The Pursuit of Knowledge: A Case Study on How Elite Universities Pose a Threat to National Cybersecurity

The Pursuit of Knowledge: A Case Study on How Elite Universities Pose a Threat to National Cybersecurity

Miguel A. Sanchez

A Thesis in the Field of International Relations

for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

September 2017

Abstract

This thesis investigates how the role of universities, as not only stewards of information but creators of it as well, have evolved with the advent of the Internet and the digital revolution. That evolution has brought about it an immense increase in access to data and information but also exposed huge vulnerabilities in the protection of that data. Due to the close partnership between academia and government, those vulnerabilities pose a significant risk to national security.

I first begin by setting the baseline that universities, specifically elite research universities like Harvard, all have a stated mission of creating knowledge and education world leaders. To do so, they must be open centers of knowledge and information. A library is nothing if not a symbol of that. However, because of that open environment, securing that information from the outside becomes very difficult.

This thesis then highlights the partnership that academia has forged with government to create knowledge, oftentimes for the advancement of national security. An example of this is the Manhattan project. The lines between academia and government become blurred yet the critical assets and information reside in both. This allows for outside attackers, specifically nation-states, to exploit academic vulnerabilities to access national security data.

The final part is a case study hypothesizing on how nation-states can leverage the open nature of universities to access sensitive data. I finish by offering some suggestions on how universities can seek to secure the information that so readily flows through their environment.

Dedication

I dedicated this thesis to my mother, Maria, to whom I owe everything good that I am or ever will be. Thank you.

I also dedicate this to my other mother, my aunt, Guadalupe, who dedicated much of her life to me and to whom I owe more than I can ever repay. Thank you.

Acknowledgements

I am incredibly grateful and humbled to the many people who have helped me not just in writing this thesis but through my personal, professional and academic life. To say that I couldn't have done it without your help and guidance is an understatement.

Dr. Doug Bond, lecturer in the Harvard Extension School and advisor in the Master of Liberal Arts (ALM) program, who guided me from the time when I didn't even know where to begin or how to even get started in writing this thesis. He's been incredibly patient and helpful and I owe him an immense debt of gratitude.

Dr. James Cuff, assistant dean of research computing and distinguished engineer at Harvard University, who devoted his time and attention to direct this project. I learned a lot from his knowledge and guidance, and am very grateful for the time and effort he gave in being my Director.

Christian Hamer, Chief Information Security Officer at Harvard University, and to the rest of the stellar Information Security team at Harvard. I learned so much being a part of that team and it is because of them that I can even begin to write this thesis.

To all the staff of the Master of Liberal Arts (ALM) program in the Extension School at Harvard University: thank you for this opportunity and for the hard work you do for students.

Finally, thank you to everyone that I did not mention but who have had a part in helping me, either directly or indirectly, in this endeavor.

Table of Contents

List of Figures

Definition of Terms

Nation-State Actors: national cyber groups, either directly within the control of a national government or tangentially connected to it via more subversive means, with significant resources, tools, and time to perform advanced and sustained cyber-attacks on targets over a long period of time. They are often known as Advanced Persistent Threat actors or APTs

Cyberattacks: an attempt by any individual to access a computer network, system, or the data that flows through them without proper authorization. It should be noted that a cyberattack does not need to be successful in order to be categorized as an "attack". The attempt only is sufficient to classify it as a threat and the attempt alone can cause significant damage to a target.

Script-Kiddie: an unskilled or amateur person who uses existing scripts or programs developed by others to attack computer systems, networks, or websites.

Cybercriminals: an individual or group of individuals that use computers as a primary means of committing illegal activities. These illegal activities mostly center around stealing sensitive data like credit card or social security numbers, destroying or manipulating data, or making systems unavailable for the primary purpose of making money.

Hacktivists: an individual or group of individuals whose purpose is the user of computers or computer networks to promote a political agenda, ideology, or ideas.

Indicators of Compromise (IOCs): based in computer forensics, it is a piece of evidence or an artifact found in a computer or a network that sufficiently indicates there exists a network intrusion. These indicators are often virus signatures, IP addresses, or hashes of software and can be used to attribute the attack to a known group or use it to detect and stop future network intrusions.

Academic Institutions: any not for profit institution that is dedicated to education and research and, in this study, has a high amount of faculty and staff with direct or indirect access to high-level people or data in U.S. governmental agencies.

Zero-Day Vulnerability: Refers to a problem or hole in software that is unknown to the vendor or maker of that software and therefore can be exploited without there being a fix for it.

Bring Your Own Device or BYOD: A policy that permits employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access the host institutions network, information, and applications.

Privileged User/Account: A user who, by virtue of their function, seniority, or role has been given powers within the computer system or network, which are greater than those available to the majority of users.

Chapter I

Research Universities as Open Centers of Information

Before we can begin to understand how universities are susceptible to nation-state actors in cyberspace, it's paramount to first understand what the purpose of universities are and how they functioned prior to the technological revolution. This chapter will address the basic mission and purpose that all universities share and how research universities expanded on that core mission. It will also address how that mission and purpose was achieved through the construction of institutions and systems designed to both develop knowledge and spread it. Finally, this chapter will discuss the intersection of government and research universities from its inception and the importance of that relationship.

The first research university dates back to the early 19th century when Wilhelm Von Humboldt reformed the University of Berlin.[1] Prior to that seminal moment, universities were designed as places to teach and prepare professionals, specifically around law, medicine and theology.[2] To achieve that purpose, universities built institutions and systems to facilitate the transfer of knowledge to the university and its members. Universities were designed to be borderless institutions where knowledge was disseminated to all its faculty and students. For this reason, the earliest European

---

[1] Fallon, Daniel. 1980. The German University: A Heroic Ideal in Conflict with the Modern World. Boulder: Colorado Associated University Press

[2] Altbach, Phillip G., and Jamil Salmi. *The Road to Academic Excellence.* The World Bank, 2012

universities used Latin as a common language by which to aggregate all previous information (written in Arabic and Greek) and circulate it.[3]

To this end, universities, starting in Europe, built institutions and places were knowledge could be accumulated and shared. The most functional and recognizable of these building are libraries. Their purpose was to both store knowledge in a central location but also provide a place whereby university participants could access it and collaborate among themselves.

Then came van Humboldt and the advent of the research university in the early 19th century. What this change did was add the element of knowledge development and advancement to the already established tenant of knowledge aggregation and sharing within the university. Research universities were now a central part of the development of information whose focus was now on "expanding knowledge, leading to new understandings, products and process that strengthen national economies, improve the quality of life of the nation's citizens and enrich its culture".[4]

What is most striking about the above is the incorporation of knowledge development within the spheres of society and government. This was not by accident. Von Humboldt purposefully tied the university closely to state and society, to the point that the president of the University of Wisconsin-Madison claimed that "the border of the

[3] Altbach, Phillip G., and Jamil Salmi. *The Road to Academic Excellence.* The World Bank, 2012.

[4] *Hefei Statement on the the Ten Characteristics of Contemporary Research Universities*. Retrieved from The Association of American Universities: http://www.scienceguide.nl/media/1633686/hefei_s_101013_pdf.pdf

university is the border of the state".[5] This incentivized national governments to support the research university model because they assisted in national development, a core mission of all national governments.

This model continues throughout the U.S. and Europe today with strong partnerships between research universities and government agencies. The United States government, for example, spends a significant amount of money in support of American research universities, particularly in the 19th and 20th centuries, as they were committed to national development and saw higher education as a contributor to that development. National governments saw the benefit that could come from research universities assisting in economic, societal and cultural development as it not only benefited the domestic population but it also enhanced the nation's international power and influence.[6]

International reputation and influence are not only central in national government's support of research universities but also within the universities themselves. In order for research universities to influence national development they must establish themselves as being able to produce original research that significantly contributes to the breadth of knowledge, both basic and applied. Because of this, research universities' organization, reward structure, and academic culture is focused on productivity.[7] An example of this is something that all universities treasure above all: academic freedom.

---

[5] Veysey, Laurence R. 1965. *The Emergence of the American University.* Chicago: University of Chicago Press.

[6] Altbach, Phillip G., and Jamil Salmi. *The Road to Academic Excellence.* The World Bank, 2012

[7] Altbach, Phillip G., and Jamil Salmi. *The Road to Academic Excellence.* The World Bank, 2012

Academic freedom is "the concept of open inquiry as core value of the university."[8] What this does is allow all university participants, be they staff, faculty or students, the freedom to pursue teaching, research, publication and expression without restriction either internally or externally. It immunizes research universities from outside interference while holding true to the central principle of the expansion of knowledge. This model has worked well for many years as it allowed for the rapid advancement of research and knowledge but it also set the stage for a culture antithetical to restrictions or controls, even those designed to keep their information safe.

