Maurice Eugene Dawson Jr.

CYBER WARFARE
THREATS AND OPPORTUNITIES

Universidade Fernando Pessoa
Porto, 2020

Maurice Eugene Dawson Jr.

CYBER WARFARE
THREATS AND OPPORTUNITIES

Final report presented to the University
Fernando Pessoa as part of the
requirements for obtaining the post-doctoral
degree in Information Science, under the
guidance of Prof. Luis Borges Gouveia

Universidade Fernando Pessoa
Porto, 2020.

Table of Contents

Acknowledgments 6
Executive summary 7
National Cybersecurity Education: Bridging Defense to Offense 10
Introduction 10
Intelligence Community Degree Program Accreditation 11
Ethical Considerations 15
Adaptive Curriculum 16
Challenges 16
Need to Develop an Offensive Security Workforce Framework 17
Development of New Skills 18
Further Study 20
Final remarks 20
Emerging Technologies in the Fourth Industrial Revolution 21
Introduction 21
Industry 4.0 22
The Promise of AI in Manufacturing 23
Evolving Environments 24
Understanding the Risks 25
Importance of Manufacturing in U.S. 28
Final remarks 29
Nefarious Activities within the Deep Layers of the Internet 31
Introduction 31
Human Trafficking 32
Online Marketplace 33
Navigating the Dark Web 35
Online Forums 36
Supply and Demand on the Dark Web 38
Cryptocurrencies and Blockchain 39
Final remarks 40
Software Security Considerations 41
Software Testing 41

Sandbox Environment 43
Emerging Computing Environments 45
Critical Infrastructures Challenges 46
Final Thoughts 49
COVID-19 50
Election 51
Supply Chain 51
Final Remarks 52
References 53

Index of Figures

Figure 1: Multidomain Concept (Bartles, Tormey, & Hendrickson, 2017) 7
Figure 2. CAEs Throughout the US and US Territories 13
Figure 3. OSINT Application 19
Figure 4. Industrial Revolutions (considering four waves) 23
Figure 5: Secure Software Development Process 27
Figure 6: Gross Output by Industry (U.S. Bureau of Economic Analysis, 2020) 29
Figure 7. Example of Online Marketplace on Dark Web 34
Figure 8. Example of Rubmaps Massage Review 38
Figure 9: Software Development Life Cycle 42
Figure 10. Linux Sandbox Environment 44
Figure 11. Mission Framework 45

Index of Tables

Table 1. NSA Cyber Operations Standards 14
Table 2. Example Offensive Cybersecurity Workforce Framework 18
Table 3: Organizational Cybersecurity Risks for AI 26
Table 4. Threats 48

Acknowledgments

This submission would not have been possible without my supervisor's guidance, Professor Luis Borges Gouveia of University Fernando Pessoa. I am thankful for my colleagues' support within the department of Information Technology and Management (ITM) at the Illinois Institute of Technology.

The opportunities to serve as a Visiting Professor or Visiting Researcher at the Technische Universität München (TUM), L'Institut Supérieur des Etudes Technologiques en Communications de Tunis (ISET'COM), and the Policía Nacional Dominicana. Thank you to organizations such as the Catholic Relief Services (CRS) for providing funding for my students and colleagues to perform assignments in Benin.

Lastly, the submission is dedicated to the memory of Juanita Dawson. Also, I dedicate this submission to my parents Maurice Dawson Sr. and Flossie Dawson. And to my children Amayah, Maurice, and Kingsley, you are the sole motivation for pursuing the impossible.

Executive summary

Cybersecurity has gone through several changes that have presented new challenges in recent years, complicated by the rise of cybercrime and digital warfare. With the introduction of militarizing the space domain, it has become apparent that we must consider multidomain concepts [See Figure 1]. Thus, the threat landscape has again shifted, and defenders must become knowledgeable about how the cyber domain crosses into maritime, land, air, and space. The traditional thinking of protecting enterprise systems locked away in a building is no longer. Thus, we have the emergence of cyber warfare and cyber as a fifth domain that brings together maritime, land, space, and air. These domains are not just for the military but the civilian sector as well. Understanding the role of cyber and how it can be used to take advantage or secure the remaining domains will give entities the upper hand in strategy.

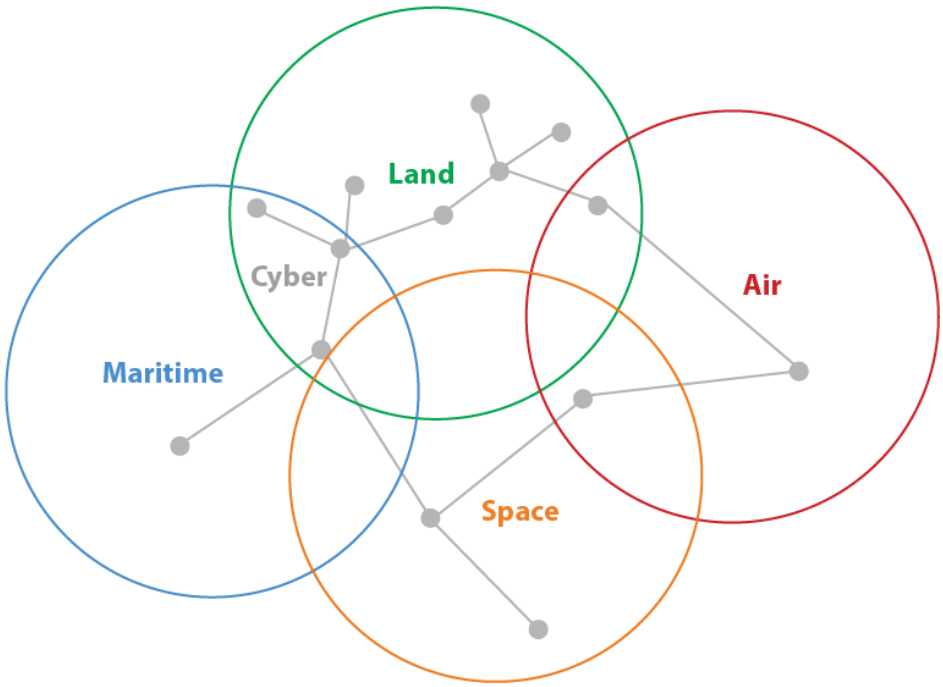

Figure 1: Multidomain Concept (Bartles, Tormey, & Hendrickson, 2017)

The technological advancements that pave the way to the mass implementation of the Internet of Things (IoT) and Internet connectivity to everyday devices have led to an explosion in cyberattacks such as breaches resulting in millions of accounts being compromised. (Dawson, Eltayeb, & Omar, 2016). Bad actors such as those focused on criminal activities regarding human trafficking and espionage navigate these domains to circumvent law enforcement agencies globally. We must understand how exploitation, circumvention, and defense needs to occur in a multidomain concept. However, knowing that the cyber domain is a domain that goes through land, maritime, space, and air can be an area that serves as a central point for realizing assured security.

Executive Orders (EO), laws, policies, doctrine, and other directives have shaped the landscape of cybersecurity. New EOs have been released that allow a cyber-attack with responsive measures such as one that involves military force. Laws created that impose rights for Personal Identifiable Information (PII) being breached, leaving millions of individuals unprotected. One of these most well-known items is General Data Protection Regulation (GDPR) as it relates to the European Union (EU) and the evolving threats with hyperconnectivity (Martínez, 2019a; Martínez, 2019b).

Understanding the role of cybercrime and digital warfare and how they continue to play in shaping the technological landscape is critical. These various actions change the spectrum regarding combating nefarious actors or design errors that leave the system susceptible. As attacks continue to rise from bad actors such as nation-states, terrorists, and other entities, it is essential to understand the threat landscape and select cybersecurity methodologies that can be put in place to provide adequate measures.

This document presents the work form a post-doctoral project that provides a perspective of cybersecurity under a information science perspective. This six-month project allows to stress

the broadly importance that information and its management (not just within the information security context), and the urgent need to deal with cybersecurity as a societal challenge.

The document is organized in four main chapters presenting different but complementary issues, going from high level to a more operational level: *National Cybersecurity Education: Bridging Defense to Offense*, stressing the importance of societal awareness and education. *Emerging Technologies in the Fourth Industrial Revolution*, stressing the importance to consider cybersecurity issues as core ones, even to economic and production areas. *Nefarious Activities within the Deep Layers of the Internet,* stressing the need to be part of digital places where information is traded, shared and, even sometimes, created. The fourth chapter provide a few hints and issues related with software development and test: *Software Security Considerations*. A final session presents several remarks as Final Thoughts, closing the work pointing out some of the current challenges that we are facing of.

Keywords: *Cyber Warfare, Artificial intelligence, cybersecurity, workforce, risk management, cybercrime, human trafficking, dark web, online marketplace, cryptocurrency, disinformation*

National Cybersecurity Education: Bridging Defense to Offense

Defense Secretary Robert Gates approved the creation of a unified cyber command under the Obama Administration that was focused on cyber operations (EUA). This organization was to oversee the protection of government networks against cyber threats known and unknown. Coupled with growing attacks on national infrastructure, digital theft of Intellectual Property (IP), and election meddling has the United States government actively working to develop cybersecurity talent. Some of the changes that have come as a result are more specialized degree program accreditation, technical frameworks, and policies to help usher this realization of the need to address the shortage of talent for today's mission.

Introduction

A significant shift in the last decade has come in the United States of America (USA). Cybersecurity has become a topic of concern for every organization. The United States Cyber Command (USCYBERCOM) has become one of the eleven unified commands of the U.S. Department of Defense (DoD) (U.S. Cybercom, n.d.). The mission of USCYBERCOM is to be a significant player in cyber operators, strategic thinking, and to be an essential player within the warfighting domain of cyberspace (Vijayan, 2009). Other agencies have cybersecurity elements within, such as the National Security Agency (NSA), Department of Homeland Security (DHS), DoD, and others. However, in terms of having a direct role in cyber operations, USCYBERCOM has the lead. The need for a combatant command focused on cybersecurity has been a talking point for years that has finally materialized (Helms, 2015; Hollis, 2010).

There have been major offensive attacks that have been towards the United States (U.S.) infrastructure and companies. Each week there is a new major data breach while sharing

news of a significant shortfall for cybersecurity professionals steady climbing. U.S. institutions are scrambling to hire faculty and develop innovative labs to attract and retain students who want to pursue his career in cybersecurity. The Federal Information Security Modernization Act (FISMA) report shows an alarming trend that the number of attacks increases while certain agencies lag behind the implementation of adequate protection. Other agencies that provide reports such as FISMA, Health Insurance Portability and Accountability Act (HIPAA), ISO 27000, and PCI-DSS Standards that overlap in areas and display gaps in others (Gikas, 2010).

Globally digital crime and cyber terrorism have run rampant. The Internet has become the new battlefield, yet it seems the majority of players are on the defensive rather than offensive (Dawson & Omar, 2015). As this problem continues to increase, it has the attention of the federal government. This problem has forced national intelligence agencies to get proactive about improving the talent pool.

Intelligence Community Degree Program Accreditation

A cybersecurity educated workforce is critical in building trustworthy systems (Schneider, 2013). To ensure this happens, the NSA sponsors two forms of the Center for Academic Excellence (CAE). The first one is the CAE in Cyber Defense (CD), which is joint with the DHS. There are a few designations with the CD program. The primary grouping discussed is the CD in education at the associate, bachelor, master, and doctoral levels (Dawson, Wang, & Williams, 2018). To meet this designation at particular levels, institutions must map their courses to the National Initiative on Cybersecurity Education (NICE) Framework and demonstrate several capabilities. These range from having full-time academically qualified faculty to teaching cybersecurity in other departments outside of the one that the cybersecurity program is housed in (Dawson, Wang, & Williams, 2018; Wang, Dawson, & Williams 2019). Other required items include an established center, a certain amount of research productivity. The CD designation is

focused on defense and has no offensive component to it as the objective is to get the student to be able to deter, detect, and mitigate attacks.

There are a total of 311 universities that have the CD, R, or 2Y designation. The CD designation is for institutions that have bachelor's degrees and higher. There are 175 that have the CD designation, 107 that have the 2Y designation, and 29 that have the R designation. Additionally, 46 of the 311 universities carry the CD and R designations. Merely 17 universities have at least one focus area that ranges from systems security engineering to policy. Only 21 universities hold the CAE in C.O. Of these, only two are DoD funded with one focused on bachelor's degrees and the other graduate. Figure 2 displays that ten states produce approximately half of the CAE institutions. Those states and percentages from highest to lowest are 1) TX: 21 CAEs, 2) VA: 20 CAEs, 3) FL: 18 CAEs, 4) MD: 17 CAEs, 5) NY: 15 CAEs, 6) CA: 14 CAEs, 7) IL: 12 CAEs, 8) MI: 12 CAEs, 9) PA: 12 CAEs and 10) GA: 10 CAEs. The percentages of the CAEs in these states are 48.1% of all CAEs throughout the entire country and territories.

