The Glowing Capitol

Capitol Reflections

Ryan Barron

December 4, 2018

Table of Contents

1. Introduction

Inevitably, and thankfully, society moves forward. Such societal progress is nuanced to the times and culture, but more often, it is defined by the technology we use to change daily life operations. Government, at the very core, is no different. As the world continues to grow smaller through the interconnectedness of ideas, institutions producing and protecting those ideas play a decisive role in the international dominance of United States institutions. At the very least, technology will advance the U.S. into a more perfect union. As government is at the core of societal decisions, computer science is at the core of technological development.

The United States Government is responsible for monitoring and protecting technological developments. Therefore, I chose to pursue an internship in the United States House of Representatives with Congressman Dutch Ruppersberger, which began in August 2018. My internship with the House of Representatives was most concerned with computer applications and the impact of computers on society. House Bill 2305 from the 115th House of Representatives defines Computer Science as "the study of computers and algorithmic processes and includes the study of computing principles, computer hardware and software design, computer applications, and the impact of computers on society." In this paper, I describe what it's like to work in the United States Congress, the general approach Congress displays towards the future of computing, and how my education and the lessons I've learned in Congress have prepared me for my future.

1.1 115th House of Representatives

The 115th Congressional Session began in January 2017 and ended in December 2018. There are two houses in the United States Congress: The Senate and the House of Representatives. The upper house, commonly known as the Senate, has one hundred members, with two Senators per state. The lower house, the United States House of Representatives, has four hundred thirty-five members portioned by population—with the average constituent population averaging one representative for every seven hundred thousand people.

1.2 Learning Objectives

There is so much to experience in the Capitol that it was important to specify my learning objectives in order to maintain an appropriate level of focus and maximize my limited time there. At the beginning of my internship, I created these initial objectives:

1. Translate subcommittee hearings & briefs about technology into written colloquial language.
2. Compare technological integration across multiple federal agencies.
3. Examine legislation directly influencing Computer Science careers.
4. Discuss technological changes in the congressional district.
5. Predict the impact of Artificial Intelligence (AI) on a Federal level.

Through these objectives, I acquired skills in how to seek information about Congressional topics, which is especially useful for computer science topics. I also learned that the race to develop technological dominance and the ability to compete with other nations can be likened to the space race to the moon in 1959. Additionally, I learned how defense agencies work together to pass information relevant to technological support, which develops a working defense network.

Like the competencies above, I learned that AI is broken into two distinct topics: narrow and general. The government mostly has a grasp on narrow artificial intelligence, which is focused on performing a specific task. As it develops its technological capabilities, it will seek to grow its general intelligence capabilities, which learn all skills generally. In a seemingly counter-intuitive move, the federal government has broken the leadership of cyber into multiple “silos,” meaning the agencies don’t communicate with each other. The separation often works to the government's consternation because relevant information may not flow to agencies that would find the information useful. We are trailing compared to some United States rivals since many eastern countries have a single head to their cyber and information warfare strategies. Such reasoning reveals hearings, such as the Interagency Cyber Cooperation enumerated in the projects below, are necessary and prudent for national security.

2. Internship

I worked in the DC office on Mondays and Wednesdays in the Rayburn House Office building. Many of the projects I was able to work on were associated with the level of trust the office felt I merited and my ability to communicate my desire to on specific topics. Since I was a trusted intern and frequently asked, I could work on tasks particular to my interest in computer science.

2.1 Employer

I interned in the office of Congressman Dutch Ruppersberger, the representative over the second Maryland Congressional district, ranging from Owings Mills over to Aberdeen Proving Grounds, then down to Ft. Mead. Congressman Ruppersberger is a member of the appropriations committee, which writes the laws that fund the federal government and the Defense and the State, Foreign Operations, and Related Programs subcommittees. He is known for his stances on education, infrastructure, and our nation's security. Although I was an intern of Congressman Ruppersberger, my direct supervisor was Victoria Graham, the digital assistant and a staff assistant.