[8] Altbach, Phillip G., and Jamil Salmi. *The Road to Academic Excellence.* The World Bank, 2012

Chapter II

Government and Social Contract Theory

Governments have played a central role in the creation and development of research universities. Before we can begin to understand the relationship between research universities and government, it's important to have a general idea of how governments came to be, what their role in society is, and how this formulates their view on knowledge and information. Note that this chapter will not delve deeply into the political science of the state theory. Rather, it will summarize some of the conceptual ideas and normative claims of the function and role of Western governments in relation to society, knowledge, and power. Finally, when I reference governments, I am specifically referring to the U.S. government and those Western European countries that are closely related to it.

Most political scientist would trace the beginning of modern American and Western European forms of government to the social contract theories put forth by Thomas Hobbes, John Locke, and Jean-Jacques Rousseau, philosophers that lived in the 17th and 18th centuries. While they differ in very meaningful ways, what they all share in common is the idea that people, who make up communities or societies, give up certain rights and power to the state or government in return for certain benefits. Most often those benefits take the form of property rights, rule of law, and security.

The fundamental difference between this concept of government and what came before is that it is built on the assumption that all men are created equal. Because of this, there is

no one person or group of people that have an authoritative claim on power. Instead, that authority comes from free and equal people entering into a contract with the state to give up some of those freedoms or rights in exchange for some kind of good. At its very essence, it is a relationship in which the people expect that government will make their lives better and governments expect that the people will adhere to predefined rules or laws.

Although the concepts for what the role of government should be is outlined in the political philosophies of Hobbes, Locke, and Rousseau, not a lot was said, at the time, about how governments should go about achieving its social contract. To highlight this point, the American founding fathers in the 18th century, using much of what Locke wrote in drafting the constitution, did so behind closed doors. They willingly entered into that social contract that guaranteed certain right, even going so far as enshrining those rights in a constitution, but refusing to be transparent about how or why they chose those rights or how they would be enforced. "The practice of withholding information when important public policies so require is nothing new; the Constitution's framers themselves kept their deliberations secret"[9].

The founding fathers didn't trust the public because they didn't think them capable of making the right decisions. However, not many political scientists or policy makers would argue that the government doesn't have a right to be secretive about the development of certain things. "Even if it is agreed that citizens should generally be able to deliberate about government action, the need for secrecy sometimes justifies

[9] Cass R. Sunstein, *Government Control of Information*. 74 Cal L. Rev. 889, 892 (1986)

government control of information" (Sunstein, 1986)[10]. Among those reason that government can control the disclosure of information are military or diplomatic secrets and "technical data": scientific information with actual or potential military applications.[11] What is most interesting, and a central tenant of this paper, is that, while it is widely accepted that this sort of technical data *should* be secret both from a nation's citizens as well as foreign governments, that secrecy doesn't extend to the places where that technical data is created. This is the intersection of government and academia.

[10] Cass R. Sunstein, *Government Control of Information*. 74 Cal L. Rev. 889, 892 (1986)

[11] Cass R. Sunstein, *Government Control of Information*. 74 Cal L. Rev. 889, 892 (1986)

Chapter III

Government and Academia

United States law has a rather broad definition of what technical data is:

> 120.10 Technical data. (a) Technical data means, for purposes of this subchapter: (1) Information, other than software as defined in §120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. (2) Classified information relating to defense articles and defense services; (3) Information covered by an invention secrecy order; (4) Software as defined in §121.8(f) of this subchapter directly related to defense articles; (5) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in §120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.[12]

To truly understand what "technical data" is, and how universities play a pivotal role in its development, it's best to use one of the most well-known, and seminal, examples of its creation: the Manhattan project. The Manhattan project is a paramount example of what kind of technological breakthroughs can come from the partnership between academia and government that Wilhelm von Humboldt envisioned in the 19th century. It is also an example of the contradictory and competing purposes that both institutions have when creating, storing, and using information.

The Manhattan project started at the latter half of 1941 at the urgent behest of two of the world's most renowned scientist: Alberto Einstein and Enrico Fermi. Both, having

---

[12] International Traffic on Arms Regulations; Part 120, Subchapter M

fled authoritarian regimes in Germany and Italy, respectively, saw the need to begin developing an Atomic bomb after learning that German physicist had begun to unlock the secrets of splitting Uranium atoms in 1939. The U.S. government code named the project to develop an atomc bomb the Manhattan project.

The research began in only a few universities – Columbia University, The University of Chicago, and the University of California at Berkley. In December of 1942, underneath the grandstands of Stagg Field at the University of Chicago, Fermi led a breakthrough producing the first controlled Nuclear Chain Reaction. After this milestone, the U.S. government began allocating great amount of funds to the project, eventually spending almost $2 billion in research and development of the atomic bomb. And central to that research and development were American universities.

The corollary to that research and development was that the project had to be shrouded in utmost secrecy. Neither the Germans, Japanese or the Soviets could know even that the Manhattan project existed, let alone the technical data that was being produced. For this reason, the project was made publicly aware nor was there any ever any public debate about its value proposition. This is in line with what Cass Sunstein, alluded to earlier, defines as the state's obligation to keep certain information secret and outside of public discourse. Furthermore, it's also part of the social contract theory in that it fulfills the state's obligation to protect its citizens, in this case by developing the technical data, in conjunction with universities, to build weapons to win a war. Even with all that secrecy, however, it was later found out that a Soviet spy by the name of Klaus Fuchs had infiltrated the inner circle of scientists and stolen some of the Manhattan project's technical data, allowing the Soviets to develop their own Atomic bomb not long

after the U.S. This only serves to highlight that even when all precautions are taken to keep sensitive data confidential, there are always ways around it.

The Manhattan project is an example of the collaboration that goes on between government and academia. The U.S. federal government has, and still does, play a significant role in the funding for university-based research and development. In fact, in the late 1960s, it accounted for almost 73% of all research and development funds in academia.[13] That figure has declined through the decades but the numbers themselves have grown. "In inflation-adjusted dollars, federal support for universities increased from around $8 billion per year in the 1960s to more than $30 billion today."[14] As the figure below shows, it still accounts for the majority of research and development funding in academia.

[13] American Association for the Advancement of Science. Retrieved from: https://www.aaas.org/page/rd-colleges-and-universities

[14] American Association for the Advancement of Science. Retrieved from: https://www.aaas.org/page/rd-colleges-and-universities

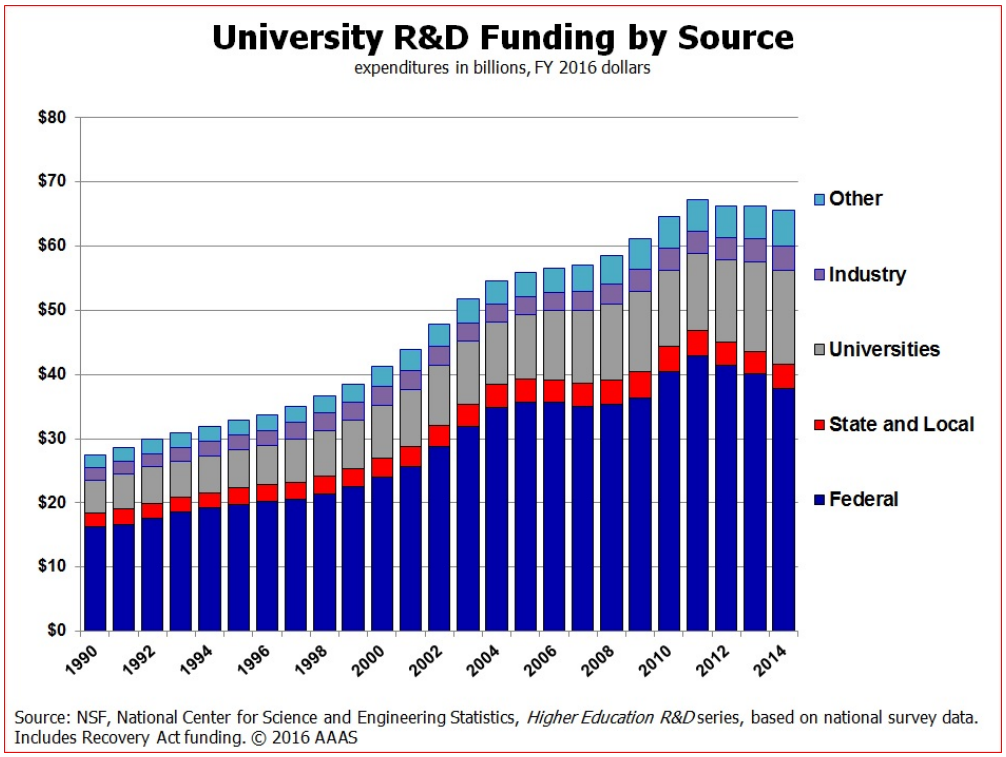

Fig. 1. University R&D Funding by Source

There is such a strong connection between academia and government that the U.S. created agencies specifically designed to allocate funds to promote the creation of information in universities. Agencies like the National Institutes of Health and the National Science Foundation are examples of such government agencies. Prior to the digital revolution, the data that was produced by those connections could be more controlled and locked down, though as the Manhattan project shows, not completely. With the advent of the Internet, all that changed.