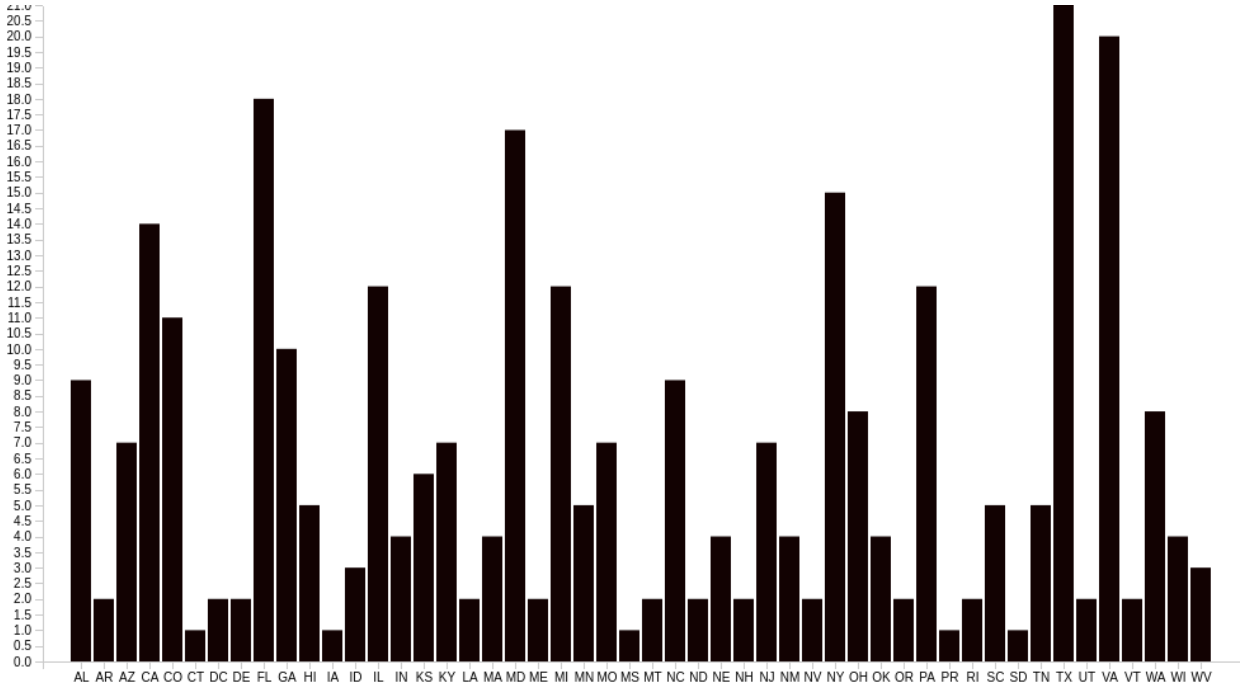

Figure 2. CAEs Throughout the US and US Territories

When reviewing Figure 2, an analysis shows that 20 states/territories have four or fewer CAEs. This analysis tells a story of that as it relates to cyber defense education, only a fifth of the states is leading the charge. In contrast, a number of states are falling behind in providing defensive education. The CO program is much smaller than the CD program two differentiating programs. The first is known as the fundamental program, and the latter is the advanced program. The fundamental program is for undergraduate and graduate institutions that have technical programs in computer science, electrical engineering, computer engineering, or a combination of two or more of these programs. The advanced program has the same degree requirements of the university to apply for the program. In Table 1, the required criterion to be met by institutions is listed.

Table 1. NSA Cyber Operations Standards

STANDARD	STANDARD NAME	REQUIREMENT
1	Academic Content	100% of mandatory / 10 of the 17 optional.
2	Cyber Operations Recognized via Degree, Certificate or Focus Area	Cyber operations must be explicitly recognized as a focus area or specialization and students must meet requirements to be awarded such recognition.
3	Program Accreditation/Curricula Review	An in-person review of the curriculum is required. The CD, 2Y, and R programs do not require this.
4	Cyber Operations Treated as an Interdisciplinary Science	Cyber operations concepts must be integrated into the core and specialization curriculum as appropriate.
5	Cyber Operations Academic Program is Robust and Active	Show evidence that courses are current and offered at most 18 months.
6	Faculty Involvement in Cyber Operations-related Research	Must provide evidence of faculty work on research papers, conference presentations, and grants that focus on cyber operations.
7	Student Involvement in Cyber Operations-related Research	Must provide evidence of student work on research papers, conference presentations, and grants that focus on cyber operations.
8	Student Participation in Cyber Service-Learning Activities	Must provide evidence of student participation in cyber exercises, outreach to high schools, or community colleges.
9	Commitment to Support the CAE-Cyber Operations Program	First application: stated commitment. Renewals: 8 students and 3 faculty members over the course of the 5-year designation window.
10	Number of Faculty Involved in Cyber Operations Education and Research Activities	Minimum of two faculty actively teaching cyber courses.

The differences with the fundamental and advanced criterium are the following; Criterium 1: 100% foundational, 60% core, two specializations, and Criterium 9. Within the 5-year designation window, the graduation of either 5 M.S. or 1 Doctoral student in addition to faculty support to the CAE-Cyber Operations Program.

The CO option requires that programs have Accreditation Board for Engineering and Technology (ABET) to include courses such as a higher-level programming language such as Assembly taught. One of the significant differences in the technical depth that a program should have. This is different as the CD programs are taught in typically less technical departments such as business or management. Generally, when technical degree programs are housed in the school or college of business requirements for math, programming, and science-oriented courses are less as the accreditation that is sought does not require that. The flagship accreditation for business schools in the Association to Advance Collegiate Schools of Business (AACSB) International that only looks at the Management Information Systems (MIS) programs. The MIS degree programs serve as a bridge between business and technology-focused people. Thus the required business courses remove any opportunity for core technical courses that go beyond the intermediate levels.

Ethical Considerations

Some institutions that teach cyber offensive content has to be sure not to cross any ethical guidelines put forth by professional bodies. These organizations, such as the International Information System Security Certification Consortium (ISC)2, Information Systems Audit and Control Association (ISACA), International Council of Electronic Commerce Consultants (EC-Council), and others, have explicit constraints. If these codes of ethics are broken, then professional certification will be removed or barred for sitting for the examination. Additional ethical considerations would be accepting funds from organizations with activities that may go against the university's mission or belief system. For example, a liberal arts college may not want to take money for a laboratory from a defense contractor if there is a strong sense of creating global citizens that are focused on nation-building through peaceful means. Currently, this has not been a prevalent concern per news in the past several years.

Adaptive Curriculum

Education has generally lagged behind compared to what is being done in the industry. For this to be useful, universities will need to alter the lab environment to reflect recent events that have made the news (Cheung, Cohen, Lo, & Elia, 2011). Reconfigurable labs with 24/7 access that can be deployed by a student in a virtual environment (Hu, Cordel, & Meinel, 2004). This could give students the ability to recreate these environments themselves before a professor or lab technician does so. Additionally, labs can be developed to incorporate augmented reality to not only enhance the technical subject matter within the security labs but have students perform in simulated missions targeted on real-world scenarios (Wang, Callaghan, Bernhardt, White, & Peña-Rios, 2018). Researchers have spent a considerable amount of time incorporating smell and taste into computers and augmented reality (Ranasinghe, Karunanayaka, Cheok, Fernando, Nii, & Gopalakrishnakone, 2011).

Challenges

When discussing the lack of supply for the cybersecurity workforce's demand, universities have to be conscious of the low amount for cybersecurity faculty. Numerous programs offer a terminal degree in computer science, MIS, or computer engineering. However, there are few doctoral programs in cybersecurity that are housed in departments with a CAE designation. So as universities launch programs, they may be doing so with no terminal degree faculty in cybersecurity but preferably another technical degree with a specialization in cybersecurity. Faculty compensation is another issue as the resource pool of qualified faculty is low.

Another challenge is getting more US citizens enrolled in these degree programs to become a pipeline into federal and state cybersecurity positions. This would be essential as the curriculum changes for teaching offensive education would be on subject matter that deals with national security.

The US government uses the Department of Defense Directive (DoDD) 8140 as a way to measure professional certifications; however, this does not cover academic degree programs. (Baker, 2013). The challenge with this is that the categories are mainly focused on management and technical tasks that focus on activities around defense. The NICE Framework is broken into the following seven categories: 1. analyze, 2. collect and operate, 3. investigate, 4. operate and maintain, 5. oversee and govern, 6. protect and defend, and 7. security provision (Newhouse, Keith, Scribner, & Witte, 2017). Out of all these categories, the only one that comes close is analysis, but reading the language is heavily focused on cyber intelligence activities. The Framework is lacking an actual offensive security role breakdown.

Need to Develop an Offensive Security Workforce Framework

There is a strong need to develop a framework for an offensive security workforce. This framework would mirror what the NICE Cybersecurity Workforce Framework is. Positions would be flipped to an entirely aggressive nature where the role is to be on the offensive rather than a primary function of defense. This would also incorporate existing professional certifications to include developing new ones as well.

Table 2. Example Offensive Cybersecurity Workforce Framework

NICE CYBERSECURITY WORKFORCE FRAMEWORK	**OFFENSIVE CYBERSECURITY WORKFORCE FRAMEWORK**
Analyze	Research and Analyze
Collect and Operate	Intelligence, Surveillance, and Reconnaise
Investigate	Reverse Engineering
Operate and Maintain	Engineer
Oversee and Govern	Strategic and Tactical Planning
Protect and Defense	Attack and Neutralize
Securely Provision	Security Engineering

Development of New Skills

Students will need to develop a new set of skills rather than mastery of tools. Kali Linux, which is an offensive security Operating Systems (OS), has been used to teach students and employees (Beggs, 2014; Najera-Gutierrez, & Ansari, 2018). Figure 3, is an example of a project where students had to develop an Open Source Intelligence (OSINT) Tool application. This OSINT application was managed as a project in accordance with the DoD's guidelines for Earned Value (EV) (Kim, Wells Jr, & Duffey, 2003). Students working on this project not only enhance their programming skills but learn techniques of OSINT (Bazzell, 2016).

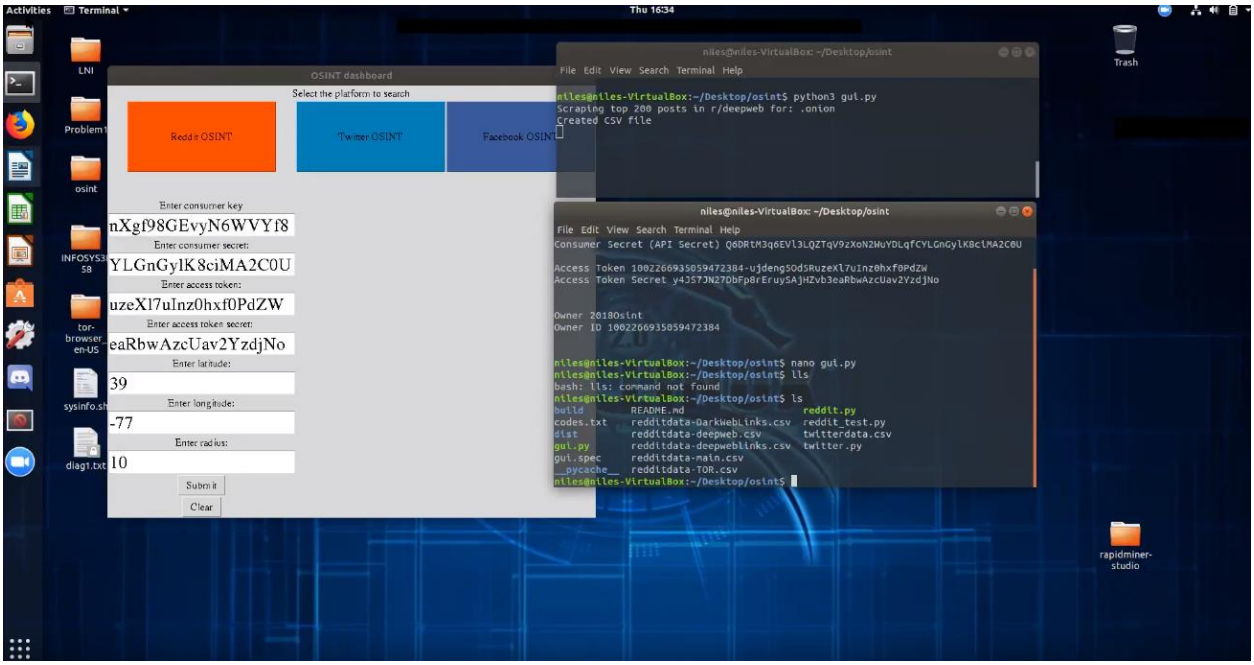

Figure 3. OSINT Application

It is not enough for students to learn concepts of offense but to develop their applications. This is a method to teach students information warfare and how to carry out an attack and understand the principles of cyber warfare (Davey, & Armstrong, 2001). Other activities include the analysis of the data taken by the application using Python. The use of Python, a tool for data science, shows students how powerful this language can be for combining intelligence application development and then analyzing all captured data to show trends (Cielen, Meysman, & Ali, 2016). To have faculty and students make this shift means prioritizing the focus heavily on offensive means that the lab environment needs to change, and students must become knowledgeable about war (Tzu, 2014). Understanding symmetric and asymmetric warfare will give the learner concerning military strategy past and present (Bruneau, & Kteily, 2017; Arreguin-Toft, 2001).