2.2 Job Description

The level of trust between an intern and his/her supervisor greatly affects the given responsibilities. The initial tasks for interns who had yet to earn any responsibilities were answering phone calls from constituents, checking the printers, and other similar office tasks. As trust grew and skillsets were shown, I was granted the ability to write mail in response to correspondence and deliver high-value documents. As trust continued to grow, I was able to attend hearings and briefings throughout the Capitol's campus, summarize works regarding legislative issues the staff members are assigned for the Congressman, or even guide constituent guests around the Capitol. On the highest levels of trust, an intern may deliver documents to the congress member on the house floor.

2.3 Projects

As a computer science major aiming to acquire greater knowledge in my area of study at the federal level, I requested work briefs, interviews, and networking opportunities that would allow me to gain a firmer grasp on the potential uses of computer science in the political field. The hearings and briefs allowed me to research topics like the Department of Homeland Security's Hacking team and a new security plan for the Internal Revenue Service (IRS) internet interactions. Often, the staff members regarding military and cyber had projects for me in accordance with my requests. Briefs and hearings I worked on for the office included:

1. Online Taxpayer Authentication: Ways and Means Committee
2. Russian Information Warfare- Implications for Defense Theory: Strategic Studies Quarterly of the United States Air Force
3. Implementation of Positive Train Control: Committee on Commerce, Science, and Transportation
4. Countering Iranian Proxies in Iraq: Foreign Affairs Committee
5. Consumer Data Privacy: Committee on Commerce, Science, and Transportation
6. End World Hunger by 2030: Food and Agriculture Organization of the United Nations (U.N.)
7. Nominations for District Courts in Florida and Alabama: Judiciary Committee
8. Carbon Capture Technology: Coal and Steel Industry
9. Hack the Staff: Department of Homeland Security's Red Team
10. Semi-Annual Testimony on the Federal Reserve's Supervision and Regulation of the Financial System: Financial Services Committee
11. Interagency Cyber Cooperation: Roles, Responsibilities, and Authorities of The Department of Defense (DoD) & The Department of Homeland Security: Joint Hearing from Committees of Armed Services and Homeland Security

In this paper, I do not elaborate on all topics previously listed, rather, I focus on those with the greatest potential impact on the future applications of computers and how computers will impact our

society. It's worth noting that number six, Ending World Hunger by 2030, is one of the topics not explained in this paper, but in the brief, it was said that the best improvement to feeding people was due to technological advances. Additionally, number four, Countering Iranian Proxies in Iraq, mentioned that intelligence gathering is the single largest issue in responding appropriately to issues arising, which could have been resolved with intelligence gathering technology.

2.4 Mentors & Office Relationships

I worked in an office that was very friendly and acted more like family to each other than office associates. My interactions with my mentor and everyone in the office were always positive and supportive. Throughout the internship, the interactions provided opportunities to participate in discussions about the impact of technology on the district.

3. District Discussions & Technology

Throughout my time with Congressman Ruppersberger's office, I was able to engage in conversations with staff members and office visitors about the impact of computational programs/issues on our district, Maryland's District Two, or the country itself. Topics discussed include: implementing 5G networks, incorporating Cloud networks in the Department of Defense, and even using the office's Internet Quorum program. The topics discussed directly fulfill Learning Objective Four, "to discuss technological changes in the congressional district."

3.1 Implementing 5G networks

A goal of Congressman Ruppersberger's office was to implement 5G internet, 5G standing for 5th Generation, megabits and meaning an enhanced internet experience. The current standard for the internet is 4G, which has download speeds of five to twelve megabits per second and uploads from two to five megabits per second. The transition to 5G networks would allow for speeds to average at ten gigabits per second (Moore) in downloads, which is ten thousand megabits per second, and about many times the current capable speeds. This improvement can potentially increase the quality of life through increased communication speeds by allowing large quantities of important information to be shared faster.