Chapter IV

The Creation of the Internet

The origins of the Internet we know today can be traced back to the early 1960s when Leonard Kleinrock published a paper on packet switching theory, a basis for computer communication protocols.[15] Many of the Internet's founding fathers at MIT then moved over to the U.S. Defense Advanced Research Projects Agency (DARPA) where they continued their research into computer communications with government funding. It was there that the first prototype of the modern-day Internet, known as "Arpanet" had its beginning in 1967.

The first node in Arpanet was setup at UCLA and connected to a second node at Stanford.[16] Even at this early stage in the development of what is now known as the Internet, one sees the paramount influence that academia had in the development of a government agency idea. From UCLA and Stanford, other nodes were added at UC Santa Barbara and the University of Utah. From there, it spread to the east incorporating other academic institutions, like Harvard and MIT, as well as some private companies and government agencies. With the spread of Arpanet, new technologies were developed to make communication easier and faster among the increasing number of computers that were connected to this inchoate Internet.

---

[15] Paul E. Ceruzzi. *A History of Modern Computing.* MIT Press, 2003

[16] Paul E. Ceruzzi. *A History of Modern Computing.* MIT Press, 2003

The fundamental technology that started with Arpanet and underpins the way the current Internet works is that of open-network architecture. Open-network architecture was the idea that, as the Internet grew, it would be a consolidation of various independent networks, starting with Arpanet.[17] The architects of the Internet realized that, in order for the Internet to be able to scale, they had to create it in such a way that would allow for a variety of different network architecture and technologies to integrate into one cohesive Internet. "In this approach, the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level 'Internetworking Architecture'".[18] This meant that, regardless of what network technology one used or how one architected their internal network, it would be still be able to communicate with the rest of the networks out there. That fundamental communication protocol, developed in academia, is now known as the Transmission Control Protocol/Internet Protocol (TCP/IP).

TCP/IP is at the basis of how computers talk to each other. Every computer, be it a server that is running an application, or a desktop that is running Windows or Mac operating system, they all have to have an IP address that allows them to communicate with other computers anywhere in the world. The reasoning behind this open architecture, as developed by the Internet architects were 1) Each distinct network would have to stand

---

[17] Leiner, Barry M. (1997) Brief History of the Internet. *InternetSociety.org.* Retrieved from https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

[18] Leiner, Barry M. (1997) Brief History of the Internet. *InternetSociety.org.* Retrieved from https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

on its own and no internal changes could be required to any such network to connect it to the Internet, 2) Communications would be on a best effort basis. If a packet didn't make it to the final destination, it would shortly be retransmitted from the source, 3) Black boxes would be used to connect the networks; these would later be called gateways and routers. There would be no information retained by the gateways about the individual flows of packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery from various failure modes, and 4) There would be no global control at the operations level. [19] Every other technology or protocol that came after it still had to adhere to those four fundamental ground rules. This, though unintended, had great consequences for the security and privacy of the data on those networks.

It is notable that, throughout the discussion on the creation of the Internet, the security of the data transmission on those networks didn't play a pivotal role.[20] It seems that the architects were mostly concerned with sending data reliably and accurately than they were with ensuring the confidentiality or security of it. It was only in 1983, more than a decade after the inception of Arpanet and after it had grown much larger and started connecting to government agencies, including the CIA, NSA, and FBI, did the Defense Communication Agency step in and begin to look at security as a concern.[21] Because of the fact that security wasn't "baked in" into how the Internet runs, and

---

[19] Leiner, Barry M. (1997) Brief History of the Internet. *InternetSociety.org.* Retrieved from https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

[20] Paul E. Ceruzzi. *A History of Modern Computing.* MIT Press, 2003

[21] Matthew Lyon; Katie Hafner. *Where Wizards Stay Up Late: The Origins Of The Internet.* Simon and Schuster: 1999.

because security measures, technologies, and protocols, have been bolted onto a fundamentally insecure system, there exists so many ways to attack systems on the Internet. In fact, not long after the Defense Communication Agency decided to take the security of the then Arpanet seriously, there came to light one of the first, if not the most well-known, cyberattacks by a nation-state.

In 1986, the Internet was connected to mostly government and university computers, and what they could do was basic: electronic mail, news groups, and remote connections between computers. [22] However, that didn't prevent cyber attackers from targeting them. An employee at the Lawrence Berkeley National Laboratory in northern California noticed an abnormality in who was logging on to the computers there. In his spare time, this employee began checking to see why this abnormality happened and who was behind it. At first, he thought that it was a UC student just messing around. As it turns out, however, it was Soviet Russia targeting UC Berkley in an attempt to get access to sensitive data. This was one of the first known nation-state cyberattacks.

From there, security incidents increased. Only two years later in 1988, the first automated network security incident was recorded, known as "the Morris Worm". [23] A student at Cornell University wrote a program that would exploit a vulnerability in a computer and then automatically connect itself to another computer via the same vulnerability. It would do this an infinite amount of times as long as the computer it was connecting to had the same vulnerability. This worm caused all the computers it infected

---

[22] Longstaff, Thomas A, et al. *Security of the Internet*. Software Engineering Institute, Carnegie Mellon University: 2017

[23] Longstaff, Thomas A, et al. *Security of the Internet*. Software Engineering Institute, Carnegie Mellon University: 2017

to stop working, virtually at the same time. As a result, 10% of U.S. computers connected to ARPANET were disabled.

What started out as a connection between a couple of dozen computers in universities and government as a way to share research and information has now spread into every sector of society and the world. With it, usage patterns have changed dramatically so that now it is "expanding into important areas of commerce, medicine, and public service" with it only increasing in the future.[24] The expansion of the Internet, and with it the data that flows through it, has led to an increase in attempts to access that data.

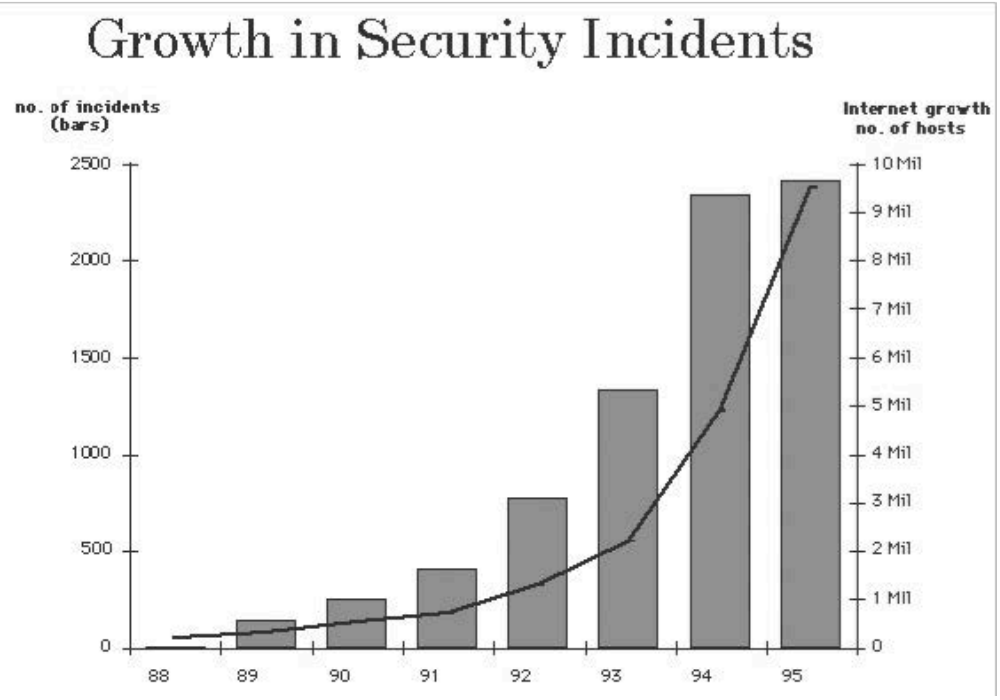

Fig. 2. Growth in Security Incidents

[24] Longstaff, Thomas A, et al. *Security of the Internet*. Software Engineering Institute, Carnegie Mellon University: 2017