Further Study

Further research needs to be done in how an offensive cybersecurity workforce framework looks. This research needs to provide categories, work roles, skills, tasks, knowledge abilities. Additionally, this framework needs to incorporate current roles for defense and offense together. As there are identified positions open for cyber defense roles, the same needs to be done for offensive ones.

Final remarks

Course instruction is focused on defending cyberspace and not inflicting damage. Institutions need to move towards teaching more offensive coursework as institutions are the places where technologists are getting their foundation. The fear of developing the nefarious hacker needs to be removed and be replaced with a cyber professional that understands the full spectrum of cyberwarfare. If the U.S. is to remain a key player in cyberspace, then the training of professionals needs to change and become a new standard drastically. Since there is a lack of citizens, there could be a fast track program similar to those who fought during the Iraq War under President Bush in 2005 (Wong, 2005). A new framework that mirrors the NICE Cybersecurity Workforce Framework is needed to create an offensive security education. Establishing this will enable the U.S. to fully start building towards its offensive capability at earlier stages such as university and high school.

Emerging Technologies in the Fourth Industrial Revolution

In today's modern digitizing manufacturing landscape, new and emerging technologies can shape how an organization can compete, while others will view this as a necessity to survive as manufacturing has been identified as a critical infrastructure sector. Universities struggle to hire university professors that are adequately trained or willing to enter academia due to competitive salary offers in the industry. Meanwhile, the demand for fields such as Artificial Intelligence (AI), data science, and cybersecurity continuously rises with no foreseeable drop in demand in the next several years. This results in organizations deploying technologies with an inadequate staff that understands what new cybersecurity risks they are introducing into the company. Examined are how organizations can potentially mitigate some of the risks associated with integrating these new technologies and developing their workforce to be better prepared for looming changes in technological skill need. With the over a 10% growth in organizations deploying AI, the current cybersecurity workforce needs are over half a million. A struggle to find a viable workforce this research paper aims to serve as a guide for Information Technology (IT) managers and senior management to foresee the cybersecurity risks that will result from the incorporation of these new technological advances into the organization.

Introduction

In the Gartner's 2019 Chief Information Officer (CIO) Agenda survey, demand for AI implementation within businesses grew from 4% to 14% (Goasduff, 2019). This survey represented over 80 organizations and 3,000 respondents, which shows the transition to a new era in IT as digitalization continues quickly (Gartner 2018). Meanwhile, in fields such as cybersecurity within the United States (US), websites such as CyberSeek show over 500,000

total cybersecurity openings with the top three titles being cybersecurity engineering, cybersecurity analyst, and network engineer/architect (CyberSeek, n.d.). The supply of these workers is deficient. Reviewing the cybersecurity workforce supply and demand ratio for a national average is 2.0, while the national average for all jobs is 4.0 in the US (CyberSeek, n.d.).

Researches looked into technical skills needed, and data science management was one of the five in the group for Industry 4.0 (Pinzone, M., Fantini, Perini, Garavaglia, Taisch, Miragliotta, 2017). For data science management, some of the identified skills were data storage, the cloud computing, and developing applications in languages such as Python (2017). For this last skill, there is no mention of secure software in developing these needed data science applications. Over seventy-five percent of vulnerable are found within the code (Murtaza, Khreich, Hamou-Lhadj, & Bener, 2016). Nowhere in this skill needs report summarization in the first four roles was the mention of secure use of these tools. However, in IT and Operations Technologies (OT) within industrial automation, cybersecurity is mentioned about data privacy, safety, and security management.

Industry 4.0

Manufacturing has undergone many industrial revolutions that have changed the ability to produce goods, as shown in Figure 4. Technological advances have made these industrial revolutions possible. The third industrial revolution introduced computers and automation. Industry 4.0 is often referred to as the fourth industrial revolution in cyber-physical systems. The need for further automation and unparalleled levels of data exchange brings about multiple changes. These changes come in the form of Internet-enabled hyperconnected devices such as the IoT and the Internet of Everything (IoE). This digital revolution is changing the manufacturing industry in terms of what can be accomplished.

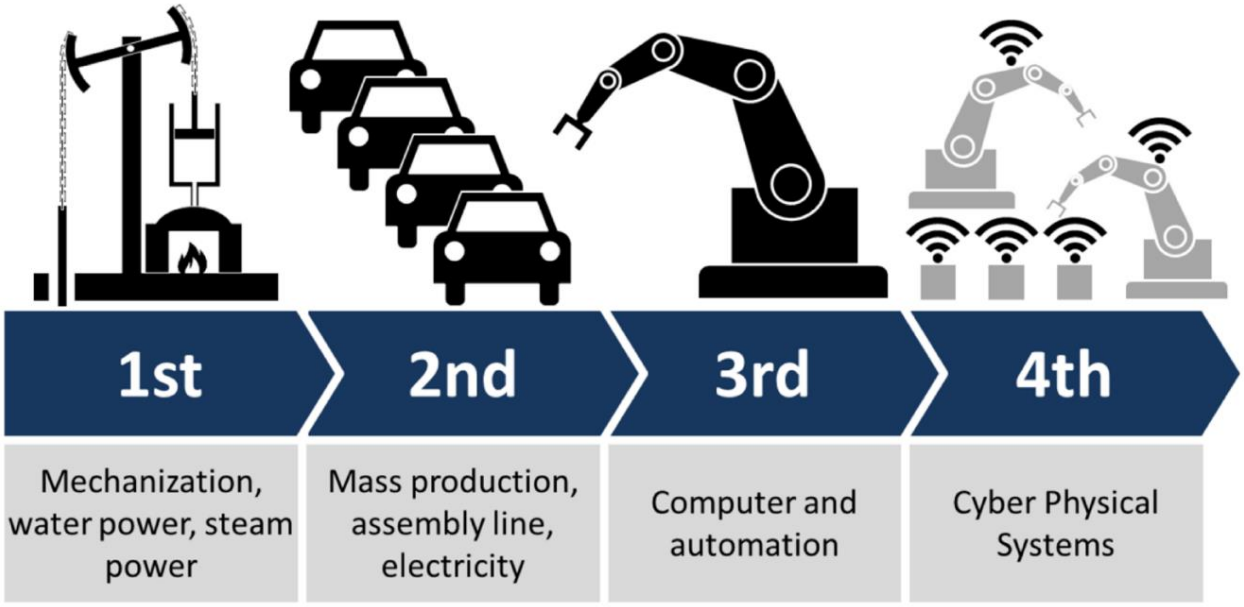

Figure 4. Industrial Revolutions (considering four waves)

Reprinted from Industry 4.0, by Wikipedia, June 19, 2018, retrieved from *https://en.wikipedia. org/wiki/Industry_4.0*. Licensed under CC Attribution-ShareAlike License.

As many industries look to incorporate IoT and other Internet-enabled devices, manufacturing is but one of them. While making this change, certain places such as the United Kingdom (U.K.) reported eighty-five participants falling victim to cyber-attacks (Ambrose, 2018). In the Middle East and Africa, the attacks have ranged from the leak of online dating profiles to oil refineries in Saudi Arabia. With cyber-attacks continuing to rise from year to year, there is a push to incorporate another sophisticated technology into manufacturing.

The Promise of AI in Manufacturing

In 2016, two reports from the White House described the promise and the future of AI as it affects automation and the economy (White House, 2016a; White House, 2016b). Specifically, some of the growth could be achieved by adopting technologies such as robots and

systems that allow for massive improvements in the supply chain (White House, 2016a). The use of AI in Industry 4.0 based manufacturing systems is still emerging, and lots of work to be done to ensure proper development and implementation (Lee, Davari, Singh, & Pandhare, 2018). The goal is to produce more goods with fewer employed workers in the facility, which would enable economic growth globally. The National Institute of Standards and Technology (NIST) shows that significant advances in AI are a rise in productivity, efficient resource use, and increased creativity. However, the downside was the negative impact on the job and helping raise inequality.

Evolving Environments

With organizations pushing for more connectivity and resulting in more complexity amongst hyperconnected systems, then the leadership must understand what the results are for organizations. As the push for a competitive edge requires more data so that our data scientists within the organization can perform statistical analysis to reveal how the information could be harnessed for the competitive edge, it becomes essential to consider the security implications of tool adaptation. The Fourth Industrial Revolution consists of high levels of automation and unparalleled data exchange levels with unknown security risks (Dawson, 2018).

With events such as Coronavirus Disease (COVID-19), remote work has been strongly encouraged in some metropolitan regions within the US (and across the world). This has increased the need for social distancing to keep employees safe, remote system management, virtual collaboration, and an expansion of cloud computing services. With systems already poorly protected, this added layer of technical work only adds to the threat landscape. Researchers debate how the COVID-19 crisis is challenging technology and how it could accelerate the revolution (IEEE, 2020). The number of cybersecurity attacks has risen since the global pandemic includes even attacks on the World Health Organization (WHO) (WHO, 2020).

Overall, attacks rose by six times the usual levels for hacking and phishing attempts (Muncaster, 2020). These have been felt among all industries, from manufacturing to healthcare.

Understanding the Risks

Organizational cybersecurity risks for AI fall into three areas [See Table 3]. The first area is people who can be associated with inadequately trained personnel. Inadequate training can lead to falling for deepfakes and allowing authentication to rely solely on stored credentials that another user could obtain through circumvention. Misplaced trust is yet another result of a corporate roll-out plan that is not inclusive and does not account for issues that will come up for those who are ultimately impacted by this technology's implementation. The second area of risk can is in the process. There needs to be proper automation of processes that incorporate proper security controls. If there are poor security controls in the AI to include the overall manufacturing systems, this will increase the threat landscape. The last area of risk is technology. The technology being implemented needs to undergo full system testing, which includes the testing in the sandbox environment to deployment. Periodic testing needs to occur to ensure that newly released and older Common Weakness Enumerations (CWEs) do not affect the system's security posture. However, testing falls also into the risk of the process as the organization would need to have selected or designed a process that consists of frequent and in-depth testing.

Table 3: Organizational Cybersecurity Risks for AI

Area of Risk	General Risk Description
People	Inadequately trained personnel using technology for operational use.
	Falling for deepfakes.
	Malicious use of AI.
	Misplaced trust.
	Improper execution of the selected process.
	Mismanagement or loss of credentials.
Process	AI automation of critical points for identification, authentication, and authorization.
	Poor automation of processes that include security.
	Incorporating an incorrect security framework.
Technology	Built-in software bugs, flaws, and vulnerabilities.
	Poor interoperability of AI into systems.
	Ineffective system security to safeguard AI.
	Supply chain risks.
	Inadequate testing.

In the area of risk, it is essential to note that people develop even the AI, so having component developers means a lot to how the AI will ultimately behave. The design of complex algorithms that give life to the system is solely dependent upon the skills of that engineer. For years, people have wrestled with AI's capabilities and exactly where that would lead society (Minky, 1982). The thing that researchers did not place enough thought into was how to equip those ultimately responsible for the AI systems to defend them. For the staff that will manage these manufacturing floors, it is imperative that they understand IoT and how AI ultimately changes this ecosystem.

Currently, in the majority of industrial engineering courses, cybersecurity is not in the curriculum, after reviewing numerous programs in managerial education, such as advanced degrees such as the Master of Business Administration (MBA). A review of over forty MBA programs shows that the technical coursework may have a course that deals with Information

Systems (IS) and a small section dedicated to cybersecurity in a high-level generalized delivery. This is inadequate and not focused enough to have those insights on future challenges.