While there are clear benefits for the next generation of internet speeds, opposition slows the implementation progress. For instance, some people believe it is bad for the health of their children to walk into the beams of the technology, believing it will cause cancer. Such beliefs cause movements to try to distance technology from school buildings. Additionally, this work requires a new infrastructure to be built in order for areas of interest to be properly covered. These constructs cause people to complain about them being eye sores or degrading to the neighborhoods.

3.2. Cloud Networks for the DoD

Cloud networks are designed to make computers more manageable, increasing business efficiency and process. The DoD is scheduled to award the Joint Enterprise Defense Infrastructure (JEDI) contract of ten billion dollars for cloud networks in the military to increase speed and manageability. There is some dissatisfaction amongst different parts of the technology world that see the contract unfairly favoring Amazon (Miller). However, if spread evenly, the contract is spread over ten years, which amounts to a billion dollars a year. In contrast, the cloud market is expected to reach a value of one hundred billion dollars a year.

3.3. Lockheed Martin's Intranet Quorum

When I saw Intranet Quorum open and then display the Lockheed Martin logo, I was surprised. Later, I discovered that Leidos owns the program, and they own Lockheed Martin. Leidos claims the program to be in use by "65% of U.S. Congress" (Leidos). This program is effective for logging and speeding up communication for the district, but it isn't as user-friendly as expected, as it feels like a program from the 2000s. It allows for phone calls, physical mail, faxes, and emails to be received and sorted by category, and even similarity, meaning if twenty similar emails come into the office's server, they can all be sorted at once for a subsequent letter response, or the appropriate action requested.

4. Projects: Hearings & Briefings

Throughout my internship I was given projects to work on that informed my office about what the rest of Congress was deliberating on. My projects took the form of attending hearings, briefings and compiling their summaries. Many of the topics I covered directly related to the security of computers, implementing better policies or procedures, or accommodating and influencing developing technologies.

4.1 Internal Revenue Service- Securing communication over the Internet

The IRS recently developed issues with stolen data and false claims for returns through identity theft. In order to combat this crime, the IRS has set out to follow the 2017 National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-63-3, the Digital Identity Guidelines. Three major concerns included authentication, proving correct user connection to access the information process—identity proofing- and communicating with other agencies for help.

4.1.1. *Authentication*

A legitimate connection must be secure from outside manipulation, deemed authentication. The IRS found this issue easier to fix and believed blockchain is the best solution. However, the IRS also stated there was a general misunderstanding that the blockchain doesn't solve all the problems of secure communication, just the authentication question.

4.1.2. Identification Proofing

After a secure connection is made, there is no guarantee the users will be who they identify as when they connect, and protecting this is known as identity proofing. For instance, a connection could be made from stolen social security numbers and birth information. This is the area the IRS is having the most difficulty with, and is seeking other agencies' help most fervently. The favored solution is facial recognition as a form of multifactor biometric authentication. This is similar to the authentication step and used to be part of authentication until NIST deliberately distinguished authentication from Identity Proofing in SP 800-63-3.

4.1.3 Inter-Agency Cooperation

The two main agencies the IRS communicated with included the Social Security Administration (SSA) and the General Services Administration (GSA). There were inquiries about reaching out to other countries for help, such as Britain, to learn how they secure their financial sector. This relates to my second learning objective, which is to compare technological integration across multiple agencies.

4.2 Russian Information Warfare Summary

I was tasked by the military staff assistant to discover the main ideas of Russian Information Warfare in *Strategic Studies Quarterly*, a book written by Ajir and Vailliant and published by the American Air Force. The Russians see the information war as self-defense, protection from outside negative images. They seek to rot nations from the inside out by breaking down societal cohesion.