Chapter V

Universities in the Age of the Internet

As noted in the last chapter, the creation and expansion of the Internet has given rise to a vast amount of information that is readily available. Universities, like they were prior to the Internet, are a central repository for a lot of that information, especially sensitive information. The best way to describe universities is by comparing them to small cities. They have hospitals, financial centers, police stations, centers of commerce, and intellectual property and human capital, to name a few. It is the exact place where a malicious actor would go if they were looking to steal information.

A lot of universities either have hospitals or medical centers attached or are affiliated with them. Even if they don't, they at least have to have a university health services center where students can get treated for minor illnesses. This gives them access to what is called Protected Health Information or PHI. Data about your health history, your insurance information, and your even your personally identifiable information or PII all is stored on university health services systems. This data can be invaluable to an attacker as access to it can be leveraged for a whole host of nefarious activities.

One of the main and specific ways that theft of health information can lead to negative consequences is through health insurance fraud. With skyrocketing medical care costs, cybercriminals can use stolen healthcare information to commit health insurance fraud by filing fraudulent insurance claims. Because of the lack of checks and balances built into the growing electronic health care industry, these fraudulent claims are often

caught too late and the burden of them, oftentimes, has to be borne by the person or persons whose data was stolen. Universities, as centers or with access to copious amounts of that data, become a ripe target for someone looking to either leverage or sell that kind of information.

Outside of health information, universities also have access to lots of very sensitive personally identifiable information through their various human resources departments. Each human resources department has to have filed a person's social security number, bank account information, home addresses, tax information, etc. These data elements can be used by cybercriminals to steal someone's identity and perform all sorts of fraudulent activity, including taking out credit cards or loans in their names.

Universities also sell a variety of goods. From books and school supplies to clothes and food, they are centers of commerce where people can buy all sorts of things, oftentimes using credit cards. In order for those credit cards to process transactions, they have to flow, in some way or another, through that universities' network. This opens universities up to malicious actors trying to steal those credit cards, much like many other credit card breaches throughout the world, including Target and T.J. Maxx.

The above are examples of the kind of data that cybercriminals are after. The explanation of the different actors will be addressed in the next chapter but it's important to distinguish this kind of information from the kind of information that nation-states are after. The reason I highlight it above is to point out the complex, and large, nature of universities with the large range of sensitive data they have access to. And, as with anything that is large and complex, it becomes much harder to secure. What nation-states are really after are two things: human assets/access and research.

Human assets can most easily be described as the people who have access to information, institutions, or other people that nation-states would want. Members of a universities' faculty are a good example of this. Taking The Harvard Kennedy School (HKS) as a case study, a quick google search and a look at their public website reveals a lot of interesting information about the faculty that work there. Fig. 3. shows that out of a total number of 51 registered faculty at the HKS, 21, or almost half of them, have held or currently do hold high ranking positions in the U.S. government. I won't single out any one person for the sake of privacy but titles like Secretary of X or Director of the Council of Y are common among HKS faculty. And this is the norm throughout Harvard University and other elite research universities.

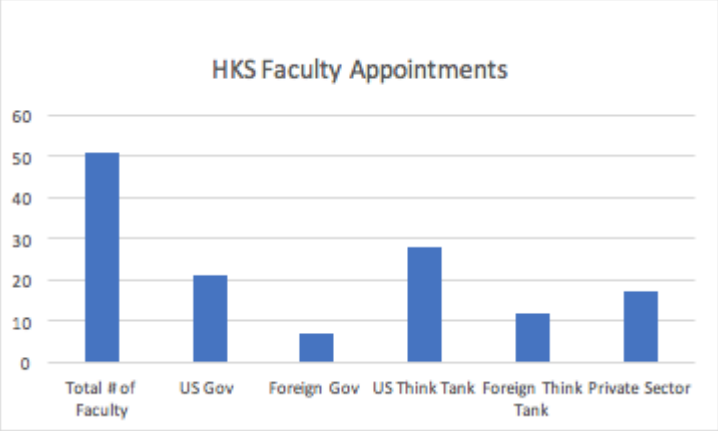

Fig. 3. HKS Faculty Appointments

As state earlier, nation-states look to compromise those kinds of people for two reasons: information and access. Even if those critical human assets in academia are no longer affiliated with those government agencies, it does not mean that they do not have access to sensitive and important information. They may have kept information on their personal computers or cloud storage devices (e.g. Google Drive, Dropbox, etc.) from

when they were in office. Furthermore, they may still be in touch with people within government, as is often the case, which could give them access to current confidential and sensitive information.

Beyond compromising the information that Harvard faculties have access to nation-states can also use these critical human assets as jumping off points. If we take as fact that universities are more open, and therefore easier, environments to breach, which will be addressed in chapter 7, then targeting Harvard faculty can result in an entry way into more sensitive systems. The idea is a simple one. Government networks are much more locked down and therefore harder to compromise. Academic ones are open and easier to breach. If a nation-state's ultimate goal is to breach a government agencies environment, what they will do first is target an easier one by compromising a Harvard faculty's email account, for example. If that faculty member held a government position, or even if they were acquainted with people in government positions, their contact list will be filled with critical government human assets that nation-states are after. From the vantage point of that Harvard faculty member's compromised systems and accounts, they can start sending targeted attacks to those government assets that are much more likely to succeed. How nation-state actors succeed is discussed in chapter 7.

Outside of the access that most Harvard faculty members have with high-level government and private sector people, nation-states are also after the research and development that goes on at Harvard and many other research universities. If we go back to the example of the Manhattan project, why would a nation-state spend the billions of dollars required in investment, resources, and time to research and build that kind of technical innovation when they can just as easily steal the information from the

institutions that create it? The IP Commission Report, a report on the theft of American Intellectual Property, estimates that hundreds of billions of dollars per year or "the order of the size of U.S. exports to Asia" is lost to IP theft, with cyberattacks claiming a large part of that, and increasing. [25] A large part of that R & D takes place at elite universities, like Harvard, but is much more open to attacks than private sector or government. Nation-states look to leverage that open environment to access that research information and use for their own national good.

I've established that universities hold a wealth of information that is valuable to a whole host of malicious actors. The next chapter will deal with who those malicious actors in cyberspace, how their motivations differ, and what they're ultimately after. Chapter 7 then goes into how universities are more vulnerable to cyberattacks and how nation-states can potentially leverage that open environment to access sensitive information.

[25] The National Bureau of Asian Research. "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property". May, 2013.

Chapter 6

The Cyber Landscape Today

Before delving into why or how nation-states target universities in cyberspace, it's important to know what other kinds of threat actors are out there and how their purpose, resources, and strategy vary. It's important to differentiate them because, by knowing their differences, and specifically the differences in attack methodology, universities can better defend themselves from each. There are three main cyber actors: hacktivists, cybercriminals, and nation-states.

The main differences between the three can be summed up by 1) what they're after, 2) the time and resources dedicated to the task, and 3) their attack methodology. While all three are related in the sense that if what an actor is harder to get, they'll most likely need to dedicate more time and resources to get it which will affect how they go about doing it. Nevertheless, it's worth analyzing them through that three-sided prism to get a comprehensive view of who they are and what they're after.

Hacktivists, as the formation of the word from hackers and activisms suggests, are people that target organizations in cyberspace to promote a certain social or political cause[26]. Hacktivism has its beginnings as early as the 1980s when people began to use their computer skills to spread messages of protest, similar to the street protests and sit-ins of decades past, but now adapted to the era of Internet and digital communication.

