postal system(ugs).” At the same time, the start of the Cold War was pushing researchers to think of new ways to transfer information in the event of a nuclear attack, and the Soviet had just launched a satellite of their own. An MIT researcher began the idea for the development of ARPANET, a satellite network of which only a select few institutions could access. The first ever message was sent from one computer to another over ARPANET in 1969, and the network steadily grew from there.

Connecting networks through satellite became a more common practice until,

according to *Hisotry.com*, “In 1991[...] a computer programmer in Switzerland named Tim Berners-Lee introduced the World Wide Web: an internet that was not simply a way to send files from one place to another but was itself a ‘web’ of information that anyone on the Internet could retrieve.”(History par. 4) This led the way for search engines like Google and Yahoo. Now that all the information was available, it still had to be found.

“For more than four decades, the Internet has grown and spread to an extent where today it is an indispensable element in the communication and media environment of many countries, and indeed of everyday life, culture and society,” says Niels Brugger in his article. These days, the primary uses of the web include email, research, downloading files and social media/news. However, recent innovations and the widespread use of sensor/actuator systems have brought the digital world directly into the real one.

| **What is the IoT?** |

The IoT, short for ‘Internet of Things’, refers to objects that have been computerized and are connected to the internet. An IoT device is defined as literally anything with an internet connection like a computer, phone, coffee-maker, printer, smart-TV, or even one with an indirect connection like a smart-watch.

According to Keith Foote, senior writer for *DATAVERSITY.net*, “The Internet of Things, as a concept, wasn’t officially named until 1999. One of the first examples of an Internet of Things is from the early 1980s, and was a Coca Cola machine, located at the Carnegie Mellon University. Local programmers would connect by Internet to the refrigerated appliance, and check to see if there was a drink available, and if it was cold, before making the trip.”(Foote

par.3) This most early example made something that wasn't possible before, just a few clicks away. This is the first, but not the last, time we see IoT technology being used for everyday convenience.

Wearable technology, as well as things you might find in your home, workspace, or outside can be considered IoT. The article "What Is the Internet of Things (IoT) in Business?" on *CDW.com* describes the IoT as, "[...]everyday devices capable of sending and receiving information via connection to the internet."(CDW par.3) To make use of a device capable of sending and receiving data, it has to have a sensor or an actuator, oftentimes both. A sensor is what a device uses to take in information from the environment around it, like how a Tesla electric car uses cameras to see the road. An actuator is something it uses to interact with its environment, like the electric motors driving the wheels.

Micheal Chui, author of "The Internet of Things" on *McKinsey.com*, splits the IoT into two major parts: Automation/control, and data collection/analysis (Chui fig.1). By itself, having control over multiple devices is incredibly useful. It allows for things such as automated assembly lines and robots that do work too dangerous for humans, however it's limited to the instructions that it's given. The opposite is true for the data collection piece of IoT; it opens a new lens for scientists and engineers to view the world through, and lets them collect data from a practically infinite number of sensors at the same time, but alone it is just information. The true power of IoT comes from merging the two.

Pt III : Research and Analysis

| IoT in Business and Industry |

IoT technology is the future of business and industry. Companies are constantly adopting available technology in an attempt to minimize the cost of operation and maximize profits. According to the book, “Leading the IoT” by Mark Hung of *Gartner Research*, “The IoT will have a great impact on the economy by transforming many enterprises into digital businesses and facilitating new business models, improving efficiency and increasing employee and customer engagement.”(Hung p. 2) The next technological revolution will involve the mass implementation of sensor and actuator systems that will serve to improve and re-invent business processes and models.

The first step to understanding how a business or industry can benefit from the IoT is to understand to what degree the IoT is currently being used to solve other problems. Mark Hung’s example involves gathering data from the components of a train system:

Brake pads, for example, had always been replaced according to standard maintenance plans based on distance (kilometer) intervals. By adding a life indicator that measures the energy dissipation capability of friction braking in real time, Trenitalia (train company) now knows that route-specific factors (hills, curves and local routes with many stops), along with kilometers, have a direct bearing on brake pad life. Combined with the addition of new health measures, such as brake pressure and temperature and whether the brake is on a locomotive or a coach, Trenitalia has been able to optimize brake pad utilization and reduce maintenance activities without impacting safety or

reliability. (Hung 5)

Trenitalia's implementation of sensor systems is an example of how an industry can reduce their cost of operation by identifying factors that affect the integrity of parts that they rely on.