4.2.1 Methods

Strategic Studies Quarterly indicated several shocking statistics showing Russian interference's value in other nations. The annual estimated budget dedicated to misinformation is three to four billion dollars. The funds buy around fifteen thousand employees, known as the Kremlin troll army, with the expectation that they will maintain six Facebook accounts, and ten Twitter accounts, to produce fifty tweets a day and fifty articles. All the troll army postings are required to contain misinformation in order to guide other countries' populations to thought processes that benefit Russia. Additionally, Western media newspapers have been tools for use in their designs, exclaiming fabricated information as if from a second or third source to make it seem more credible. Another avenue for spreading Russian intentions to the west is by legislators, as the Russians lobby Congressional offices. For instance, Henry Kissinger owns Kissinger Associates, which has aided Russian agendas as a lobbyist to Congress.

4.2.2 Implications

With so much force going into misinformation, the Russians cause countries to deteriorate from the inside out. It benefits Russia to have weak neighbors, as countries in turmoil are less likely to attack or compete in trade. Strategic Studies Quarterly, printed by the Air Force, suggests breaking information

warfare into two categories with common areas: a cyber domain and a psychological domain. Two domains allow for tailored and specific responses to attacks since American teams will train specifically for each threat in their respective domain.

4.2 Consumer Data Privacy

In September, the Senate had many large tech companies, such as Facebook, Twitter, Google, and Netflix, testify about how they use consumer data, and give recommendations for federal legislation. The regulations will aim to protect consumers and their data rights.

In further investigations, Congress held a second hearing in October to discover perspectives from regulators in the field, including The U.N., the promulgator of California's Data Privacy ballot initiative, an executive professor from the Georgetown Law Center on Privacy & Technology, etc.

4.2.1 Influences

The U.N. has passed consumer protection directives over the last two decades that failed since no one listened. As a result, they developed a full European board that binds all the nation-states under one guideline instead of forcing companies to abide by twenty-eight different laws. The board acts as an arbitrator when countries have disputes about who should investigate companies.

A second regulator perspective is from the organizers of California's data protection ballot initiative, forcing technology companies in Silicon Valley to abide by strict rules. In the September hearing, companies asked Congress to make a uniform law to supersede state legislation, hoping that federal law would be more relaxed than California's. However, suppose Silicon Valley could get California's data privacy law to relax. In that case, they would no longer want federal oversight to be able to continue data manipulation as they please in other states.

4.3.2 Suggestions to Congress

The main witnesses' suggestions for Congress were:

1. Agree that consumer data should not be used to discriminate against consumers.

2. Information should not be used to amplify hate speech, with robust enforcement methods through fines and warnings. Company fines should be proportionate to their revenue.
3. Consumers should have the right of action to determine what happens to their data when companies wish to sell, move, delete, or correct consumer data.
4. The law Congress makes to protect consumers' online data should have a mechanism to allow it to keep up with changing technology and be a privacy floor, not a ceiling.
5. Create an agency, like the Federal Trade Commission, invested with the ability to 1) create rules and 2) enforce the rules. State attorney generals should have the authority to enforce the agency rules.
6. Limiting the type of data companies can collect and, correspondingly, shortening the permitted time for data retention can limit the extent of breaches.

Finally, it was mentioned that computer scientists want a rule to follow in original designs rather than learning of requirements ex post facto, where they must recode for missing parts.

4.4 Hack The Staff

The Department of Homeland Security (DHS) has a penetration testing team, commonly called a red team. This means their job is to hack federal systems to determine vulnerabilities ethically. The DHS red team is responsible for testing all federal agencies aside from the Department of Defense, which the National Security Agency (NSA) tests. The DHS Red team also takes on private company contracts to check for their vulnerabilities. Issues discovered are communicated in a report given to the agency under scrutiny at the end of the testing period. The report includes how to fix the issues discovered in the scope or the legal bounds for the number of computers tested, as well as which parts of the networks were attacked. The red team mentioned that all the information they tested was open-sourced but claimed that the test results had non-disclosure agreements to protect the agencies from public exploitation.

In the team’s testing, they create an average of twenty virtual servers to maintain steady and consistent communication with the test’s artificial victims. All built infrastructure is torn down at the end

of the scope period, which is challenging to rebuild, should one of the clients request additional tests. Ninety days is the average hacking time period, but the team regularly maintains four simultaneous operations. The team stated they are non-operational five weeks out of the year, known as blackout periods, for mandatory technology upgrades.