---

[26] Denning, Dorothy. (2015, September 8). *The Rise of Hacktivism*. Retrieved from journal.georgetown.edu/the-rise-of-hacktivism/

Hacktivists tend to be formed by a loose affiliation of people with the same social or political cause(s). They are usually spread out throughout the world and are not well-funded by any public or private institution. They, like many of their predecessors from the social movements of the 1960s and 1970s, are passionate believers in certain causes that want to create change by drawing as much attention to their cause as they can. This is usually in the form of destruction, disruption, and hijacking/defacement.

An early example of destruction was the WANK ("Worms against Nuclear Killers") worm that Australian hacktivists used to target the computer networks and systems of the National Aeronautics and Space Administration and the US Department of Energy in 1989 to protest the launch of a shuttle which carried radioactive plutonium. Their goal was to destroy, or at least hobble, the computers that controlled the shuttle to delay or stop the launch from happening. Their method was quite different from that of, for example, Stuxnet, which will be addressed in the next chapter, which was a worm used to target and destroy Iranian centrifuges. The difference in these attacks is that in the shuttle example, hacktivists were not tied to any government and did not do it in secret but as part of a wider awareness campaign against the use of nuclear weapons.

Hacktivists then added another tool to their arsenal in the 1990s: the denial of services or DoS attack. The Denial of Service attack, as explained in the glossary,[27] is an attack method used to overwhelm a computer system by flooding it with information, to the point that it is no longer available to be used for its original purpose by those for whom it was intended. An early example of this was in the late 1990s when a New York-based hacktivist group called the Electronic Disturbance Theater (EDT) developed a

[27] See Definition of Terms

software tool called FloodNet for what conducting what they called "virtual sit-ins". The tool automatically flooded targeted websites with information requests in an attempt to tie up traffic to the site and make it unusable by anyone else[28]. EDT used the tool to flood Mexican and US-Government websites in support of the Mexican Zapatistas.

Finally, the last major tool in the hacktivists arsenal is the hijack/defacement of websites. Whereas DoS attacks are used to make websites unreachable, hijacking and defacing websites is meant to take over control of the website and alter its content to broadcast the intended message of the hacktivists. This has been widely done by hacktivists since the inception of its use in the 1990s. What allows hacktivists to take control websites are common mistakes like not changing defaults passwords, using weak passwords, or using outdated or unpatched software. An early example of this was in 1996 when hacktivists took over the US Department of Justice websites and changed it to read the "Department of Injustice" while displaying pornographic material. They were protesting the passage of the Communication Decency Act of 1996, later ruled unconstitutional.

In today's world, there are thousands of hacktivist group supporting essentially every social and political cause on the planet. The most visible in the past decade has been a group called Anonymous. Anonymous is a loose collection of activists and hackers with regional and local offshoots that have launched thousands of cyberattacks against virtually every segment of the political, governmental and social world. They're known for wearing Guy Fawkes masks and using the image of a man in a suit with a "?"

[28] Denning, Dorothy. (2015, September 8). *The Rise of Hacktivism*. Retrieved from journal.georgetown.edu/the-rise-of-hacktivism/

as a head. Most recently, they've partnered with several other hacktivist groups to launch larger-scale cyberattacks, notably against Israel to protest its action against Palestinians.

There are several reasons why hacktivism has become so widespread in the past several decades. First, it does not require a lot of technical expertise or time and money to launch. Many of the tools are prepackaged and easy to use and simply require a computer and an Internet connection. Second, it poses little physical or legal risk to participants. Law enforcement agencies rarely prosecute hacktivist either because the damage done is minimal or because attribution is difficult. This is in stark contrast to street protests or sit-ins where it requires people's physical presence. Third, anyone in the world can join a cause. It does not require people to travel to a specific location, thus dramatically lowering the transportation barrier. Fourth, it enables individual action as well as group collaboration. People no longer have to be within a country to fight for a common cause. They can join whether in their home country or living abroad. Fifth, the effects of hacktivism are very visible as in the hijacking and defacement of a website or the complete loss of availability of a system through Denial of Service attacks. Oftentimes, those actions are publically pushed out through social media networks for even greater awareness.

Bringing hacktivism back to the academic realm, universities are by no means immune from their social crusades. In fact, Anonymous targeted MIT in 2014 for its perceived role in the suicide of hacker Aaron Swartz. The group took over a server for one of MITs projects and defaced with a message highlighting their grievances with MIT and vowing to keep fighting for Swartz's justice. This was not the first time MIT was

targeted by hacktivists, underscoring that academic institutions are within hacktivists' spheres of influence.

The Other Non-State Actor – Cybercriminals

There are many definitions under the umbrella term "cybercrime". The broadest is a crime that involves a computer and a network.[29] This definition encompasses things like cyberbullying, espionage, and intellectual property theft. For the purposes of this paper, and particularly this chapter, cybercrime will refer to one specific type: fraud and financial e-crime. Using this narrow definition, cybercriminals are motivated by one simple thing: money. This is in stark contrast to hacktivists who, as was shown in the previous chapter, have a variety of causes or movements they support.

The genesis of cybercrime really came from the realization that with more people sharing personal and confidential information online, money could be made by attacking those computers and networks. From 2013 to 2015, the cost of cybercrimes quadrupled with the cost of data breaches estimated to hit over $2 trillion dollars by 2019.[30] The scope of those affected ranges from individual people/consumers to large scale corporations. One of the main reasons for this incredible growth in cybercrime is the emergence of organized crime as a major player.

---

[29] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing

[30] Morgan, Steve. (2016, January 17). *Cyber Crime Costs Projected To Reach $2 Trillion by 2019.* Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5873db5a3a91

Organized crime has expanded from the traditional aspects of drug trafficking and the like to the digital world. Some of the reasons are similar to why activism has expanded to the digital world as well. It requires little time or resources to pull off. Law enforcement is rarely able to prosecute the criminals, either because of lack of attribution or because the cybercriminals reside outside of their jurisdiction. Finally, and most importantly, there's a much better return.[31]

One of the ways cybercriminals have focused on making money is by stealing credit card numbers. The news often reports this as a data or credit card breach affecting major corporations. One of the most well-known and publicized examples was the 2013 Target data breach where an estimated 70 million credit and debit cards were stolen. Attackers initially compromised one of Target's HVAC vendors and used that as an entry point to Target's environments. From there, attackers pivoted from less important systems to the ones that were used to process credit card information. They installed malware on them and were able to steal millions of credit cards from them. Target was not the first, nor the biggest, and they certainly won't be the last company to be targets of cybercriminals looking to steal credit card information.

Corporate data breaches, like Target, are just one way that cybercriminals make money off sensitive information, like credit cards. Another, and much more popular way today, is by encrypting information. This is known as ransomware. Ransomware is any method by which a malicious actor gets access to a person's data and then makes it

---

[31] Baraniuk, Chris. (2017, July 26). *It's a Myth That Most Cyber-Criminals are 'Sophisticated'.* Retreived from http://www.bbc.com/future/story/20170726-why-most-hackers-arent-sophisticated

unusable until the victim pays the attacker a specific set of money. There are many ways to achieve this but the most common is phishing.

Phishing can be defined as "the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money) often for malicious reasons, by disguising as a trustworthy entity in an electronic communication".[32] An example of this is when a malicious actor sends an email purporting to be from a bank, a social media account, an email provider, or even a friend asking that you either enter your information or open an attachment. It essentially leverages the trust you have in other institutions and service providers to get you to do something. Once they get access to your data or system, they can then hold the data ransom by using software to make it unreadable without a special key, which they have. The only way to get that key is by paying the ransom for it.

Nation-States

Nation-states differ from hacktivists and cybercriminals in virtually every way. They do not care about sending a message or promoting a cause, like hacktivists, and, in fact, prefer to stay as secretive and anonymous as possible. Do also do not care about stealing credit card data or holding data hostage for monetary gains, like cybercriminals. What they care most about is high-level access to the important government agencies and private companies, and the information that that access gets them.

---

[32] Ramzan, Zulfikar *"Phishing attacks and countermeasures*". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer: 2010.

Because their goal is more focused, their approach is also more targeted. Instead of trying to make the most amount of noise (hacktivists) or compromise the most amount of people (cybercriminals), nation-states tend to be very targeted about who they try to breach. They do much more reconnaissance on their targets, have much more patience in when they choose to attack, and have many more tools at their disposal, including ones that no other actors have: zero-day vulnerabilities.[33] And the reason they're able to leverage all of those resources and tools is because they have the backing of national government behind them. Their methodology can best be described by the Advanced Persistent Threat [34] kill chain.