Another utilization of IoT technology is using internet connected 'robots' to complete complex tasks with lots of moving parts. Ovidiu Vermesan et al., explain that, "Robotic engineering systems are deployed today in industry and are considered vital elements for the progress of humanity from an industrial perspective in the new digital age." (Vermesan) This is the automation/control piece; something that the modern day industry couldn't possibly do without.

Improving Workplace Safety

Industrial robots can often complete tasks with less risk and more efficiency than a professional, making it an obvious choice in places like the cattle industry. The article "Meet the Robot That's Making Cattle Herding Safer" on *Cargill.com* describes the risks of working with cattle, "Three quarters of a ton. That's the size of the average bovine moving through Cargill's beef plant in Schuyler, Nebraska. Multiply that by 5,000— approximately how many head of cattle the facility processes on a daily basis—and you begin to understand the scale of the potential safety risks that are inherent to working alongside these hefty mammals." In response, they designed a remote-controlled robot on wheels designed to usher the cattle in a desired direction. A member of the team responsible says, "From a safety standpoint you don't have to have an individual there pushing cattle forward,' [...] 'So, if the animal decides to turn, it's not a person hurt. It's just a machine that we can fix' (Cargill)."

Human-Robot interaction is becoming inseparable from modern production. Ales Vysocky and Petr Novaka ask in their article about robot and human interaction, "Robots are

tough, fast and very accurate machines which can complete their tasks faster, with better quality and for a lower price than humans. Why then should we keep the human factor, which can produce errors, and deal with collaborative robots? Some operations have to be adapted to actual conditions.”(Vysocky 1) Operations being adapted to actual conditions is a way of saying that, often, it is efficient to use mechanical muscle with a human operator. Thus, they answer their question with good news for businesses and individuals alike; in Human - Robot Collaboration, businesses are able to ramp up production with more precision and consistency, while individuals keep their jobs and are able to perform them more safely.

A Computer for a Brain

As useful as IoT is for data analysis or robotic actuation, it's true strength lies in the ability to combine the two. This is what *Microsoft.com* calls an 'IoT measure and control loop'. A measure and control loop, “keeps an IoT device within the tolerable range[...], through a real-time, closed-loop control process. The device may be part of a larger physical system controlled by software that contains one or more networked devices.”(Microsoft par. 1) Essentially a measure and control loop means: Instead of an IoT network of devices designed to measure a set of parameters or use motors/actuators to interact with its environment, it does both in a closed loop fashion; the IoT device or network takes information from its environment, and interprets it into an action.

A simple example is the fire suppression system in most modern buildings, where when multiple sensors detect smoke, it triggers the alarm and sprinkler systems. As far as data goes, smart fire detection systems in use today allow firefighters to collect live data from multiple areas of a burning building, allowing them to navigate it more safely. Horowitz, writer for *IEEE.com* says, “For years, first responders relied on paper maps to reach a fire in an

apartment building or office. Incomplete information would delay firefighters from arriving at an emergency, and false alarms would set them on the wrong path altogether.”(Horowitz par.1)

Cutting down the time it takes for first responders to arrive at a scene is a super simple way to save lives. Although firefighters won't be replaced by robots anytime soon due to the complexity of their work, an IoT system is also capable of taking action towards the safety of its occupants. Horowitz also writes, “An IoT system could shut down an HVAC system or put elevators in fire mode if smoke is blowing around a building.”(Horowitz par. 3) Shutting off HVAC and triggering sprinklers will slow or even stop a fire, and disabling elevators can prevent people from becoming trapped inside, effectively saving them in the case of a blaze.