Training is another critical factor in executing organizational processes regarding technology (Umble, Haft & Umble, 2003). For any selected process to work effectively and efficiently, those responsible for carrying out the process should have been trained and aware of the actual processes. It will be already challenging enough to insert new changes into the organization, but this must be done in a manner that allows retention.

For designing the AI, developing security throughout the lifecycle is vital, as displayed in Figure 5. This means there is a need for well-defined requirements and interactive testing of software. Doing this allows for proper inspection of the code to ensure there are no backdoors, dead code that allows for exploitation, or hidden malicious programs.

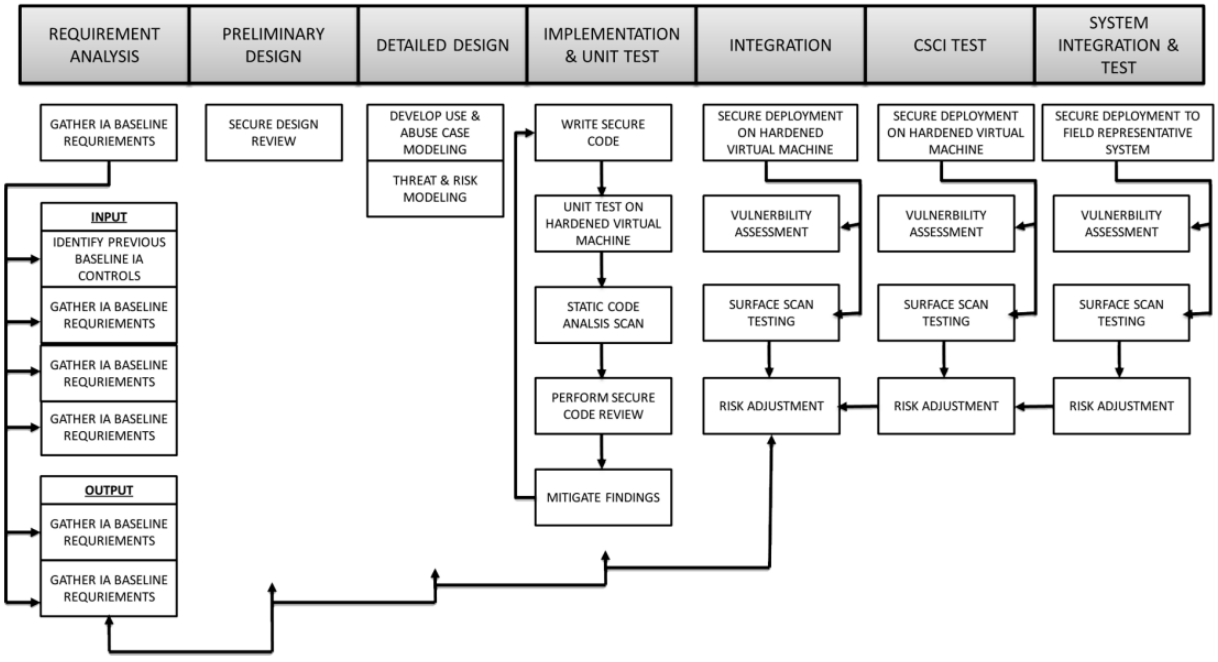

Figure 5: Secure Software Development Process

Technology has been identified as the final area of risk to address. As managers and senior leader leaders wish to add these technologies, several things can be done. The supply

chain and the acquisition of systems is a risk within technology. Not knowing the origin of a particular piece of code or hardware poses a risk as the quality or security of that specific item may create a vulnerability for the more extensive system. Imagine the actual algorithm being developed by a nation-state that ends up rerouting critical data or causing a catastrophic event at a facility such as fire due to overheating.

Importance of Manufacturing in U.S.

As of February 2019, an EO issued maintaining leadership in AI (Trump, 2019). It calls for promoting AI research and innovation while protecting American AI. At the same time, Putin wants to be the global leader for AI and use it in AI-driven asymmetric warfare (Polyakova, 2019). However, after investigating the investments in AI, Russia falls far behind countries like China. Countries are scrambling to ensure they are global players in AI with significant investments, while Nevertheless, cybersecurity attacks on the manufacturing industry could be devastating.

The U.S. Bureau of Economic Analysis (BEA) data from 2010 to 2019 shows the gross output for multiple industries. In Figure 6. The industries evaluated are the following: 1. Manufacturing, 2. Agriculture, forestry, fishing, and hunting, 3. Educational services, health care, and social assistance, 4. Construction, 5. Utilities, 6. Transportation and warehousing, 7. Mining, and 8. Information. The year 2019 shows manufacturing being 16.57% of total gross output (U.S. Bureau of Economic Analysis, 2020). In 2018 that percent was 16.98%, 2017 was 16.86%, 2016 was 16.9%, and 2015 was 17.73% (U.S. Bureau of Economic Analysis, 2020). This data provided by the BEA shows that manufacturing is significant to the gross output for the U.S., meaning that if this industry becomes under attack, it could result in catastrophic events such as loss of critical IP, manufacturing output, and overall lower gross output that would lower the total output by an estimated 16%.

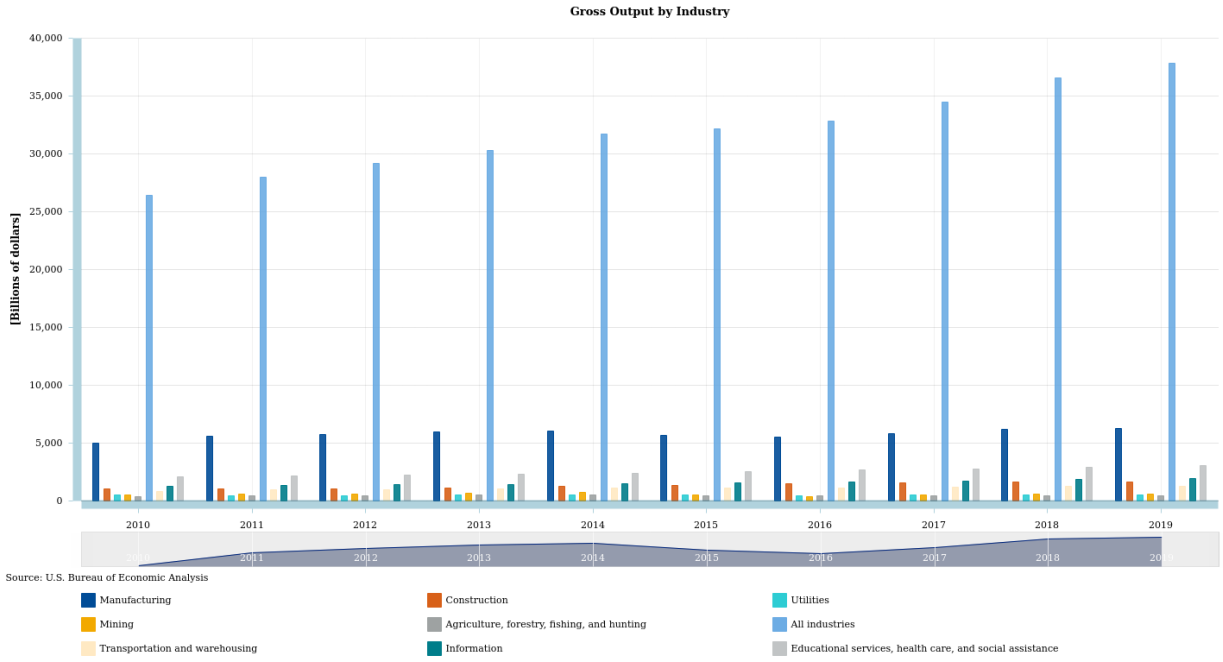

Figure 6: Gross Output by Industry (U.S. Bureau of Economic Analysis, 2020)

Final remarks

Today's modern manufacturing IoT environment requires organizations to manage expectations and risks as they relate to cybersecurity effectively. Organizations need to consider how they fully utilize technologies such as data science while protecting the data that is being analyzed. We examined some risks associated with organizational uses for AI. Understanding cyber defense and cyber offensive viewpoints may yet provide some insight into how organizations should conduct tests to review the threat landscape (Dawson, 2020).

They were identified three areas of risks that need to be managed for implementation of AI into Industry 4.0. Reviewing data from BEA proves the significance of manufacturing in the U.S. industry to include the impact of the cybersecurity vulnerabilities that are not managed appropriately. The conclusion is that as the increased use of AI in critical industries such as

manufacturing, it is essential to ensure that proper security controls are in place to thwart any possible threat, whether internal or external (Gill, 2019).

Nefarious Activities within the Deep Layers of the Internet

Cybercrime affects multiple areas of society with nefarious activities ranging from human trafficking to illegal arms sales. The Internet has allowed some nefarious activities to be revived as others have emerged in this new age. In turn, this has become a national security issue for countries as this requires resources to combat this evolving threat. These activities include undermining legitimate services that provide government services to its citizens, such as passport, national identification, tax services, and more. This session introduces some of these activities, enabling readers to understand this digital criminal world further.

Introduction

The Internet has allowed for many technological advances that have brought forth positive outcomes. In retrospect, the Internet has also allowed for criminal activities to flourish. Moreover, while both positive and negative effects are expected, the use of the Internet by a criminal organization, nation-states, terrorists, extremists, and others finds another means to market their illegal activity. As the introduction of the technological phenomenon is no longer seen as a luxury but rather a basic need in some parts of the world (Reglitz, 2020; Greenwood, 2013). However, some nations heavily regulate Internet activities under the umbrella for terrorism, maintaining a political stronghold, censorship, or enforcement of that country's religious laws (Ayalew, 2019; Deibert, 2009). A handful of nations have been known to engage in censorship, such as China, Iran, and Saudia Arabia, to name a few (Deibert, 2009). Meanwhile, more countries have been known to use the Internet to target political dissidents

such as Cuba, Ethiopia, Eritrea, Gambia, Morocco, North Korea, Russia, and more (Committee to Protect Journalists, 2020). Even with this mentioned censorship and oversight, illicit activities remain on the rise through the Internet.

In recent years, police and other law enforcement organizations have shut down pages that advocate prostitution. Originally websites such as Craiglist were known for the infamous ads that asked for donations in exchange for time (Hemmingson, 2008). This was the beginning of a new age for sex work, which took prostitution off the streets and created an atmosphere where the buyer could purchase a wanted service online (Cunningham & Kendall, 2011). From Craigslist, Backpage became the new marketplace for sex with a sophistication, unlike others. Sites alike followed to assist in identifying law enforcement masquerading as prostitutes to warm others before they finalized an arrangement. This included keywords, emojis, and code talk that avoided communicating in a manner that didn't incriminate them. Other measures that modern computing platforms had using cloud services that were used as an untraceable telephone, voicemail, and text messaging. Previously, a telephone number could be used to identify a person. Still, with Google Voice services, this allowed people to create an email and cloud-based telephone service to avoid using their actual provider. And if confronted by law enforcement, it was easier to hide the number with removing the application or now having the cloud service forward the call to their phone. In turn, this made it challenging for law enforcement entities to use that as a sure means to locate the person providing services as now individuals could screen potential customers.

Human Trafficking

Websites such as Backpage were not only known for prostitution but human trafficking. Encrypted currency such as Bitcoin has allowed for illegal transactions of human sales to remain undetected and nearly untraceable (Portnoff, Huang, Doerfler, Afroz, & McCoy, 2017).

And even when the Federal Bureau took down Backpage for Investigation (FBI) shortly after similarly named sites popped up. Thus, taking down the page served only as a quick win as one can use cached pages and repost information used previously.

For those involved in more sophisticated methods, the Dark Web remains the best avenue to stay undetected. As hyperconnected systems create a unique problem solving this matter becomes complex (Martinez, 2019). This means that when users have multiple social media pages, IoT devices, public information, and data revealed through breaches, it allows someone to become a target through careful analysis of that information. Unprotected and uncontrolled data enable an attacker to target entities through careful selection (Martinez & Dawson, 2019).

Social media pages such as Facebook, Instagram, Twitter, and others create an environment that enables personalized social engineering (Stewart & Dawson, 2018). Information such as a birth month, home address, location, and even a public network allows an attacker to begin working on exploitation techniques. These can be in the form of someone carefully selecting a target to a third-party having access to the account through a developed application in which a user has granted rights to their information to use it. Researchers have looked at what factors lead to gullibility in an individual faced with social engineering threats based on personality traits. For human trafficking, it has been uncovered that some tactics are through the promise of work overseas with the hopes of escape from an oppressive or dangerous environment.