The DHS Red team didn't exist in 2010. They had no computers or location from which they could operate but have developed nine hundred stakeholders since. Additionally, when tests were first conducted, agencies were slow to respond, regularly waiting two hundred seventy days before implementing a fix. The red team developed binding operational directives, which force the agencies under consideration to fix issues within thirty days, reducing the average fix time to seventeen days. The team's recent focus is working on the nation's voting systems to discover weaknesses in the firmware. The type of machine under their examination is used for seventy percent of the nation's voting process.

4.4.1 Methods & Suggestions

During actual tests, the DHS testers usually go for phishing attacks, as they're the easiest and fastest way into networks. Even cloud networks have very strong perimeters, but if someone has access to the inside of a cloud service, they can be used as a pivot point by the DHS team to gain further access inside. While the DHS doesn't test cloud networks, breaches in normal computer networks operate similarly.

The phishing targets are usually people who must interact with the public by the nature of their job, such as a press secretary. The hackers send multiple emails, pretending to be someone whom the press secretary would normally interact with, and then send their payload near the seventh email, which is the program that allows the team to have remote access to the computer and network. From the callback functions available on the payload, the user's files can be accessed, privilege can be escalated to the administrator, keyloggers can be deployed to capture keyboard strokes, or the network itself can be traversed by pivoting on several computers.

Throughout the test, the next attack action is determined by how discrete it will be to monitoring systems and people that should be alerted, including firewalls, antivirus programs, and network

administrators. This checks the effectiveness of the set trigger thresholds if they even exist. The red team considers ransomware the most pronounced activity on a network and is faked, but no data is encrypted. However, some files are prevented from opening easily, and messages are delivered to the user as if the system were encrypted.

The DHS operation is data-driven. They claim to have an eighteen percent click rate in their phishing attempts, although when the Ashley-Madison dating site was used, there was a ninety-three percent click rate. When one payload delivery method fails, other methods for delivering the same program can be used, which means two-factor authentication is not obstructive to the red team's objectives. They have tested election machines in forty-three states and found consistent vulnerabilities throughout. The DHS has no mobile device testing capability, but they are considering its development. The DHS has classified vulnerability equity process meetings, where technologies' trends and futures are discussed to determine testing priorities.

The team stated information is informally shared between agencies via platforms like conventions. They consider the offensive security community small, and therefore people from different agencies often attend similar conventions, which is how the information is exchanged. However, the eleventh hearing from the DHS and DOD, Interagency Cyber Cooperation, proved otherwise. This shed light on my two learning objectives: to compare technological integration across multiple federal agencies.

The DHS believes the end of fishing emails in the government can be attained through *Domain-based Message Authentication, Reporting & Conformance* (DMARC), and *Sender Policy Framework* (SPF). Both of these are email validation protocols to test the source server of emails in Domain Name Service records.

Finally, the hacking team stated understaffing is an issue due to the pay rates of new hires compared to private industry, as well as other agencies, such as the NSA. The DHS can hire people at the e7 rate (equivalent to a Sergeant First Class), but other agencies can hire at e9 (Sergeant Major). Additionally, security clearances make the process longer than people are willing to wait. The DHS offers

“Scholarship for Service,” where a candidate's degree is paid off if he/she enters a contract with the DHS red team to work for a period equivalent to the length of the scholarship.

5. Legislation

All legislation resets at the end of a congressional session. This means an act, a bill that has passed one of the two houses, or a bill, a document introduced to the first house, must be passed into law before the end of the two years of a session. In this case, the 115th session ends December 13th, 2018, and the 116th session starts January 3rd, 2018. Congressman Ruppersberger was reelected to the 116th session.

5.1 Law: Bills That Passed Both Chambers

The following four bills have passed both houses and become law. (If they have an S in front, they originated in the Senate, and if they have an H.R. in front, they originated in the House of Representatives.)