Industrial applications of closed loop IoT systems can be mind-bogglingly complex, but extremely productive and reliable. According to researchers at *Siemens*, “CLM (short for ‘closed loop manufacturing’) enables firms to synchronize and optimize production across product design, production planning, manufacturing execution, automation and intelligence from consumer use in the field. Creating a collaborative, connected information loop, CLM continuously improves the cost, time and quality of the manufacturing process to accelerate the delivery of products at the optimal level of quality and cost.”(Siemens) Closed loop manufacturing systems rely on data gathered from the manufacturing process and analyzed by software to optimize productivity and quality. They react in real time to the conditions around them, allowing for complete automation of things like production lines and construction, without the need for human intervention.

Closed loop IoT in the energy world often uses what's called a digital twin. According to Maggie Armstrong of *IBM.com*, a digital twin is a complex digital tool that uses implemented sensors and actuators to mirror and control the system it's connected to(Armstrong). For

example, General Electric uses what they describe as, “[...]a virtual version of GE’s gas turbines, steam turbines, and wind turbines. These ‘twins’ live in the cloud and are supplied with all the data and insights that come from their physical twin—the turbine itself.”(GE Renewable Energy par. 2) The digital twin both monitors and predicts the temperature, speed, and power of the turbine, and adjusts them automatically for optimal efficiency. This means no more overheating, perfect grid supply, and more precise maintenance routines. Integrated digital twin technology has its own initial cost, but can reduce the cost of operation for as long as it’s in use.

Overall, it’s easy to see how the IoT will become a driving factor in the competitive world market. Systems like real time maintenance monitoring, closed loop manufacturing, and digital twin control allow companies to better understand their products and processes, and can have long term impacts on savings. As well as providing remote access to almost every corner of an industry and data about manufacturing and customer usage, it can also provide a new medium for customers to interact with a company’s product.

| The Changing Face of Human-Computer Interaction |

As smart homes, services, and wearable technologies become more common, human computer interaction is rapidly evolving to better meet our needs. However, it will become increasingly difficult to remain independent from technology. We will see common services replaced by computers capable of performing tasks better

Smartphones and Accessories

Apple released its first smartphone in late June, 2007. Today, most Americans own a smartphone. *Pew Research Institute* estimates that 21% of the same demographic wear a

smartwatch or fitness tracker(Pew, Facts), which are usually an extension of your smartphone that can be used to answer calls, view messages etc. and has very little processing power of its own.

Undeniably, smartphones have some major advantages as an everyday carry item. “Imagine combining a mailbox, a newspaper, a TV, a radio, a photo album, a public library and a boisterous party attended by everyone you know, and then compressing them all into a single, small, radiant object. That is what a smartphone represents to us. No wonder we can’t take our minds off it,” says Carr, author of “How Smartphones Hijack our Minds”. It’s in their usefulness that they become addictive.

Technology continues to directly influence the world around us. While it has revolutionized communication, information, automation, and convenience, becoming too dependent on it can be a detriment to individuals. Research from the Department of Nursing and Health Sciences at Notre Dame University found, “Prevalence rates of smartphone-related compulsive behavior, functional impairment, tolerance and withdrawal symptoms were substantial. 35.9% felt tired during daytime due to late-night smartphone use, 38.1% acknowledged decreased sleep quality, and 35.8% slept less than four hours due to smartphone use more than once.”(Matar, Results). The study, conducted on other undergraduate and graduate students, found that things like depression and anxiety serve as a positive predictor of smartphone use.

We almost all use a smartphone to communicate these days, and although smartphone use has been linked to depression and anxiety, accessories like AppleWatch and Fitbit can help track fitness as well as vital functions. For people with heart, muscle, or nervous system conditions, they can even save lives.

Smart Homes and Environments

As IoT becomes more common and available, the environment we interact with daily will be shaped by it. Environments that will be shaped by IoT technology include homes, workspaces, and public spaces. First, it's important to understand what changes will become more common in homes. According to a journal on *Hindawa.com*, "A smart home is an advanced form of traditional home automation. An early definition of a smart home, which was influenced by home automation, is using common communication devices to integrate with a variety of services at home, assuring economic, secure, and comfortable operation of the home."(Hindawa p.2) This means that homes will have advanced live security, comfort, and entertainment systems, making them more luxurious and secure. Zion Market Research predicts that the IoT smart home market will reach \$53.45 Billion by 2022.