Online Marketplace

While human tracking has mostly moved to the Internet, so has other illicit activities such as the purchase of narcotics, government documents such as USA driver licenses, passports from multiple countries, and services such as contract killers. Former sites such as the Silk

Road served as a crypto market for illegal drug trading until it was closed two years later (Maddox, Barratt, Allen, & Lenton, 2016). Since Silk Road has been taken down, numerous pages have taken its place. Furthermore, the problem with shutting down the operations on these pages is that the Dark Web consists of unindexed pages that are not found using an everyday browser such as Firefox, Chrome, or Internet Explorer. To even access these Dark Web pages, The Onion Router (Tor) is required to be installed in the system. Figure 7 displays a screenshot of an onion page accessed with the Tor Browser using Hidden Wiki to locate the page. The Hidden Wiki serves as a guide to pages on the Dark Web to be accessed, describing its service (Sinha, 2017).

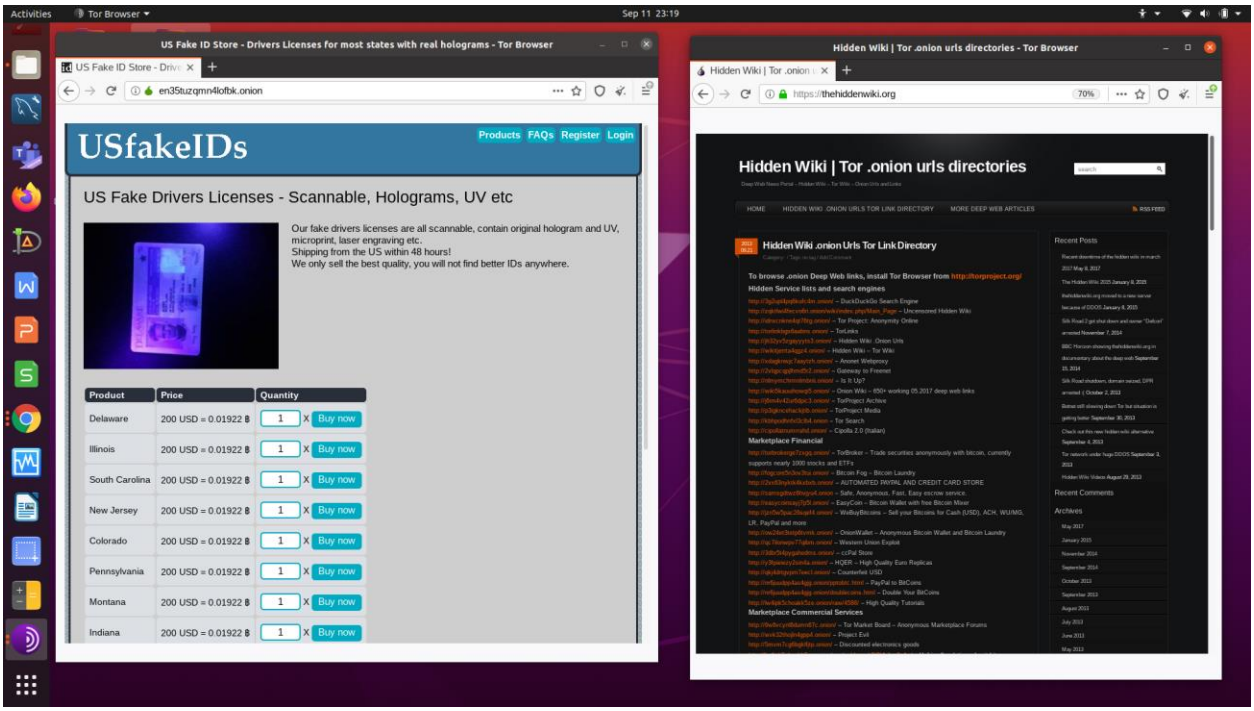

Figure 7. Example of Online Marketplace on Dark Web

Sites such as USfakeIDs provide their customers to purchase a driver's license from any state. These licenses are advertised as being near authentic to including the hologram. This site could serve underage teens in the purchase of alcohol, illegals who require proper documentation, or individuals who seek something much more sinister as maintaining an

identity to plan a terrorist attack. Other items sold are passport, birth documents, and other government-provided documents that are used to establish an identity on similar sites.

While the Hidden Wiki is not all-inclusive, it does provide a starting point for those getting familiarized with the shadowy marketplace. Some sites that provide auctions and other services require Bitcoin payment before giving the actual onion link. This action is to show a real desire to participate rather than just browsing a storefront of illegal services and goods.

Navigating the Dark Web

The Dark Web requires Tor Browser to be installed on the system. While installing the browser allows someone to be safe, the other issues remain around the privacy of an Internet Service Provider (ISP) viewing activities. So the installation and the use of additional services of Virtual Private Network (VPN), encryption, and other security tools to altogether cloak activities is recommended. If the user uses Ubuntu or another Debian based Linux distribution, then installing the necessary Personal Package Archives (PPAs) must be done through the Command Line Interface (CLI). After that typing, the below installs and runs Tor.

```
sudo apt update
sudo apt install torbrowser-launcher
```

Once Tor Browser is installed, then in the CLI typing *torbrowser-launcher* will launch Tor. Navigating to show the application, then one could locate the application as well. OSs such as Kali Linux and Tails have a number of these applications prebuilt. These OSs can do more than navigating the Dark Web while others are developed with digital crime and cyber warfare (Dawson & Omar, 2015).

Online Forums

Another critical aspect of the Dark Web is online forums. Countries have laws in place to protect and provide rights, such as freedom of speech. Therefore online forums provide a medium where people can freely share how they feel with like-minded people. This is especially important in certain countries, where current regimes do not reasonably support information freedom. However, alt-right groups, nationalists, and domestic terrorist groups use these forums routinely to spread violence and hatred filled messages, and disinformation. In 2019, sites such as 8chan were removed from their host provider as three separate white nationalist groups posted manifestos in the forum. Pages such as 4chan and Reddit still have subthreads such as r/pol, banned. These pages are used to spread disinformation, propaganda, and incite violent behaviors. In social media pages, it was uncovered that Russia controlled one of the largest Black Lives Matter (BLM) groups and used the Internet to further create a racial divide among Americans (Jamieson, 2020; Johnson, 2019). The website 4chan has banned the politically incorrect thread on the message board that could be found using *https://boards.4chan.org/pol/* in the address bar.

Other platforms may not give into online disinformation or spread hate but instead, inform individuals on how to obtain information for a service or good that may be deemed illegal, such as the sale of illegally acquired credit card data or other personally identifiable information – making the Dark Web an attractive platform for those engaged in similar activities. There are several pages that professionals sell their services. For example, you can rent the services of a professional hacker in exchange for Bitcoin.

Additionally, one can purchase an assassin if the need is to remove someone. Another outlining issue is how this site can lead to the purchase of illegal or counterfeit goods on the Dark Web.

These activities threaten national security as they can be identified and other legitimate credentials that allow a bad actor to navigate freely while being undetected. With gun crime high in some US cities, law enforcement must be able to track down firearms that are used in crimes. With 3D printed guns and gun parts, anyone can manufacture unlicensed and untraceable weapons. One such 3D gun that started this discussion was the Liberator gun (Walther, 2015). The federal government moved swiftly to have the file removed from the web, but hundreds of downloads occurred before this happens. Since then, the file has been shared on selected channels and still available today.

When discussing human trafficking, sex work is one area where women and children are trafficked into where they work under the cloak of a legitimate business. Massage parlors have been known to traffic people illegally.

One particular site, *rubmaps*, served as a forum for massage parlors and provided detailed reviews. This site offered detailed reviews and mapped directly to the active or inactive massage parlor. This particular site uses a .ch domain as numerous others to avoid being shut down by the US government.

This allows a site to operate outside the legal jurisdiction of the US. Figure 8 shows the amount of detail provided from ethnicity to which provider does what service. Other details include operating hours, payment accepted, and if business accommodates semi-trucker.

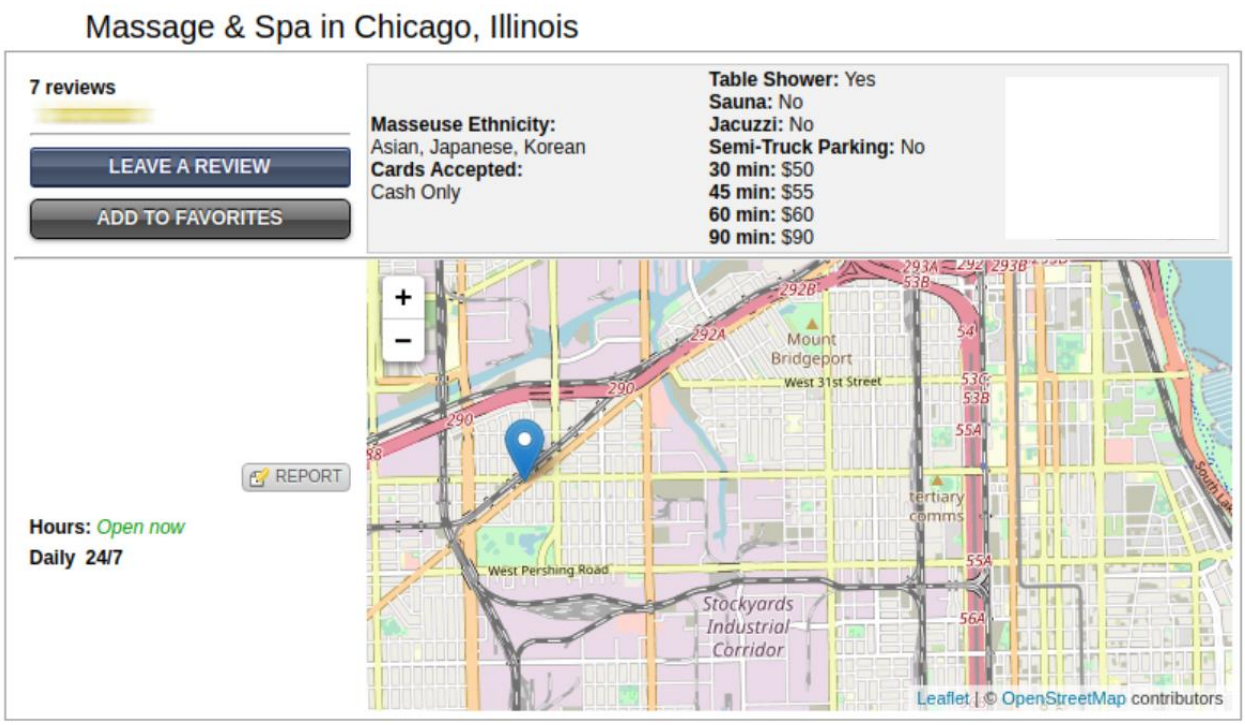

Figure 8. Example of Rubmaps Massage Review

Supply and Demand on the Dark Web

Prices on the Dark Web can vary. Some factors determining the costs of these illegal assets is the type of the data being sold, the balance associated with the accounts, and the limits of possibilities of reuse of the stolen information (Stack, 2018). The economic concept of the fluctuation of supply and demand exists in this underground market: a set of account credentials is going to be cheaper than purchasing IP information illegally; and newly hacked credit card numbers will be bought for higher prices than records from breaches that happened months ago (Ablon, 2018). Credit card account information can be purchased either individually or in bulk (Spalevic & Ilic, 2017). Also, Stack suggests that there are often bundle offers containing various types of data bundled together to provide a valuable package for identity thieves (Stack, 2018). Specifically, Social Security Numbers (SSN) can be bought for about $1, credit or debit cards range somewhere between $5-$100, which is on the higher end. Data from

online accounts such as PayPal have sold for $20-$200, while driver licenses about $20, US passports for $1000-$2000. diplomas for $100-$400, and medical records for $1-$1000 (Stack, 2018). Driver licenses sold from other countries have sold at lower rates.

Cryptocurrencies and Blockchain

One attractive payment method on the Dark Web is cryptocurrency. In recent years, cryptocurrency has been the rave, but that has been surrounding the exploding growth in Bitcoin's value. There are only aspirations and hopes of regulating cryptocurrencies (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016). In the meantime, this form of payment is prevalent for the exchange of illegal goods and services. One researcher takes an in-depth look into Bitcoin money laundering, exploring the negatives and positive outcomes of using cryptocurrency (Bryans, 2014).