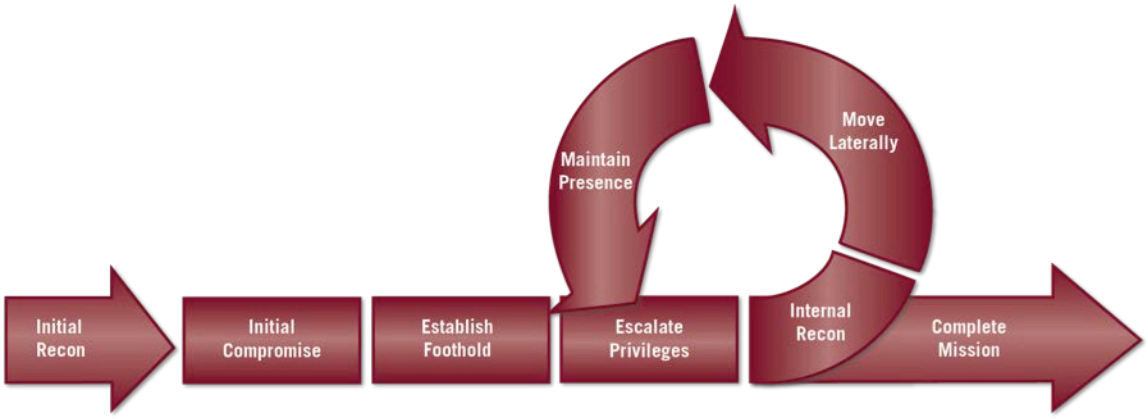

Fig. 4. The APT Attack Lifecycle

Fig 4. shows how nation-states or APT actors try to infiltrate any network. They first begin by doing low-level and under-the-radar reconnaissance to figure out things like who are the key people in that environment, what kind of software/hardware they use and is it vulnerable to any exploits, what kind of security measure they have in place, etc. All

[33] See Definition of Terms

[34] See Definition of Terms

of this is done without alerting any of the security team since a nation-state wants to be as invisible as possible. Once they find out as much as they can about the environment, everything from the people, technology, and procedures, they will launch an initial attack to get a foothold in the environment. Oftentimes this is what is referred to as “low-hanging fruit” or the easiest system to compromise with as little effort as possible and, more importantly, as invisible as possible. Once they are in the environment, they can then do more reconnaissance to find out more about the environment and then escalate to either more sensitive accounts or more sensitive systems. The hope is to leapfrog from the initial compromise point, which is most likely a system that does not have the sensitive data or access they are after, to ones that do. This is what “move laterally” means. Every step they make, they ensure that they have continued access to the system and environment through various means, almost like planting a flag at every checkpoint, before “moving laterally” again to more sensitive systems. Only after they get access to the data they are after do they exfiltrate it.

Chapter 7

Universities are the Current (and Next) Frontier - Harvard Case Study

Universities, by their nature, are generally open to the non-academic world. This characterization is particularly true with respect to wireless connectivity.

The open nature of Harvard (and other universities): Harvard Wireless Network

Universities are open centers of knowledge and information. To truly understand how open they are, it is worth using Harvard as a case study to analyze how universities' networks are architected and how data, systems and users interact with that environment. Of course, every university has their own unique network design and tools but the general concept still applies, and is worth contrasting with how the private and government sectors generally architect and lock down their environments.

Harvard's network, like most modern ones today, is separated into several segments. Theoretically, each segment is designed for a specific purpose and, more importantly, with its own security controls in place. The easiest way to understand this is by looking at Harvard's WiFi or wireless networks. Harvard currently has three wireless networks: Harvard Guest, Harvard University, and Harvard Secure. Each one is different in 1) who can access it, 2) the way that one is authorized to access and how they are authenticated, and 3) the security of each. Starting from the least secure, Harvard Guest can be accessed by anyone, even those that have no affiliation with the university. The

connection is not secure meaning that anyone on that network can “sniff” or view unprotected data from other people connected to Harvard Guest with the simplest of computer programs. To highlight the importance of this, it means that sensitive data, like credit card, social security numbers, protected health information, etc. can be intercepted by anyone on that network.

Harvard University wireless is a step up in security. Harvard University requires that a person authenticate themselves and their affiliation with the university using a Harvard account. This should limit the number of people that connect to the network to only those that are affiliated with the university. While this does prevent some people from getting on the network, there are several ways around it, including stolen Harvard credentials. Furthermore, once on the Harvard University wireless network, either through authorized or unauthorized means, the connection is the same as Harvard Guest, meaning that it is unsecured.

Harvard Secure, as the name implies, is the most secure of the Harvard wireless options. It not only requires that a person authenticate themselves using a Harvard account but it also protects or encrypts the connection. This means that even if someone with nefarious intentions were to get on the Harvard Secure network and try to intercept data going through it, they would not be able to as the data is encrypted providing a secure tunnel for data from the person’s machine to wherever they are sending data, including sensitive or confidential information. Like everything with technology, it is by no means completely unbreakable but the barrier is much higher that it should deter all but the most persistent and resourceful of attackers.

Harvard's Other Networks

Harvard wireless network are just one example of how universities can separate out, or segment, their networks and put different kind of controls and restrictions on them. The same thing applies to networks on campus that are wired, meaning that they require some kind of Ethernet cable connected to them to access Harvard's network, as opposed to wireless access. Whereas wireless networks allow Harvard students, faculty, staff, and guests to access the public internet, wired networks do much more than that.

Wired networks don't just allow people and their workstations to access things like websites and email, they are actually used to *run* Harvard websites and email as well as a vast range of other Harvard systems and applications, including sensitive ones like payroll, student information systems, and research computing. Because of the sheer size and complexity of Harvard, controlling what connects to what and what data flows to where can be a very daunting task. This can become even more challenging when one is faced with the decentralized nature of Harvard where each school, and sometimes even departments/groups within schools, has autonomy to purchase systems and put them on Harvard's network without proper controls.

I'll use an example to illustrate this a bit more, and then explain why it's important. Let's just say a researcher at Harvard gets a government grant to look into new military applications for a chemical compound that he's been analyzing. Part of it requires him to collaborate with other researchers at different universities and gather data from a variety of external sources. To do this he'd like to build a website or a web application that allows him to not just collaborate and gather data but also analyze it.

However, this researcher is keenly aware of that the grant has a limited set of funds which limits him from spending too much on the technical development of their research. Given that this researcher is intelligent and motivated (like every researcher at Harvard) and they have accumulated some technical skills through their academic career, they decide to do what any rational researcher under budget constraints would do: build the website or web application on their own.

Using grant funds, they buy a server from the internet or a retail store and build the system from scratch. Now it's time to connect it to the internet. They get an Ethernet cord, plug it into the jack in the wall, perhaps do a little bit of configuration in the network settings of the machine, and they connect to the Harvard network. What this actually means is that the machine this researcher built, with no help or authorization from Harvard IT, is now on a network segment along with several other systems. Furthermore, that network segment can, and often is, connected to other network segments. And this is what attackers as part of their modus operandi.

Corporate and Government Networks

Harvard's networks are quite different from corporate or government networks. Corporate and government networks are much more regulated and locked down. There are a lot of reasons for the difference between the two, not the least of which is the difference in principle and purpose between academic institutions and everything else. Academic institutions are designed to be open and shared information. Corporations and

government entities, by and large, choose to keep information private and out of the public view. The way their data networks are set up reflects that difference.

Corporate and government networks are much harder to get into. They rarely have wireless networks and, if they do, they are locked down so that not only does the person have to authenticate with a username and password but access is also limited to the individual machines by a hardware or network address. The concept of Bring Your Own Device or BYOD[35] is a foreign one in most government agencies and private sector companies.

The reason that personal devices are not allowed is that the company has no way of controlling or locking them down. In government or corporate networks, where only allowed devices can connect to the network, they are setup in such a way as to restrict unauthorized access to applications, websites, and content. They can also restrict what can of data leaves the environment, through such things like email, which prevents attackers from not only getting into the network but, if they were able to get in, prevents them from exfiltrating data. Those controls extend beyond the workstations themselves and into the network itself.

The network is configured to be completely isolated from the public. Unlike academia, information is meant to be contained and enclosed in its host environment. It is not meant to be shared or disseminated outside. For this reason, the entire network is architected to keep data in and keep unauthorized people out. An example, as pointed above, is limiting the devices that are allowed to connect to the network. No device, either connected through a wire or wirelessly, is allowed to connect to the network

[35] See Definition of Terms

because that system could be used as an entry point into the environment. I'll highlight an example of this in the next section.