Another aspect of society that is bound to be influenced by internet technology is public environments. In the near future, we will likely see jobs at places like theatres, theme parks, and gyms replaced with robots capable of the same task. In the background, IoT infrastructure will streamline utilities and services such as clean energy, water, and even some government services. "Essentially,[...] one is able to create intelligent infrastructure systems (i.e. cyber-physical systems) that have the potential to change almost every aspect of mankind's interaction with the environment," says Mullet, author of "Teaching the IoT". Basically, the same technologies like digital twin and closed loop control will be implemented in key background societal functions.

IoT Utilities

The market for IoT Utilities is expected to grow to just above that of IoT smart homes. According to *TDWorld.com*, "The use of IoT in the electricity grid offers an unprecedented

opportunity to move the energy industry into a new era of reliability, availability, and efficiency, which will contribute in enhancing the overall economic and environmental health. An electricity grid having IoT capabilities has smart sensors, receivers, smart meters, and energy boxes, which communicate with each other.”(T & D World par. 4). This can improve the overall efficiency of the system as a whole, as well as help it safely and quickly react in the event of a natural disaster.

| A Secure IoT |

One of the biggest challenges when it comes to internet based systems is security. Horror stories of hackers infiltrating and destroying systems like hydro-electric generators, holding private information for ransom, or remotely controlling home systems are real. These are legitimate concerns, and as Paul Marks puts it, “[...]security is not an optional extra, ‘but should be considered at the beginning, and throughout the life cycle of IoT applications’.”(Marks p. 2). Security is integral to the success of IoT.

The most important weakness of integrating sensor and actuator devices into a large system is that **every single device** has the potential to be an entry point for hackers. Software that monitors the communication between every device is essential to a secure IoT. Judith Lamont, researcher for *K and M World*, explains that an internet connected printer at a hospital should not be trying to access patient records. She suggests that software should be in place to detect unwelcome requests so that a human operator can block the action and trace the request back to the hacker (Lamont p. 12). This kind of software, firewalls, and other internet security measures are necessary to make IoT applications worth the risk hacking them could pose for individuals and businesses that rely on the technology for everyday operations.

One of the ways multiple IoT devices can become compromised is through what's called a botnet. This kind of attack infects a device, then sends itself to all the devices connected to the infected one. These can be really difficult to slow down and identify because of how fast they spread. IoT systems are the most vulnerable target to this kind of attack because they are exactly what botnets are designed to take control of. According to *akamai.com*, "Botnet owners can have access to several thousand computers at a time and can command them to carry out malicious activities." (Akamai par. 2) The owner of a botnet can control any or all of infected devices, allowing them to disrupt activity, steal information, carry out physical attacks on a system, and more.

The botnet attack credited with being 'the world's first digital weapon' was a malware called 'Stuxnet'. First discovered in 2010, Stuxnet was a self replicating program that found its way into the computers responsible for controlling an Iranian nuclear power facility. "It targeted the computer system of the machines used to enrich uranium, known as centrifuges, and instructed them to spin the machines out of control. Eventually that force broke the centrifuges. At the same time, Stuxnet would report to the control room that nothing was amiss." (Lauder par.5) The attack was considered genius, and serves as a warning to the vulnerability of important IoT systems.

Although IoT solutions are applicable to a wide range of problems and luxuries, they are not worth the risk unless they are properly secured. Businesses, infrastructure, homes, and personal items all need to be protected behind an advanced level of security. This means initial security measures **as well as** regular security updates. Of the 20 Billion internet connected devices out there, one weak link can cause permanent damage to the system it belongs to.

Pt IV : Conclusions

Without a doubt, the internet is becoming one with the world around us and between us. Everything from a phone, to a coffee machine, to an entire city can be ‘smart’. Whether for luxury, convenience, profit, or data, IoT devices are becoming ever more popular.