The first bill, S.770 – The National Institute of Standards and Technology (NIST) Small Business Cybersecurity Act. In the law, the focus is to produce NIST guidance on cybersecurity topics for small businesses, including an awareness and education program, a strategy itself, public availability through normal technology, and adequate funding to produce results.

The next bill is S.782 - PROTECT Our Children Act. This law is designed to reauthorize the National Internet Crimes Against Children Task Force Program, focusing on "providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2017" (Congress.gov), until 2022. With more resources going into regulating how children interact with the internet, they will be less likely to be harmed by malicious actors.

Third, H.R.5515 - John McCain National Defense Authorization Act for Fiscal Yr. 2019, is about Department of Defense funding and artificial intelligence. There are two sections on AI(AI), Title 2, subtitle B, section 238, on joint AI research, development, and transition activities, as well as Title 10, subtitle D, section 1051, on the National Security Commission on AI

Title 2, subtitle B, section 238, is mostly focused on developing autonomous and intelligent systems with appropriate oversight for defense and safety. The section also encourages consultation with experts and cooperation with non-profits, and other entities, such as universities.

The second section, Title 10, subtitle D, section 1051, on the National Security Commission on AI, is designed to be composed of fifteen people. Appointments will be made from House and Senate committees, the white house, and the Secretaries of Defense and Commerce each. The committee will consider trends, competitiveness, investments, partnerships, defense, risks, etc, for artificial intelligence, machine learning, and other associated technologies. The same section mentions, "$10,000,000 shall be made available to the Commission to carry out its duties under this subtitle." (Congress.gov)

Section 238 and Section 1051 have their respective funding at the end of the law. Additionally, the entirety of title 16, subtitle C is Cyberspace-Related Matters. These two sections show the direction the United States is heading for Artificial Intelligence, in accordance with my learning objective 5, about AI These sections, other than AI, are outside the scope of the paper. However, a direct link to the law is here: H.R.5515.

5.2 Acts: Passed the House, Now To The Senate

The following bills passed the House, which means they are halfway to becoming implemented laws. They only have the Senate left, as they all originated on the House side.

The first law, H.R.3388 - SELF DRIVE Act, is about the National Highway Traffic Safety Administration and their plan for incorporating a safe road environment as automated driving continues to become mainstream. They include a cybersecurity plan that protects the consumers, as well as a privacy plan for the same purpose. Later in section 5.5, there are other laws that define and develop the regulation of automated driving, but they are less comprehensive than H.R.3388.

Another bill that has passed the House is H.R.6229 - National Institute of Standards and Technology Reauthorization Act, which will allow NIST to continue to exist. The act is for $1,125,000,000, and focuses on quantum information, cybersecurity AI& data science, the internet of things, and composite research.

5.3 Bills: Introduced in One or Both Chambers

The following bills have not passed in either house. Most bills originate in a single house and then are passed onto the other side of the capitol once approved. However, it is common for a bill such as the Computer Science Career Education Act to be introduced to both houses simultaneously. If amendments are made individually to this bill, but it passes in both houses, it will go to the conference committee to work out the differences.

5.3.2 Artificial Intelligence

Certain laws introduced by Congress show their careful depiction of AI from the rest of the topics in computer science. The first two are H.R.4625 - Fundamentally Understanding The Usability and Realistic Evolution (FUTURE) of AI Act and H.R.4829 - Artificial Intelligence Job Opportunities and Background Summary (AI JOBS) Act. Both are about analyzing the technology in the United States workforce, regarding who will be affected and which skills workers will need to be competitive.

The third law is H.R.5356, the National Security Commission Artificial Intelligence Act, designed to create an 11-person committee. This committee is identical to the one created in the John McCain National Defense Authorization Act, except with fewer people. Congressmembers sometimes introduce bills similar to others introduced by other members to give more weight to the topic.