Even though the hype is dying down around cryptocurrency, this is still the currency of choice to evade law enforcement (Wolfson, 2018). Among the largest unregulated markets in the world are cryptocurrencies. Researchers estimate approximately $76 billion of illegal activities per year, with one-quarter of Bitcoin users involved (Foley, Karlsen & Putniņš, 2019). These numbers are astronomical and transforming the known black markets by enabling new e-commerce. Currently, exchange rates are among the highest rates despite the American political climate and economy.

There has been a movement to trace criminal activity across the Bitcoin blockchain. By examining the blockchain activity through a process called clustering, discovering accounts purpose uncovers what type of storefront it is linked to. For example, if an account is used to make purchases on a Dark Web marketplace, we can begin to pinpoint appearances tied to the same Bitcoin wallet. This action may mean the same entity also controls them. Once that entity

becomes known, then analysis can be done to begin uncovering who that entity is through methods such as OSINT and other forms of intelligence analysis coupled with data-driven tools.

Final remarks

The activities that were once considered in the shadows over the years were brought into the light. For a moment, law enforcement agencies globally were able to, at the least, understand what needed to be done and begin to use resources to combat these issues. With the emergence of the Dark Web, and cryptocurrencies Internet-driven illicit activities have a refuge. To effectively combat this problem, sufficient resources must be made available. Another action is educating people early enough to become aware of safe and secure Internet use to minimize the risk and exposure associated with their PII. When individuals know how to properly lock down their pages and understand how to limit their threat landscape, it will be more difficult for predators to prey upon them.

Bad actors have shown the ability to quickly move people and goods largely undetected, which demonstrates multiple holes in a supply chain, policing, and detecting abnormalities in a more extensive system built to protect its citizens. However, with online websites that provide access to various illegal products and services in an almost untraceable manner with a click of a button, fighting these crimes is an ambitious effort. With the widespread engagement in social media, disinformation nation-states and others alike can influence massive crowds. Through the use of cryptocurrencies, the funds used for illegal activities become difficult to track. Internet-driven illicit activities can undermine what governments have set up to build confidence among its citizens to include circumventing established laws.

Software Security Considerations

For the year 2020, it shall be the year of the global COVID-19 pandemic and the impact this virus had on economies worldwide. This virus has spread from China to the rest of the world, and this has effectively changed how organizations had to operate, causing them to migrate online quickly. This rather quick transition led to organizations increasingly becoming under cyber-attacks as they were not prepared to operate as fully virtual organizations. During this period, many cyber-attacks were executed successfully. Some attacks were targeted to dismantling key services while others for massive data collection.

Towards the end of December, the US underwent a serious hack that affected multiple companies such as Intel, Cisco, and numerous government agencies (Clark, 2020; BBC, 2020). This attack shows the far reach of offensive cyber capabilities and why it is so important to understand the ever-changing threat landscape fully. Understanding this landscape while actively deploying not only security mechanisms but developing security into the software lifecycle can serve as a way to mitigate threats.

Software Testing

Software testing is a misunderstood task that can make an application vulnerable and increase the threat landscape (Potter & McGraw, 2004). As many of the system's vulnerabilities are found within the application layer, testing is critical to minimizing the overall system (Alhazmi, Malaiya, & Ray, 2007; Paul, 2016). Secure software testing is an essential task for developing an application that is not readily susceptible to attacks. In Figure 5, a process is

displayed that enables developers to produce code that undergoes ri.gorous testing phases before deployment, following the Software Development Life Cycle [Figure 9].

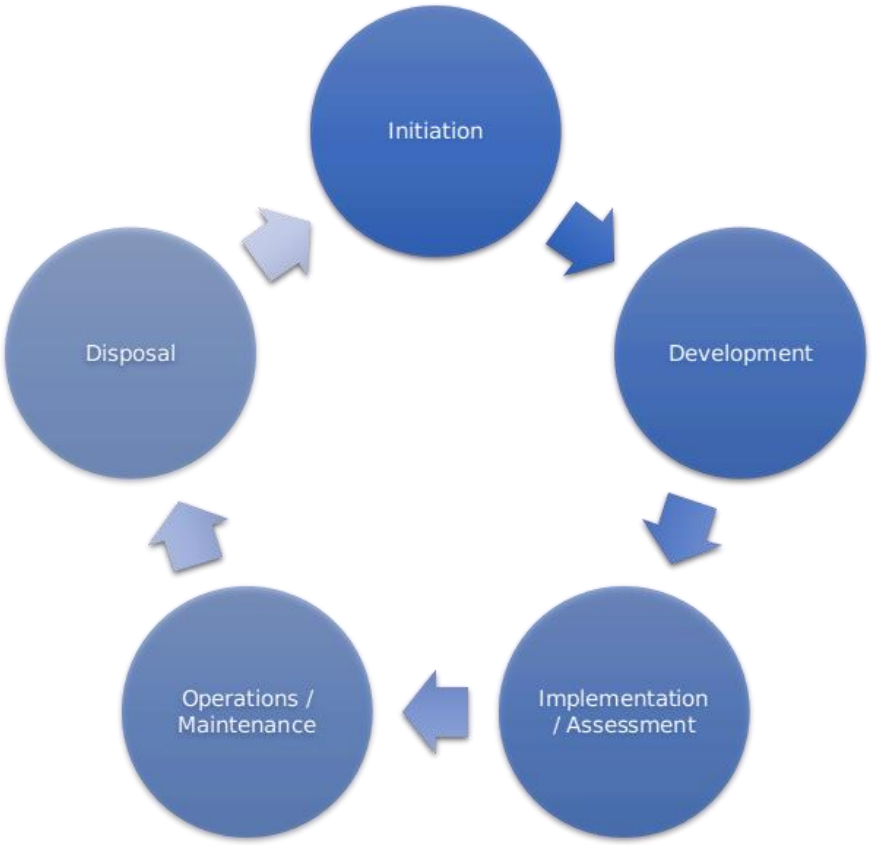

Figure 9: Software Development Life Cycle

In the requirement analysis phase, baseline requirements must be defined. All threshold requirements must be established that need to be met. This would also include how they are tested, such as inspection, observation, analysis, and an actual test. In the next phase, the application or system's preliminary design goes through a secure design review. This review goes through the requirements, expected system functionality. Once this phase is finished, the detailed design occurs where threat modeling, risk modeling, test cases, use, and abuse cases are developed. Only once this stage has met all criteria for moving forward, the implementation and unit test begins. Here secure code is written and unit testing on a hardened Virtual Machine (VM). The VM is hardened according to the environment the expected production unit will be in.

For example, if it were the application needed to be placed into a federal system, then it would need to complete the NIST Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. This would mean that the VM has either low, medium, or high-security controls applied to the VM before the test begins. Once this occurs, static code analysis and code reviews start. Upon completion of these tasks, vulnerabilities are discovered and then mitigated down to an acceptable level.

The integration phase would take the secure, hardened VM and perform a vulnerability assessment, surface scan, and risk adjustment. Afterward, there are two more testing phases: the Computer Software Configuration Item (CSCI) test and system integration and test. During these phases, the same subtasks occur as in integration. At the end of this process, the completed code has the possibility of achieving a status indicating it has passed through a rigorous test regarding a yearly review unless there has been a risk introduced into the code. The technical lead could help set what those thresholds are only if there is no industry-standard requiring compliance. However, that lead proposes the delta requiring change that decision needs to be documented and part of the system and software design testing process.

Sandbox Environment

Performing multiple tests in a sandbox environment allows time to discover any bug or vulnerability before a production release. This discovery process, through rigorous testing, minimizes the number of vulnerabilities that the end-user will have to inherit. Additionally, this allows the application to be isolated and in a safe environment, so if something does occur, it will not affect any other systems. Without knowing the application's full behavior in a production

environment or one that is integrated with other methods, this sandbox would allow developers to add in those other systems while testing them incrementally slowly. If there is a failure, it is easy to identify the system environment or configuration in which the fault appears. Figure 10 displays how a Linux sandbox environment where Javascript source code is being tested using a static code analysis tool. This application shows the user precisely the flaws, dependencies, and other associated bugs. Additionally, the severity impact is also provided, which informs an individual of this discovery's criticality and the potential damage that can be caused if exploited.

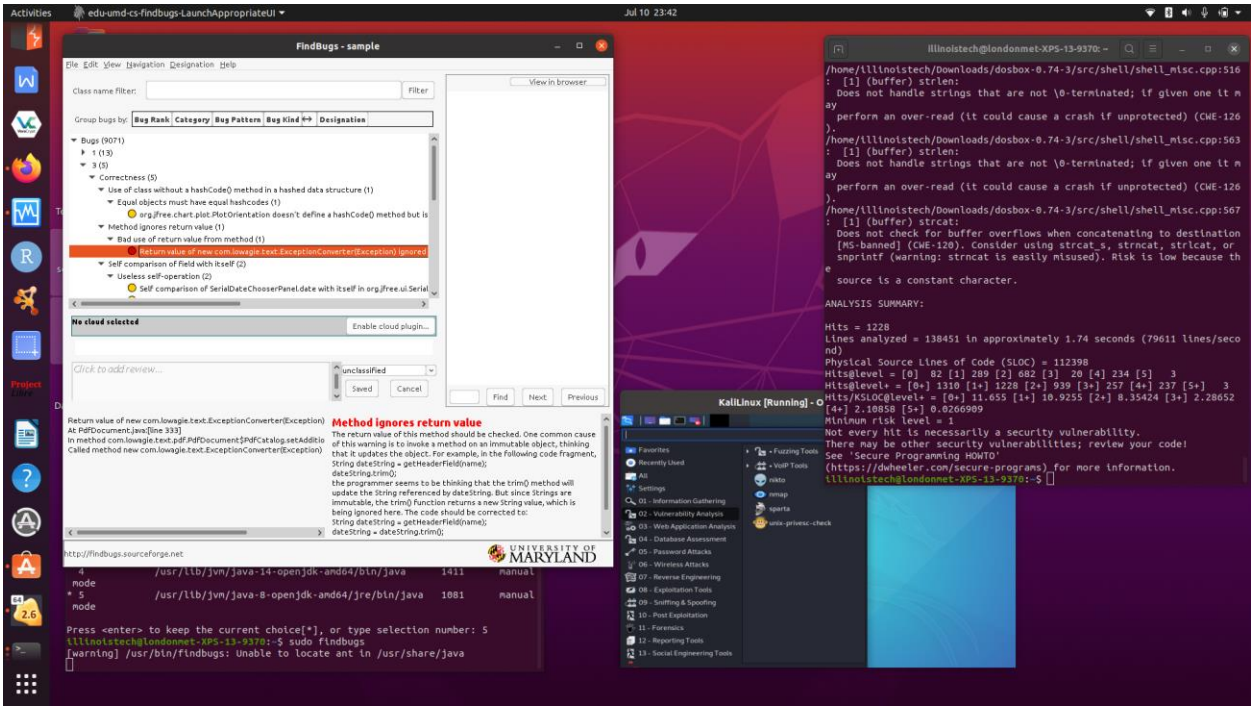

Figure 10. Linux Sandbox Environment

This environment also allows for the proper discovery of how to successfully inject malicious code or malware into a system. A virtualized lab can be used to teach offensive tactics regarding penetration testing, reverse engineering, malicious code, privilege escalation, and more (Timchenko & Starobinski, 2015).

Emerging Computing Environments

To better deal with the emerging computing environments, frameworks need to be implemented that are suited to handle this change. Applying a holistic cybersecurity framework such as the Mission Framework would allow organizations seeking to establish environments that would enable them to be successful regardless of location while examining external and internal conditions (Dawson, 2018). This framework comprises three themes education, policy, and technology to implement cybersecurity within an organization [See Figure 11].