Stores like Amazon-Go have ditched human checkout lines in favor of a scanning system that charges you as you walk out based on what it saw you leave with. Some jobs are disappearing: BlockBusters replaced with Redbox kiosks, grocery store workers replaced with store-wide sensors, etc. Smart objects and systems have obvious advantages in terms of efficiency, analysis, and control. The IoT will leave a lasting impact on individual businesses and industries, with ripples that will last generations to come in the global economy. It will redefine what jobs are safe for people to do. Jobs that involve working side by side with robots or IoT systems will become more common, which will drive further research into the best ways for humans and robots to effectively communicate. In the near future, it could become near impossible to not work side by side with internet connected systems. Even farming, which happens deep in the country, already benefits hugely from IoT technology.

The ways we’re used to interacting with computers and each other are being re-imagined everyday. It’s reasonable to expect that, although wearable and personal communication devices will make communication and information more accessible than ever, unsuspecting individuals will become dependent on and addicted to the seemingly limitless functions they have to offer.

Virtual assistants like Siri, Google, or Alexa are becoming common household items. They are able to control IoT functions of an environment like lighting, locking/unlocking doors,

and climate control. This type of human-robot interaction is more and more common as families across the country add smart speaker systems to their living room and kitchens. To this end, robots are getting better at mimicking and interpreting human speech.

Last but not least, we cannot forget about the major weakness of any internet based system, cyber security. Hackers infiltrating a large system have the potential to do major damage to said system and steal private information. An IoT system without integrated security poses a huge risk it's user. All IoT systems should be designed with security as a first priority; an unsecured network with unsecured devices should not be allowed to operate due to the risks involved were they hacked. Cyber criminals are constantly adjusting their tactics to avoid security measures, and so an IoT system should be subject to regular security checks and updates. This is not to say that a secure IoT is not to be trusted, as it can still be a powerful tool, but rather that the security of the system **must** be constantly maintained.

Overall, the IoT is a powerful tool that is instrumental to the advancement of the human race. Basically every problem that could be solved with automation has a solution in the IoT. Humans will become more used to interacting with robotic systems, and robotic systems better at communicating back. Internet technology is becoming inseparable from human society.

Both becoming dependent on technology, and letting it change us is dangerous. As a society, we are grasping a double-edged sword. With the security of the everyday world hanging in the balance, the difference between the next technological revolution and the next technological catastrophe depends on how carefully we proceed. Will wielding such a tool prove to be the key to our advancement, or will it be the instrument of our own demise?

Sources:

A Brief History of the Internet, www.usg.edu/galileo/skills/unit07/internet07_02.phtml.

Armstrong, Maggie. "Cheat Sheet: What Is Digital Twin? Internet of Things Blog." *Cheat Sheet:*

What Is Digital Twin?, 16 Feb. 2021,

www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/.

Brugger, Niels. "Introduction: Internet Histories." *Taylor & Francis*,

www.tandfonline.com/doi/full/10.1080/24701475.2017.1317128.

Carr, Nicholas. "How Smart-Phones Hijack Our Minds." *WSJ.com*, 7 Oct. 2017,

cs12.cs.gc.cuny.edu/~waxman/How%20Smartphones%20Hijack%20Our%20Minds%20-%20WSJ.pdf.

Chui, Michael, et al. "The Internet of Things." *McKinsey & Company, McKinsey & Company*,

13 Feb. 2019,

www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-internet-of-things#

"Demographics of Mobile Device Ownership and Adoption in the United States." *Pew Research*

Center: Internet, Science & Tech, Pew Research Center, 5 June 2020,

www.pewresearch.org/internet/fact-sheet/mobile/.

Foote, Keith D. "A Brief History of the Internet of Things." *DATAVERSITY*, 6 Aug. 2016,

www.dataversity.net/brief-history-internet-things/

“Grid Innovations.” T & D World,

www.tdworld.com/grid-innovations/article/21120887/iot-in-utilities-market-worth-538-billion-by-2024.