AI will have a significant impact on the world, specifically on how the government operates. In accordance with learning objective 5, which is to predict the impact of AI on the Federal government, AI will make all computing faster and free up life for most people.

5.3.2 Automated Driving

Another topic Congress has proposed legislation on is Automated driving, which is particularly interesting to me because it will improve the quality of life for all people. The following bills deal directly with their regulation and general Congressional acknowledgment. The bill numbers, without the H.R., since they are all house bills, are 3430, 3405, 3407, 3411. These laws are all very similar and focus on the National Highway Traffic Safety Administration, specifically in making an Advisory Council for

Automated Driving System Cybersecurity and allowing more information sharing between the manufacturers of automated cars. Similarly, there is an exemption for the testers of the cars on roads to allow the promulgation of a working model in H. R. 3405. These cars will be very productive for our society in moving goods, as well as allowing people to work or relax while traveling.

5.3.3 Computer Science

Finally, several laws have been introduced to Congress in the 115th session showing the advancement of computer science in education. The first, S.648/ H.R.2304 - Computer Science Career Education Act, is designed to be a grant program for four to six-year higher education programs that also help education for kindergarten through grade 12 students and works with regional employers to develop the skills required. Similarly, the Code Like a Girl Act of S.1968, is also about grant programs, but with a special focus on girls under the age of eleven, as a result of their finding that "all the new STEM (Science Technology and Mathematics) occupations created from 2014 to 2024, nearly ⅔ will be computing jobs" (Congress). The final bill, H.R.2305 - Computer Science in STEM Act, is focused on computer science and is still similar to the previous two, to focus education in Computer Science related STEM education since that is what the country will need the most soon.

6. Analysis

Overall, I had a great and insightful experience at Capitol Hill. Many, if not most, of the topics were related to the impact of computers on society, especially in the governmental sector. Specifically, I learned about AI, in accordance with my final learning objective five, to predict the impact of AI on a Federal level. As a result of my internship, I believe the next five years will develop AI capabilities through the government's engagements with research bodies, such as universities, through H.R.5515 - John McCain National Defense Authorization Act for Fiscal Yr. 2019. The subsequent developments will rapidly reform the operation of our society, as information, statistics, and processes will be nearly instant instead of the current human rates of processing the same.

6.1 Project Specifics

My projects consisted of attending the hearings and briefs, as mentioned above, and are in accordance with my first learning objective, about translating subcommittee hearings & briefs. The briefs can be found on the House of Representatives website at house.gov/committees.

Most conversations, topics, and debates in the briefs are logical. Many of the topics covered in my discrete structures class aided my understanding of the flow of the conversations. Similarly, many of the solutions to federal problems, such as the IRS authentication and the DHS Red Team, required an understanding of many technical concepts, such as the application of the National Institute of Standards and Technology Special Publication 800 series, the guidelines for safe computing, and technical vocabularies, such as pivoting, trigger thresholds, and binding operational directives. These computer topics all change how society will function, opening up methods through security in the same way encryption algorithms allow secure transactions over the internet.

Key skills I used during this process were: recognizing the definitions of the technical words and concepts without needing to look them up or ask what they meant, which greatly improved my comprehension of hearings. Similarly, I could easily organize data on the computers since I am familiar with computer shortcuts and methods to make data presentable due to working with them often.

6.2 Key aspects of the projects

For the projects, I had several critical points to manage in order to complete what I needed. I was required to balance completing required office tasks, like communicating with constituents, with my other projects. Second was ensuring the office had intern coverage while I attended the hearings. Third was getting to the locations and understanding how the information was communicated, such as context and application. From this understanding I had to keep detailed enough notes to relay a written communication of the assignment to the staff member in the office that would find the information useful, as they all have different areas of responsibility. Many of the technological aspects had to be especially clear.