Not only are systems tightly regulated and locked down but so are people. Government and corporate environments are much more locked down so that unauthorized people are *physically* prevented from entering the environment. Controls such as retina scanners, fingerprint readers, locked and regulated revolving doors, ID card readers, and keypads are all used, oftentimes in conjunction with each other, to prevent unauthorized people from entering the government or corporate locations. This is very different than universities as anyone can enter into almost any building with little or no controls stopping them. If there are controls, like ID cards, they can easily be circumvented by following someone else in, for example.

Finally, the tools that are put on the networks themselves are configured in such a way that is much more locked down and controlled than those in academia. Tools are put in place to not only monitor the activity on the network for nefarious or abnormal activity but they're also put in place to *stop* certain actions. An example of this is preventing people from uploading files to cloud data hosting providers like Dropbox or Google Drive as well as preventing them from accessing outside email or even sending attached emails using work accounts to outside email addresses. All these controls are designed to keep data within the environment and prevent unauthorized data from leaving it.

Government, because of its stated mission of keeping nation security and technical data secret, can and does lock down their environments using many more tools and procedures than academia. Secrecy, as was stated in chapter 2, is built into how government operates and this translates to how they control the flow of information. It

was the same prior to the digital revolution and it's the same now in the age of the Internet. While it's true that governments, or even private companies, don't always secure their sensitive data appropriately. It is true that they have the mandate, capability, and the motivation to do so because it's ingrained in their purpose.

Academia is much different. From the beginning, their purpose has been to share information. The idea of preventing anyone, let alone a researcher, faculty member, of high-level administrative officer from accessing whatever kind of website, application, or data repository is anathema to their purpose. Even if universities *could* enforce the same draconian measures that governments and private corporations do, doesn't mean they *should.* However, as I'll show you in the next section, that opens up those academic institutions to much greater risk.

How attackers operate in academia – An example

This section is meant to be a hypothetical example of what could take place at Harvard, or any other academic institution. It uses real-world examples of common attacks and attack methodologies that are used by every cyber actor, including nation-states. It is not meant to be an indication of an actual event nor is it meant to spotlight Harvard or any other academic institution. I simply wish to contextualize how nation-states could exploit the open nature of any university.

Drawing on Harvard's open network architecture highlighted in Figure 4 and earlier in this chapter, let us presume that there is a new faculty member or researcher at Harvard. Let's call him John Harvard. Dr. Harvard is very much interested in pursuing

his academic and research endeavors while at Harvard. Part of that pursuit is creating a website where other researchers in other universities, government and non-government agencies, and private sector can collaborate on his research. Dr. Harvard was given a grant from the National Science Foundation but doesn't want to spend a significant portion of that hiring an outside technical person or company to help build the website with all its components. So John Harvard does what any intelligent and resourceful academician would do: he decides to build it himself using the many publically available documents and free software available online.

John Harvard orders a computer, download the software, and without too much time or effort has all the software and hardware components installed and configured to run the website. Now, all he has to do is get it online. Dr. Harvard decides to take the computer to his Harvard lab or office and plug it in directly to the jack in the wall. With only a couple of clicks and an automatic registration of the system using his Harvard credentials, the machine now has a valid IP address and is connected to the public internet. The website is up and running.

Now that he's able to pursue his research, Dr. Harvard forgets about the computer running in his office or lab. What Dr. Harvard doesn't know, not being a technologist or security professional, is that the software that allows him to run his website requires some maintenance. Because he doesn't take care of it or administer it in any way (it's up and running after all), the software quickly becomes out of date and now has several vulnerabilities that can be exploited. The more Dr. Harvard leaves the system running without updating it, the more vulnerable the system becomes. But since the website is running and Dr. Harvard is allowed to continue his research, he doesn't really care.

A nation-state actor, like many other cyber actors are constantly doing, is poking at Harvard's network looking for ways to get in. After some initial scanning, this nation-state actor, we'll call them Panda Bear, finds Dr. Harvard's publicly available website. Using free tools that can be downloaded online, Panda Bear begins to do some reconnaissance and realizes that Dr. Harvard's website is very out of date and has a lot of vulnerabilities on it. Panda Bear does a bit more reconnaissance to make sure that there are no red flags that could jeopardize this intrusion and then launches an initial compromise.

This initial compromise takes over Dr. Harvard's website and gives Panda Bear full access to the system that resides in Dr. Harvard's office or lab. Luckily, however, there is no sensitive data running on it. Dr. Harvard's research is not sensitive. Panda Bear is not dissuaded, nevertheless, because what Dr. Harvard's website has given them is a foothold into Harvard's network.

From there, Panda Bear begins doing some more reconnaissance by scanning inside the network for other systems that are vulnerable. After a bit of research, Panda Bear finds other systems that, like Dr. Harvard's website system, have vulnerabilities that can be exploited. Panda Bear runs the attacks and compromises those systems. This is what is called moving laterally.

One of those internal systems that were compromised was logged on to it by a privileged user with a privileged account. [36] Panda Bear is able to take that credential and break it so that they now have access to that privileged account. They then begin to see what that account gives them access to. As it turns out, the account they just

[36] See Definition of Terms

compromised is an account that gives them access to virtually every system on the network. This is what's called escalation of privileges.

Panda Bear then keeps moving laterally or jumping from system to system until they get access, using that same privileged account, to the system that stores all the username and passwords for all the email addresses at the Harvard Kennedy School. They then exfiltrate this data, target several key accounts from HKS faculty that are known to have connections within the Department of Defense, and get access to their email account. With access to these HKS faculty members email, they can start sending targeted attacks using emails that contain malicious code or malware to their connections in the Department of Defense. Given that the email is coming from a trusted sourced, namely an HKS faculty member they know, those Department of Defense people receiving the malicious email click on the links or open the attachments they believe are sent to them from the compromised HKS faculty member but is, in fact, Panda Bear. Their accounts and systems then become compromised and the entire attack lifecycle begins again in the Department of Defense's network.

This hypothetical scenario is designed to give you an idea of why and how a nation-state would target a university, like Harvard. This is just one scenario. An alternate, and likely scenario, is that, instead of pivoting into a governmental agency, like the Department of Defense, they pivot into a system that houses sensitive research data akin to the Manhattan project of our time. Instead of getting access to people, nation-states look for access to intellectual property in the form of research and development at universities. All this is to show that universities are softer targets but that have access to incredibly important people and data.

Chapter 8

What Can Be Done

In this chapter, I discuss several options for mitigating the vulnerability of University computer systems.

Critical Human Asset Classification Table

Many, if not most, universities generally have a good sense of where their sensitive data is. This is what a data classification table is for. It is designed to give people a sense of what sensitive data is, like social security numbers, financial accounts, and protected health information, and then designate the systems that process, house, or transmit that kind of data to be more tightly controlled and locked down. What universities don't have a good sense of, or even a standard classification table for, are the sensitive or critical human assets or research.

The first step in fixing a problem is being to identify what the problem area is. Therefore, universities need to put more emphasis on identifying who the critical human assets are that either have access to other critical human assets in government, NGOs, or the private sector, or, by virtue of their research, have access to critical intellectual property. Building that sort of classification table of critical human assets allows universities to begin addressing those human assets in a more comprehensive and holistic manner.

One way to start building that table or list is simply by looking at what's publicly available online. Searching school or departmental websites, Wikipedia, or even personal websites for previous high-level government positions, seats on important committees or foundations, pictures with high-ranking officials, etc. can give institutions a good sense of who within their environment may have connections that can be exploited by a nation-state. Often overlooked but equally important are the second-degree contacts to those critical human assets. People like faculty or executive assistants and teaching assistants or fellows often are just as important as the critical human assets themselves because of the level of access they have. Building them into that human asset classification table becomes important as well.

Outside of publicly available information, looking at funding is another way to build out the human asset classification table. As was seen earlier, the majority of academic research funding still comes from federal agencies like the NSF and the NIH. Universities have access to that kind of funding information. Being able to leverage that data and build out a list of where a significant portion of governmental funding is going can help identify the critical human assets that are doing sensitive or important research. Institutions can even go a step further and look at the grants themselves to get a better sense on what the research is and if it poses a risk to national security if leaked. Querying for key words like "nuclear", "stem cell", "artificial intelligence" and such can help narrow the list down and isolate the most sensitive or critical research.