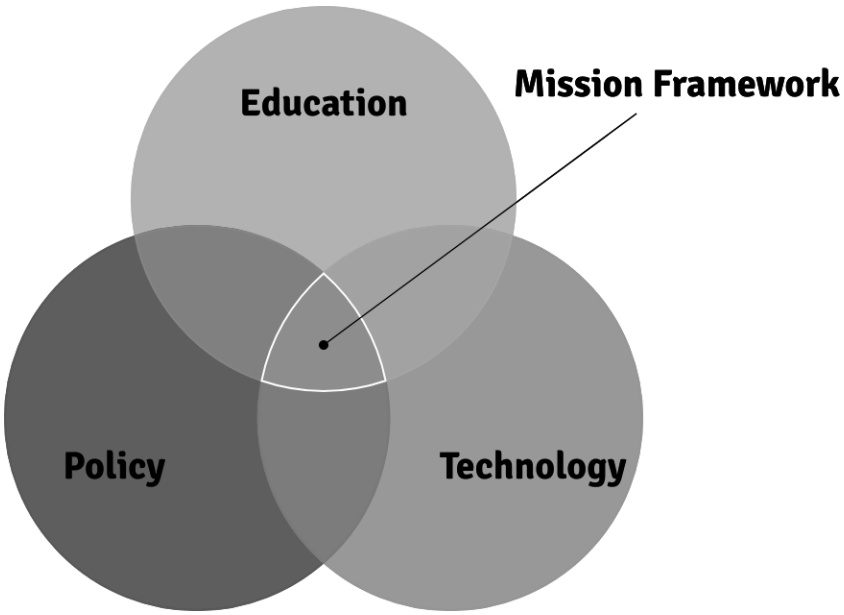

Figure 11. Mission Framework

The Mission Framework allows an organization to protect their critical systems and provides a means to develop attacks at a high level strategically. If one of the framework's elements is not adequately met, it allows an attacker to take advantage of that. In one scenario, an attacker can start identifying areas not being taught, such as secure low-level programming. Then look at technologies identified by that region that has that deficiency in their education system and begin the process of attacking targets in that region. The hope is that by targeting companies in this, this region for that specified and concrete technology threat is that the hired employees are not knowledgeable about identifying this threat or how to remedy this vulnerability properly. This is weaponizing the Mission Framework to develop strategic and tactical cyber offensive measures.

Critical Infrastructures Challenges

The cybersecurity of critical infrastructures is an essential topic within national and international security as 16 critical infrastructure sectors touch various aspects of American society. Because the failure to provide adequate cybersecurity controls within the critical infrastructure sectors renders the country open to an attack that could have a debilitating effect on security, national public health, safety, and economic security, this matter is so vital that there is the Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning and resilient critical infrastructure. An organization identified as the Cybersecurity and Infrastructure Security Agency (CISA) at the DHS has the mission to be the risk advisor for the United States (US). Other organizations, such as the NSA, have approved a specific Knowledge Unit (KU) to

address cybersecurity for critical infrastructures associated with doctoral-level granting programs. To address this challenge, it is necessary to identify threats better and defend against them while mitigating risks to an acceptable level. Only then can a nation build a more secure and resilient infrastructure for the future while defending against present-day bad actors as cyberwarfare, cyber espionage, and cybersecurity attacks are the modern-day threats that need to be addressed in planning, designing, implementation, and maintenance.

With recent events from global pandemics to the shift in economic powers, many challenges lay before us. These challenges created new adversaries and motivated older ones to get re-engaged. Understanding these challenges will help develop a mitigation plan to avoid these severe consequences by failing to do something. Table 4 shows the threat and gives an example of what that threat is. This table provides insight at a high level of what organizations will need to be aware of when deploying systems that may be inadequately secured.

Motivated hackers, hacking groups, and nation-states aim to sabotage infrastructure systems by changing or adding code in such systems to negatively manipulate functions with the goal of information leakage, total system failure, or system harm (Wilson, 2014). An example of this could be a hacker injecting malware into a power grid system. With this unauthorized control, the hacker can manipulate electrical power functions or possibly shut the grid down. There are many dependencies when it comes to critical infrastructure working as expected. If an attack happens on one system, it disrupts multiple other networks (Robles, Choi, Cho, Kim, Park, & Lee, 2008).

An example of this is initially shutting down a traffic control system to disrupt vehicle traffic flow and creating a constant traffic control system, such as keeping all traffic lights green to increase traffic violations. Cyber attacks on water supply infrastructure systems can be devastating, both directly and indirectly (Lewis, 2002). Presently, if hackers can gain unauthorized control of a watergate system, they can cause flooding resulting in damages to property and lives. Indirectly, effects can lead to sanitation and purification issues for

neighborhoods and cities or even deny access to water for firefighters in emergency events. Cyber attacks on electrical infrastructure systems can occur when a hacker gains unauthorized control of an electrical power system to cause nearby blackouts/brownouts resulting in limited access to the Internet (Lewis, 2002). This can carry over into other effects such as shutting down traffic lights to cause traffic complications and limiting public communication channels as Wi-Fi connection to routers that use electricity can be shut down without a proper backup electrical source. Table 4 shows the threat, damage to occur, and example.

Table 4. Threats

Threat	Damage to Occur	Example	Keywords	Reference
Cyber-Physical system break-ins	Compromising automated manufacturing processes leading to a halt in production or employee safety risks.	A hacker is gaining access to a manufacturing system that utilizes physical feedback technology, such as sensors, to track manufacturing output. Once access is achieved, the hacker can stop system processes such as manufacturing output.	Cyber-physical system	(Bracho, Saygin, Wan, Lee, & Zarreh, 2018).
Process parameter manipulation	Once an attack changes system process parameters, product quality assurance is affected by the potential to bring faulty/harmful products to the market.	An attacker is manipulating design files or process parameters to modify the quality assurance process.	Cyber-physical system	(Wells, Camelio, Williams, & White, 2014)
Intellectual property theft	Sensitive files such as product designs and system processes are becoming comprised of the use of spyware.	Opposing companies/countries using such compromised information to copy the competitive edge manufacturing companies operate.	Cyber espionage, Spyware, Data theft	(Friedman, Mack-Crane, & Hammond, 2013)
Cascading failure	Once one manufacturing system is compromised, other dependent systems become affected/nonoperational such as delivery systems for the manufactured products.	Once a hacker can break into a manufacturing system, other supply chain components can be damaged. This can result in product loss or damage.	Cascading failure	(Tang, Jing, He, & Stanley, H. E. (2016)
Supply chain (stuxnet)	Sensitive intelligence of manufacturers subcontractors becomes available for hackers to understand their system specifications better, increasing their vulnerability to attacks.	Finding out who the subcontractors are in a supply chain to then find vulnerabilities on a target.	Cyber espionage, Spyware, Data theft	(Friedman, Mack-Crane, & Hammond, 2013)

Final Thoughts

In the year 2020, many attacks have occurred with those targeting critical infrastructure, governments, and corporations. These attacks have used many tactics that include exploiting the supply chain by uncovering the suppliers who have allowed them to enter multiple organizations to gain access to critical information providing them unlimited data to analyze for the future at the highest levels. This unprecedented year yet shows why cybersecurity further needs an elevated status within the United States Government. This final section reviews some of the largest attacks and what is to be learned from the attack.

Cybersecurity originally has been part of the US federal government to protect mission-critical systems. The civilian sector did not consider the need nor importance of having compliance with a cybersecurity framework or implementing basic cybersecurity controls. Until the early 2000s, organizations slowly started to have data breached, and nation-states saw this as a domain for warfare. This changed the landscape for cybersecurity and, ultimately, created the new superpowers in this domain. One of the challenges globally was talent, where to find it, how to develop it, and how to recruit it. This meant that the talent had to be first a citizen and second loyal to the country for militaries. To make matters more complicated in countries such as Saudi Arabia (KSA), military officers need to be at least third-generation Saudi. This rule, in itself, makes it difficult as a significant number of tech talent are ex-pats. The number of attacks within the Middle East and the African region was high in recent years, with approximately 94% of companies being victims of cyber attacks in 2017 (Cisco, 2018).

In many other countries, matters are a bit more complicated. This ranges from a lack of a national cybersecurity policy, poorly defined digital borders, and a nonexistent national cybersecurity policy (Goel, 2020; Senol, M., & Karacuha, 2020). These items have created wide gaps that have allowed hackers to circumvent not only authorities but to take advantage of the

non-implementation of cybersecurity policies, procedures, and technologies that would serve as deterrents.

COVID-19

COVID 19 has provided innumerable opportunities for those looking for easy opportunities in 2020 (Lallie et al. l., 2020). With the rush to comply with global stay-at-home orders and curfews, organizations were not prepared to support a mass amount of employees working virtually to curve the rising numbers of daily cases (Xu et al. l., 2020). This meant that organizations didn't have healthy authentication controls, cloud data encryption, and removal of dead code or backdoors. This created an opportunity for those looking to control user accounts, employee, and customer data.

For the individual, the security of home networks were tested (Security Magazine, 2020). The hyperconnectivity concept proved to be a real one in were home networks had many devices on the same network without proper security mechanisms in place home networks thus became a target. However, due to this increase in targeted attacks, several corporate guidance and policy were developed due to teleworking (Abukari & Bankas, 2020). In previous years, televised examples were attackers taken advantage of baby monitors, and now it has elevated to home security systems (Stanislav & Beardsley, 2015). The same computing system to provide surveillance to the home now was given a nefarious actor insight into the residence's activity.

Election

In the 2016 election, it was determined that Russia was behind the Information Operations (IO), and active measures were successfully carried out in favor of Donald J. Trump. This was a coordinated event where fake profiles were created to influence thought and provoke a pre-existing bias in American society (Shane, 2017). In the recent election, it was determined that the new troll farm was in Ghana and Nigeria targeting African Americans, creating racial discord using current issues such as police brutality (Ward, Polglase, Shukla, Mezzofiore, & Lister, 2020). This is a variation of Internet-enabled psychological warfare, which is targeted at specific populations to motivate them to do a task of their choosing. This new use of cyberattacks mixed with a form of intelligence created shockwaves in the cyber community. The other item was the weaponization of data and how Facebook allowed this to occur, resulting in a colossal mistrust of users' privacy (Isaak & Hanna, 2018). This action showed just how robust data could influence others and uncover links that affect individuals' decisions to move them to specific activities.

Supply Chain

Towards the last quarter of 2020, it was determined by multiple agencies that Russia was responsible for the SolarWinds hack (Barrett, 2020). This has been one of the largest and significant hacks in years as it shows the issues with the software supply chain. As the organization responsible for the final delivery of the product has security mechanisms in place, the same cannot be said for those in the supply chain. Thus, targeting those in the supply chain, a higher chance of success is attained. For professional certifications that address this, there are not many. One well-known certification that has a specific domain dedicated to this is the Certified Secure Software Lifecycle Professional (CSSLP) from (ISC)2 (Paul, 2016). Russia

performed what is known as a supply chain attack meaning that they comprised a trusted tool rather than a direct attack such as exploiting an identified CWE that could have been identified through a static or dynamic code analysis (Barrett, 2020). This highlighted the known issues that can be used to develop targeted attacks and sneak in compromised code. However, if one were to look at Flame and Stuxnet's problems where a Programmable Logic Controller (PLC) was targeted among other industrial controls through a similar attack, this was expected to be a strategic method to exploit systems in the future.

Final Remarks

With the ever-growing number of attacks, people and organizations must develop a **cybersecurity ecosystem**. This ecosystem needs to include three things such as **technology, policy, and education**. This ecosystem needs to be evaluated annually to ensure that it is incorporating the latest items that affect its overall security posture. It is vital for those requiring harsh measures to understand those three items within the Mission Framework as a starting point to reference an attack and develop a threat landscape that allows for a successful attack.

Ongoing challenges as the ones placed by the pandemic event and the need to go with the full spectrum of both defensive and offensive cybersecurity education, **demands for more people talent to be developed**.

References

Ablon, L. (2018, March 15). A Close Look at Data Thieves. Retrieved September 23, 2020, from https://www.rand.org/pubs/testimonies/CT490.html

Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research*, 11(4), 1401-1407.

Alhazmi, O. H., Malaiya, Y. K., & Ray, I. (2007). Measuring, analyzing and predicting security vulnerabilities in software systems. *computers & security*, *26*(3), 219-228.

Ambrose, J. (2018, April 23). Half of UK manufacturers fall victim to cyber attacks. Retrieved June 4, 2020, from https://www.telegraph.co.uk/business/2018/04/22/half-uk-manufacturers-fallvictim-cyber-attacks/

Arreguin-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International security*, *26*(1), 93-128.

Ayalew, Y. E. (2019). The Internet shutdown muzzle (s) freedom of expression in Ethiopia: competing narratives. *Information & Communications Technology Law*, *28*(2), 208-224.

Baker, M. (2013). State of cyber workforce development. *Software Engineering Institute, Carnegie Mellon University*.

Barrett, B. (2020, December 20). Russia's SolarWinds Hack Is a Historic Mess. Retrieved December 27, 2020, from https://www.wired.com/story/russia-solarwinds-hack-roundup/

Bartles, C., Tormey, T., & Hendrickson, J. (2017, March/April). Multidomain Operations and Close Air Support: A Fresh Perspective. Retrieved December 02, 2020, from https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2017/ART-011/

Bazzell, M. (2016). *Open source intelligence techniques: resources for searching and analyzing online information*. CreateSpace Independent Publishing Platform.

BBC. (2020, December 15). SolarWinds Orion: More US government agencies hacked. Retrieved December 23, 2020, from https://www.bbc.com/news/technology-55318815

Beggs, R. W. (2014). *Mastering Kali Linux for advanced penetration testing*. Packt Publishing Ltd.