6.3 Challenges

One of the challenges I experienced was the traffic and time I experienced getting to the internship. To get to the internship by nine AM, I would leave my house at six AM to drive an hour to the train station in rush hour traffic. I believe there is a tremendous opportunity for automated driving to fix issues experienced in traffic. Another challenge I experienced was finding the best subcommittee hearings. I went to the internship on Mondays and Wednesdays, so some technical hearings happened simultaneously or while I had to work on another project or were on days, I was not in the office.

6.4 Lessons Learned

Looking back on the experiences I went through, I believe I learned a lot in accordance with my objectives. Specifically, I learned how communication flows in a Congressional office, as well as through the district and the capitol itself. Much of this communication is enhanced through the application of computers. I can use this in my studies to

7. Overall Perspectives

Congress is a great place to learn about core issues on many topics, but more relevant to me and my career are the computer topics. I'm grateful to Congressman Ruppersberger and his office for allowing me the opportunity to work in his office for the fall. I would highly recommend the same opportunity to anyone considering it and am gladly willing to work further to progress in the United States, as I learned through the internship.

7.1 Expectations

The internship far surpassed all the expectations I had. I learned a large quantity of information, and most of them had computer applications. As a result, I'm certainly more confident in my studies and can see long-term legal possibilities.

7.2 Career Goals

In my career, I hope to improve the quality of life for all people. Specifically, I value applications of AI and automation to allow us to focus on greater and greater solutions in life. I hope to work for a company that develops automated driving, or a process that will be equally as productive, such as Artificial intelligence. Further into my career, I would enjoy developing the policy, even law, for the safe and practical use of such systems.

7.3 Coursework Evaluation

I believe much of my course work allowed me to learn at the internship. Specifically, my Computer Science 203 Discrete Structures course and my Computer Science 201 course on Python programming helped to understand where the technology is headed topically. In Discrete structures, I learned logic, which greatly allowed me to formulate logistics for events and paperwork, and associations between events in the government. The Python course allowed me to easily enter information into computer systems for logical reporting.

7.5 Full-time Career with the Organization

I would happily pursue any opportunity for full-time employment with Congressman Ruppersberger's office. There is a strong sense of connection and value in the day-to-day work that will impact society for the better. As I see it, the best way to work is for a long-term purpose, a value I see daily in the office.

7.6 Applications

I'm now familiar with the structure of the Federal Government, the highest power in the country, and how it approaches computer science, as well as the developments that proceed from it. With this knowledge I can help guide the computer community to be cohesive with federal practices and expectations. I would suggest to other people interested in positions with the Federal Government to get involved with all opportunities possible at their internships, which greatly increases the depth of understanding of the experience and value of the time on site. Additionally, this knowledge helps me to focus my own studies on areas that are more relevant to the needs of the nation.

Works Cited

Ajir, Media, Bethany Vailliant. “Russian Information Warfare: Implications for Deterrence Theory.” *Strategic Studies Quarterly*, Air University, 2018, Pages 70-89.

Barron, Ryan. The glowing Capitol. 7 November 2018, United States Capitol, Washington D.C.

Committee on Commerce, Science, and Transportation. Consumer Data Privacy. 10 October 2018.

Congress. Library of Congress, 2018, https://www.Congress.gov. 15 November 2018.

Department of Homeland Security. Hack The staff. 29 October 2018.

Grassi, Paul A., Michael E. Garcia, James L. Fenton. “Digital Identity Guidelines” National Institute of standards and Technology, June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. November 10, 2018

Internet Quorum. Leidos, 2018, https://www.intranetquorum.com/. 10 November 2018.

Miller, Ron. “Putting the Pentagon $10B JEDI cloud contract into perspective”. Tech Crunch, Oath Tech Network, September 2018. https://techcrunch.com/2018/09/26/putting-the-pentagon-10b-jedi-cloud-contract-into-proper-perspective/. 29 October 2018.

Ways and Means Committee. Online Taxpayer Authentication. 26 September 2018.

Moore, Mike. “What is 5G? Everything you need to know”. Tech radar, Future Publishing, 10 November 2018, https://www.techradar.com/news/what-is-5g-everything-you-need-to-know. November 12, 2018.