Hanuk. “IoT Measure and Control Loops - Azure Example Scenarios.” Azure Example Scenarios | Microsoft Docs,

docs.microsoft.com/en-us/azure/architecture/example-scenario/iot/measure-control-loop.

History.com Editors. “The Invention of the Internet.” History.com, A&E Television Networks, 30 July 2010,

www.history.com/topics/inventions/invention-of-the-internet#:~:text=Berners%2DLee%20created%20the%20Internet%20that%20we%20know%20today.

Horowitz, Brian T. “IoT Makes Fire Detection Systems Smarter.” IEEE Spectrum: Technology, Engineering, and Science News, 2020,

spectrum.ieee.org/tech-talk/sensors/remote-sensing/how-iot-makes-fire-detection-systems-smarter.

Hung, Mark. Leading the IoT: Gartner Insights on How to Lead in a Connected World. Gartner.

“Improving Wind Power with Digital Twin Technology: GE Renewable Energy.” Improving Wind Power with Digital Twin Technology | GE Renewable Energy,

www.ge.com/renewableenergy/stories/improving-wind-power-with-digital-twin-turbines.

“IoT and the Campus of Things.” EDUCAUSE Review,

er.educause.edu/articles/2016/8/iot-and-the-campus-of-things.

“IoT Smart Home Adoption: The Importance of Proper Level Automation.” *Journal of Sensors*, Hindawi, 22 May 2018, www.hindawi.com/journals/js/2018/6464036/

Kasper, Wolfgang, et al. “Competition.” *Econlib*, www.econlib.org/library/Enc/Competition.html.

Lamont, Judith. *The IoT: Security and Integration Are Key to Success*, KM World, 2018, web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=2&sid=e9d6542e-31a3-44b6-875a-00578f7eb47e%40pdc-v-sessmgr05.

Lauder, Jo. “Stuxnet: The Real Life Sci-Fi Story of 'the World's First Digital Weapon'.” *Triple j*, Australian Broadcasting Corporation, 12 Oct. 2016, www.abc.net.au/triplej/programs/hack/the-worlds-first-digital-weapon-stuxnet/7926298.

Marks, Paul. “Fix the Holes.” *Semantic Scholar*, 3/24/2018, www.semanticscholar.org/paper/Fix-the-holes-Marks/b7dcaa1e69bfd2281c0f3cd81e0953b30e758320.

Matar Boumosleh J, Jaalouk D (2017) Depression, anxiety, and smartphone addiction in university students- A cross sectional study. *PLoS ONE* 12(8): e0182239. <https://doi.org/10.1371/journal.pone.0182239>

“Meet the Robot That's Making Cattle Herding Safer .” *Cargill*, www.cargill.com/story/meet-the-cowboy-robot-thats-making-cattle-herding-safer.

Mullett, G. J. (2016, June), *Teaching the Internet of Things (IoT) Using Universally Available Raspberry Pi and Arduino Platforms Paper presented at 2016 ASEE Annual Conference & Exposition, New Orleans, Louisiana. 10.18260/p.26053*

Rogers Y. (2009) *The Changing Face of Human-Computer Interaction in the Age of Ubiquitous Computing*. In: Holzinger A., Miesenberger K. (eds) *HCI and Usability for e-Inclusion*. USAB 2009. *Lecture Notes in Computer Science*, vol 5889. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/978-3-642-10308-7_1

Tips for Using the Internet: A Brief History of the Internet,
www.usg.edu/galileo/skills/unit07/internet07_02.phtml.

Tips for Using the Internet: Basic Description,
www.usg.edu/galileo/skills/unit07/internet07_01.phtml.

Vermesan, Ovidiu, et al. “Internet of Robotic Things Intelligent Connectivity and Platforms.”
Frontiers, *Frontiers*, 2 July 2020,
www.frontiersin.org/articles/10.3389/frobt.2020.00104/full.

What Is a Botnet Attack – Definition | Akamai.
www.akamai.com/us/en/resources/what-is-a-botnet.jsp.

“What Is the Internet of Things (IoT) in Business?” CDW,
www.cdw.com/content/cdw/en/articles/networking/2019/01/24/what-is-the-internet-of-things.html