Bruneau, E., & Kteily, N. (2017). The enemy as animal: Symmetric dehumanization during asymmetric warfare. *PloS one*, *12*(7), e0181422.

Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal*, 441-472.

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Cielen, D., Meysman, A., & Ali, M. (2016). *Introducing data science: big data, machine learning, and more, using Python tools*. Manning Publications Co.

Cisco. (2018, May 24). Cyber security threat and protection report 2018 – Cisco

Middle East and Africa. Retrieved October 1, 2020, from https://www.cisco.com/c/m/en_qa/campaigns/security/cyber-threats-and-protection-2018-report/index.html

Clark, M. (2020, December 21). Big tech companies including Intel, Nvidia, and Cisco were all infected during the SolarWinds hack. Retrieved December 22, 2020, from https://www.theverge.com/2020/12/21/22194183/intel-nvidia-cisco-government-infected-solarwinds-hack

Committee to Protect Journalists. (2020, July 02). 10 Most Censored Countries. Retrieved September 12, 2020, from https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/

Cunningham, S., & Kendall, T. D. (2011). Prostitution 2.0: The changing face of sex work. *Journal of Urban Economics*, 69(3), 273-287.

CyberSeek. (n.d.). Cybersecurity Supply And Demand Heat Map. Retrieved March 15, 2020, from https://www.cyberseek.org/heatmap.html

Davey, J., & Armstrong, H. L. (2001). An Approach to Teaching Cyber Warfare Tools and Techniques. *Journal of Information Warfare*, *1*(2), 87-94.

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*, 35(2), 60-67.

Dawson, M. (2018). Cyber security in industry 4.0: The pitfalls of having hyperconnected systems. J*ournal of Strategic Management Studies*, 10(1), 19-28.

Dawson, M., Eltayeb, M., & Omar, M. (Eds.). (2016). *Security solutions for hyperconnectivity and the Internet of things*. IGI Global.

Dawson, M., & Omar, M. (2015). New Threats and Countermeasures in Digital Crime and Cyber Terrorism (pp. 1-368). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7

Dawson, M., Wang, P., & Williams, K. (2018). The role of cae-cde in cybersecurity education for workforce development. In *Information Technology-New Generations* (pp. 127-132). Springer, Cham.

Deibert, R. J. (2009). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. *Routledge handbook of Internet politics*, 323-336.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?. *The Review of Financial Studies*, *32*(5), 1798-1853.

Gartner. (2018, October 16). Gartner Survey of More Than 3,000 CIOs Reveals That Enterprises Are Entering the Third Era of IT. Retrieved February 5, 2020, from https://www.gartner.com/en/newsroom/press-releases/2018-10-16-gartner-survey-of-more-than-3000-cios-reveals-that-enterprises-are-entering-the-third-era-of-it

Gikas, C. (2010). A general comparison of fisma, hipaa, iso 27000 and pci-dss standards. *Information Security Journal: A Global Perspective*, 19(3), 132-141.

Gill, A. S. (2019). Artificial intelligence and international security: the long view. Ethics & *International Affairs*, 33(2), 169-179.

Goasduff, L. (2019, September 12). Top Trends on the Gartner Hype Cycle for Artificial Intelligence, 2019. Retrieved March 15, 2020, from https://www.gartner.com/smarterwithgartner/top-trends-on-the-gartner-hype-cycle-for-artificial-intelligence-2019/

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. Connections: The *Quarterly Journal*, 19(1), 73-86.

Greenwood, F. (2013, January 28). Internet access is "essential" human right, rules German court. Retrieved September 12, 2020, from https://www.pri.org/stories/2013-01-28/internet-access-essential-human-right-rules-german-court

Helms, C. P. (2015). *The Digital GCC: USCYBERCOM As a Combatant Command*. Air Command And Staff College Maxwell Air Force Base United States.

Hemmingson, M. (2008). Cyber-hookers aka providers: Off the street and onto Craigslist. Available at SSRN 1084415.

Hollis, D. M. (2010). *USCYBERCOM: The need for a combatant command versus a subunified command*. NATIONAL DEFENSE UNIV WASHINGTON DC.

Hu, J., Cordel, D., & Meinel, C. (2004, October). A Virtual Laboratory for IT Security Education. In *EMISA* (Vol. 56, pp. 60-71).

IEEE. (2020, June 4). How COVID-19 is Affecting Industry 4.0 and Innovation. Retrieved June 8, 2020, from https://transmitter.ieee.org/how-covid-19-is-affecting-industry-4-0-and-the-future-of-innovation/

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51(8), 56-59.

Jamieson, K. H. (2020). *Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know*. Oxford University Press.

Johnson, D. E. (2019). Russian Election Interference and Race-Baiting. *Colum. J. Race & L.*, *9*, 191.

Kim, E., Wells Jr, W. G., & Duffey, M. R. (2003). A model for effective implementation of Earned Value Management methodology. *International Journal of Project Management*, *21*(5), 375-382.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*.

Lee, J., Davari, H., Singh, J., & Pandhare, V. (2018). Industrial Artificial Intelligence for industry 4.0-based manufacturing systems. *Manufacturing letters,* 18, 20-23.

Lee, K. (2016). Artificial intelligence, automation, and the economy, The White. *House Blog.*

Lewis, B. K. (2012). *Social Media and Strategic Communications: Attitudes and perceptions Among College Students* (Doctoral Dissertation). Available from ProQuest Dissertations and Thesis Full Texts Database. Oklahoma State University. Retrieved September 13, 2020, from http://www.prsa.org/Intelligence/PRJournal/Documents/2012LewisNichols.pdf

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society*, *19*(1), 111-126.

Martínez, F. G. (2019a). *Special Problems in Information Security: From Privacy to Emerging Technologies for Hyperconnected Systems.* (Master's thesis, Universidad Politécnica de Madrid, 2019) (pp. 1-49). Madrid: Universidad Politécnica de Madrid.

Martínez, F. G. (2019b). Analysis of the US Privacy Model: Implications of the GDPR in the US. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, *3*(1), 43-52.

Martinez, F. G., & Dawson, M. (2019). Unprotected Data: Review of Internet Enabled Psychological and Information Warfare. *Land Forces Academy Review*, *24*(3), 187-198.

Minsky, M. L. (1982). Why people think computers can't. *AI magazine*, 3(4), 3-3.

Muncaster, P. (2020, April 1). Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites. Retrieved June 5, 2020, from https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/

Murtaza, S. S., Khreich, W., Hamou-Lhadj, A., & Bener, A. B. (2016). Mining trends and patterns of software vulnerabilities. Journal of Systems and Software, 117, 218-228.

Najera-Gutierrez, G., & Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication*, *800*, 181.

Paul, M. (2015). *Official (ISC) 2 Guide to the CSSLP*. CRC Press.

Pinzone, M., Fantini, P., Perini, S., Garavaglia, S., Taisch, M., & Miragliotta, G. (2017, September). Jobs and skills in Industry 4.0: An exploratory research. In *IFIP International Conference on Advances in Production Management Systems* (pp. 282-288). Springer, Cham.

Polyakova, A. (2019, October 25). Weapons of the weak: Russia and AI-driven asymmetric warfare. Retrieved June 7, 2020, from https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

Portnoff, R. S., Huang, D. Y., Doerfler, P., Afroz, S., & McCoy, D. (2017, August). Backpage and bitcoin: Uncovering human traffickers. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1595-1604).

Potter, B., & McGraw, G. (2004). Software security testing. *IEEE Security & Privacy*, *2*(5), 81-85.

Ranasinghe, N., Karunanayaka, K., Cheok, A. D., Fernando, O. N. N., Nii, H., & Gopalakrishnakone, P. (2011, November). Digital taste and smell communication. In *Proceedings of the 6th international conference on body area networks* (pp. 78-84). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Reglitz, M. (2020). The Human Right to Free Internet Access. *Journal of Applied Philosophy*, *37*(2), 314-331.

Robles, R. J., Choi, M. K., Cho, E. S., Kim, S. S., Park, G., & Lee, J. (2008). Common threats

and vulnerabilities of critical infrastructures. International journal of control and automation, 1(1), 17-22.

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, 11(4), 3-4.

Security Magazine. (2020, November 30). Consumers underestimate how often their networks are targeted by threat actors. Retrieved December 27, 2020, from https://www.securitymagazine.com/articles/94042-consumers-underestimate-how-often-their-networks-are-targeted-by-threat-actors

Senol, M., & Karacuha, E. (2020). Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering*.

Shane, S. (2017). The fake Americans Russia created to influence the election. *The New York Times*, 7(09).

Sinha, S. (2017). Dark Web and Tor. In *Beginning Ethical Hacking with Python* (pp. 173-177). Apress, Berkeley, CA.

Spalevic, Z., & Ilic, M. (2017). The use of dark web for the purpose of illegal activity spreading. Ekonomika, *Journal for Economic Theory and Practice and Social Issues*, 63(1350-2019-2771), 73-82.

Stack, B. (2019, March 11). Here's How Much Your Personal Information Is Selling for on the Dark Web. Retrieved October 1, 2020, from https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

Stanislav, M., & Beardsley, T. (2015). Hacking iot: A case study on baby monitor exposures and vulnerabilities. *Rapid7 Report*.

Stewart, J., & Dawson, M. (2018). How the modification of personality traits leave one vulnerable to manipulation in social engineering. *International Journal of Information Privacy, Security and Integrity*, *3*(3), 187-208.

Timchenko, M., & Starobinski, D. (2015, February). A simple laboratory environment for real-world offensive security education. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (pp. 657-662)

Trump, D. J. (2019). Executive order on maintaining American leadership in artificial intelligence. *Federal Register: White House*, 3967-72.

Tzu, S. (2014). The art of war. In *Strategic Studies* (pp. 86-110). Routledge.

U.S. Bureau of Economic Analysis (2020). *Interactive Access to Industry Economic Accounts Data: GDP by Industry*. Retried from https://apps.bea.gov/iTable/iTable.cfm?reqid=51&step=1#reqid=51&step=1

U.S. Cybercom. (n.d.). Command History. Retrieved December 22, 2019, from https://www.cybercom.mil/About/History/.

Umble, E. J., Haft, R. R., & Umble, M. M. (2003). Enterprise resource planning: Implementation procedures and critical success factors. *European journal of operational research*, 146(2), 241-257.

Vijayan, J. (2009, June 23). Defense Secretary Gates approves creation of U.S. Cyber Command. Retrieved December 22, 2019, from https://www.computerworld.com/article/2525896/defense-secretary-gates-approves-creation-of-u-s--cyber-command.html.

Walther, G. (2015). Printing insecurity? The security implications of 3d-printing of weapons. *Science and engineering ethics*, *21*(6), 1435-1445.

Wang, M., Callaghan, V., Bernhardt, J., White, K., & Peña-Rios, A. (2018). Augmented reality in education and training: pedagogical approaches and illustrative case studies. *Journal of Ambient Intelligence and Humanized Computing*, 9(5), 1391-1402.

Wang, P., Dawson, M., & Williams, K. L. (2019). Improving cyber defense education through national standard alignment: case studies. In *National Security: Breakthroughs in Research and Practice* (pp. 78-91). IGI Global.

Ward, C., Polglase, K., Shukla, S., Mezzofiore, G., & Lister, T. (2020, April 11). How Russian meddling is back before 2020 vote. Retrieved December 27, 2020, from https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html

White House. (2016a). *Artificial Intelligence, Automation, and the Economy*. Executive Office of the President. Retrieved from

https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF

White House. (2016b). *Preparing for the future of Artificial Intelligence*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

WHO. (2020, April 23). WHO reports fivefold increase in cyber attacks, urges vigilance. Retrieved from https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

Wikipedia. (2018, June 19). Industry 4.0. Retrieved May 17, 2020, from https://en.wikipedia.org/wiki/Industry_4.0

Wilson, C. (2014). Cyber Threats to Critical Information Infrastructure. Cyberterrorism,

123-136.

Wolfson, R. (2018, December 15). Tracing Illegal Activity Through The Bitcoin Blockchain To Combat Cryptocurrency-Related Crimes. Retrieved September 12, 2020, from https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/

Wong, E. (2005). Swift Road for US Citizen Soldiers Already Fighting in Iraq. *New York Times*, *9*.

Xu, J., Hussain, S., Lu, G., Zheng, K., Wei, S., Bao, W., & Zhang, L. (2020). Associations of stay-at-home order and face-masking recommendation with trends in daily new cases and deaths of laboratory-confirmed COVID-19 in the United States. *Exploratory research and hypothesis in medicine*, 1.