Awareness and Education

Once a critical human asset classification table and list is developed, and those human assets identified, universities can begin to put controls around them. Without knowing who to protect, it becomes impossible to begin to get a handle on the problem. One of the most effective and least utilized ways of protecting is that of education. This paper argues for a more targeted awareness and education campaign for those critical assets that takes a more hands-on approach. Because these people have access to sensitive data and connections, it becomes paramount that universities take the time to properly educate them on the threats and the solutions. This requires a more "velvet-glove" or "hands-on" approach where university security officials sit down with the critical human assets and not just educate them but also go through the steps with them. All of the controls are simple ones that have been around for a while but are not used enough for lack of awareness.

Nation-states often use the same techniques that hacktivists and cybercriminals use for one simple reason: it works. There is no reason to spend a significant amount of time, resources, and money developing a unique solution when a more common and easy one will work just as well. The reason they work, however, is that people are unaware of the simple steps that can be taken to protect themselves from the most common attacks. In this paper I will highlight three.

Two Factor (Multi-factor) Authentication

One of the best protections for any account that uses a username and password is enabling two-step authentication. There are many names for it out there including multi-factor authentication and two-step verification but it all means the same thing. To authenticate into any system or application, there are there ways to do it: 1) something you know or remember like a username and password, 2) something you have on you like a fob or a phone, and 3) something that you are like a fingerprint or a retina scan. Multifactor authentication simply means using more than one, if not all three, of those methods to get access to a system or to data. If a password gets compromised, as in the hypothetical example in chapter 7, with multifactor authentication any malicious actor will not be able to get access to sensitive data or systems without the person's phone, fob, eye, or finger.

Password Managers

Because people have to remember so many passwords for the dozens of accounts they have, most of them use either a single password, a couple of passwords, or an easily guessed pattern of passwords in order to make it easier. This opens people up to risk because any data breach, like at Yahoo, that exposes passwords can then be used to pivot into more sensitive accounts. However, remember long, strong, unique passwords for every account becomes virtually impossible. This is where password managers come in.

Password managers are tools that are specifically designed to help people create strong, unique passwords for every account without having to remember them all. It does require a behavior change as it is a different way of logging into accounts and systems but the benefit is that a breach in one account doesn't put your other accounts or systems at risk. This paper will not go into how to enable or use password managers as there are many options that are used differently and, for this purpose, it doesn't matter which are used. What does matter is that every account and system is protected with its own unique password, using whatever tool or mechanism is most convenient.

Patching/Updating Software

Going back to the hypothetical example in the last chapter, the way that Panda Bear was able to get access to Dr. Harvard's system is through vulnerabilities or holes that can (almost always) be fixed or patched. Every time that an operating system, like Windows or Macintosh OS, comes up with a request asking for the user to install patches or updates, its most likely trying to fix a hole that was found in the software. All software, not just operating systems, has holes and its incumbent on the person who installed or owns the software to update and patch it. Making people like Dr. Harvard aware of the purpose of patching is paramount to ensuring that those vulnerabilities used by nation-states to get access to university environments are fixed.

Technical Controls

Outside of general awareness and education, once those human critical assets are known, technical controls can be put in place to augment the general education and awareness. Much of these controls will mimic existing government and private sector but the key is to balance those controls without impinging on the academic freedom, access to information, or general collaboration that is ingrained and a key to research universities. While there are many technical tools and configurations that can be put on a network, this paper will highlight two broad level controls that can be used as a foundation upon which to build further technical enhancements.

Network Segmentation

As was explained earlier, network segmentation is the idea of separating out a large network into different sections, oftentimes based on the kind of system or data that will be on that network. The reason is that it is far easier to control individual smaller networks than one big one. Furthermore, different controls and tools can be out on each network that can be customized to the kind of data and systems that are on it instead of a uniform, one-size-fits-all approach.

In this particular context, network segmentation can be used to separate out the critical human assets from all other users. By doing so, universities can better monitor, defend, and react to attacks on those critical users better and faster than the other networks. All universities have certain amount of cybersecurity resources and it's widely

understood concept that security professionals need to focus on critical assets. What this does is extend that basic principle to critical *human* assets by placing them in their own network that universities can better protect.

Endpoint controls

Following up the network segmentation control, universities can better help protect their human assets by installing software that better monitors and defends against malicious activity. Some of that is being done now but only on those devices that are managed by the university. Little is done for personal devices or devices that are bought with outside funds and are not managed by the central university IT department. The software would have to be configured in such a way to avoid the often-Draconian tools put on government and corporate devices but still provide valuable information that could either fend off an existing attack or warn the right people about an on-going one.

Final Thoughts

Universities have historically been centers of knowledge and information. This was true from the first research university in Berlin till today. It is no coincidence that virtually every universities' mission statement has something like "create knowledge" or "educate future leaders". Their purpose was, is, and will always be to develop knowledge and share it with whomever chooses to walk their hallowed halls. This purpose is quite different from that of government or private companies. From their perspective,

information, especially sensitive information, is something to be kept secret and protected, not shared. Prior to the digital revolution and the advent of the Internet, these two worlds existed in parallel yet retained somewhat defined borders. Once systems, and people, became connected, those walls virtually disappeared, and with it the protections that they provided.

In the current world of mass data and interconnectedness, universities need to play a more active role in protecting the data that they are so willing and able to produce, especially when it connects with government and national security. This means redefining what, or whom, universities need to focus on, and how they should go about it. This paper has sought to draw the connection between academia and government, expose the heightened risk with data being on the Internet, and highlight some general methods by which to mitigate some of that risk. It is meant to begin the conversation around how elite universities, like Harvard, should take the lead in protecting the important people and research that goes every day in their environment. For if they do not, these research universities not only put themselves, reputation, and their people at risk but the entire nation as well.

References

Altbach, Phillip G., and Jamil Salmi. *The Road to Academic Excellence.* The World Bank, 2012

American Association for the Advancement of Science. Retrieved from: https://www.aaas.org/page/rd-colleges-and-universities

Baraniuk, Chris. (2017, July 26). *It's a Myth That Most Cyber-Criminals are 'Sophisticated'.* Retreived from http://www.bbc.com/future/story/20170726-why-most-hackers-arent-sophisticated

Paul E. Ceruzzi. *A History of Modern Computing.* MIT Press, 2003

Denning, Dorothy. (2015, September 8). *The Rise of Hacktivism*. Retrieved from journal.georgetown.edu/the-rise-of-hacktivism/

Fallon, Daniel. 1980. The German University: A Heroic Ideal in Conflict with the Modern World. Boulder: Colorado Associated University Press

Gass, H. (2016, 02 29). *UC Berkeley breach: Universities increasingly targeted in cyberattacks*. Retrieved from The Christian Science Monitor: http://www.csmonitor.com/USA/Education/2016/0229/UC-Berkeley-breach-Universities-increasingly-targeted-in-cyberattacks

Glaser, A. (2017, July 27). *Here's what we know about Russia and the DNC hack.* Retrieved from Wired: https://www.wired.com/2016/07/heres-know-russia-dnc-hack/

International Traffic on Arms Regulations; Part 120, Subchapter M

Kaplan, F. M. (2016). *Dark territory : the secret history of cyber war.* New York: Simon & Schuster.

Krantz, L. (2015, July 01). *Harvard says data breach occurred in June*. Retrieved from The Boston Globe: https://www.bostonglobe.com/metro/2015/07/01/harvard-announces-data-breach/pqzk9IPWLMiCKBl3IijMUJ/story.html

Leiner, Barry M. (1997) Brief History of the Internet. *InternetSociety.org.* Retrieved from https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Longstaff, Thomas A, et al. *Security of the Internet*. Software Engineering Institute, Carnegie Mellon University: 2017

Matthew Lyon; Katie Hafner. *Where Wizards Stay Up Late: The Origins Of The Internet.* Simon and Schuster: 1999.

Morgan, Steve. (2016, January 17). *Cyber Crime Costs Projected To Reach $2 Trillion by 2019.* Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5873db5a3a91

The National Bureau of Asian Research. "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property". May, 2013.

Cass R. Sunstein, *Government Control of Information*. 74 Cal L. Rev. 889, 892 (1986)

Veysey, Laurence R. 1965. *The Emergence of the American University*. Chicago: University of Chicago Press.

Ramzan, Zulfikar *"Phishing attacks and countermeasures*". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer: 2010.