THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES & TECHNOLOGY

TRUTH, JUSTICE, AND THE INTERNET WAY:
SECURITY IMPLICATIONS OF THE ONLINE ACTIVIST MOVEMENT

ELIZABETH BRENNAN BARTELS
Spring 2012

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees
in Security and Risk Analysis and Information Sciences and Technology
with honors in Security and Risk Analysis

Reviewed and approved* by the following:

Gerald Santoro
Senior Instructor of Information Sciences and Technology
Assistant Professor of Communications Arts and Sciences
Thesis Supervisor

Peng Liu
Director, Cyber Security Lab
Director, LIONS Center
Professor of Information Sciences and Technology
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

The Internet revolution has led to the development of a parallel culture where the rules are different. Existing in a purely digital form, this cyber-culture has nurtured its own social systems that parallel social systems in the 'real' world. One important example, the hacker activist, or hacktivist, has emerged as a very real and growing threat to the confidentiality, integrity and availability of information and communication systems worldwide. This thesis examines the phenomenon of hacktivism to reveal its methods, motivations, and implications for cybersecurity professionals.

TABLE OF CONTENTS

LIST OF FIGURES

Introduction

The digital revolution has led to the creation of an entirely new "cyber" culture. The Internet has become a world in its own right, with its own citizens, rules, and negligible boundaries. The Internet exists in sync and coordinated with the non digital world; many of the real world interactions that we take for granted have online analogs. As more and more people gain access to the Internet and become more technologically capable, and as corporations, governments, and other entities increasingly turn to an online presence, cyber culture grows significantly. This growth heavily reflects its roots in offline society. One such movement that sprang from this growth, ideological hacktivism, has exploded into the public awareness as the media increasingly covers the activities of an expanding activist hacker community. Recent reports published on the state of the cyberworld and its security have begun to point to the trend as one for cybersecurity professionals to watch and anticipate. The purpose of this thesis is to examine and shed light on hacktivism, and discuss the implications of this trend for cybersecurity professionals as well as the rest of the world.

The term hacktivism ("hacker activism") stems from the recent trend of hackers to use direct action in the Internet world to expose, draw attention to, or otherwise act to support an ideological cause, and through this bring awareness to the cause. Their uniqueness stems from two sources: their identity and their motivation. Hacktivists are not state-affiliated or state-sponsored in any way, nor are they out for political, martial, or economic gain. Often hacktivists start out as, or affiliate themselves with, cybervandals, who typically aim to deface websites and perform other acts of irrational vandalism in order to obtain recognition.

Who are Cyberactivists?

To understand the unique position that the hacktivist element occupies, is important to note the wide variety of internet citizenry. It takes all kinds to make a community, and like every place humans inhabit, the internet contains a deviant element. The deviant elements can be separated into several categories of cyberactors and cyberactivity. While the distinctions are not always hard and fast, it is important to understand what makes hacktivism stand out from other cyberactivity on the internet; most media fail to distinguish between types, either lumping all forms of deviant cyberactivity into the same category or inconsistently characterizing the cyberactivity.

Hacktivists remain unique in their cyberactivity because their primary distinguishing factor is that they are socially motivated. Although often lumped with cybercriminals and cyberterrorists, they are not acting for monetary or political gain, or specific revenge. To this end, many hacktivist groups attempt to portray themselves as defenders of the weak and innocent, as vigilantes who fight for those who cannot defend themselves. The fact that they must sometimes commit illegal activity to do so allows Hacktivists to further paint themselves as the anti-heroes of the Internet: fighting for truth, justice, and their way of life. This self-characterization has strong parallels with social activists, who sometimes commit crimes as well to defend their beliefs and organizational sense of morality.

Table 1: Cyberactivity Types

Cyberactivity Types		
Type of Cyberactivity	**Cyberactor**	**Motivation**
Cyberactivism (Hacktivists)	Individuals	Social Activism / Bring Awareness to Cause
Cyberespionage	State-Sponsored Actors	Political Gain/ Economic Gain / Strategic Gain
Cybercrime	Corporation-Sponsored Actors	Economic Gain / Corporate Advantage
	Individuals / Criminal Enterprises	Monetary Gain
Cyberterrorism	Individuals / Groups	systematic use of vandalism and intimidation to achieve some goal
Cybervandalism	Individuals	Skill Recognition / For Fun
Cyberwarfare	State-Sponsored Actors	Military Advantage

What do Hacktivists do?

Generation of support and awareness of a hacktivist cause is usually accomplished by its advocates in three ways: deface, disrupt, and distribute. First, hacktivists deface websites and web applications in order to bring attention to their cause. Often hand in hand with that comes their second method: disrupting the cyberservice. By bringing down the web service of whatever or whomever they are protesting against, while also defacing the website associated with what is under protest, they can bring attention to their cause most handedly. Finally, hacktivists seek to gain access to, and distribute, information that could bring public attention to their cause or weaken the standing of their opponent. This information is often usernames and passwords or specific personal information about members of an organization.

In order to understand how the trend of hacktivism has experienced such rapid and steady growth in recent years, it is important to consider the most common methods currently used by hackers: the denial of service attack, SQL injection, and social engineering (iMPERVA, Verizon RISK Team). Comprehension of these definitions aids in the understanding of how past hacktivist actions were executed. These methods, widely acknowledged by cybersecurity professionals, continue to be problematic for two reasons. First, instructions and how-to manuals on these techniques are widely available, making hacking anyone's game. Secondly, and much more importantly, however, is the fact that the people who create the systems attached to the Internet are not testing, managing, or securing these systems. Security management is still an art rather than a science, and often ineffectively deployed. Effective cyber-security continues to be a challenge for most organizations.

A denial of service attack, as the name suggests, is a hacker exploit aimed at disrupting the website or service, either temporary or permanently. A common method is for hackers to overwhelm the target machine with communication requests, causing it to be either unable or very slow to respond to any legitimate communication requests it might also receive. Denial of service attacks are easy because a flood of communication requests can be created by an action as simple as accessing a website many times over (Patrikakis, Masikos, and Zouraraki). Denial of service attacks are carried out by many different deviant elements of the Internet world; hacktivists generally use denial of service attacks to make inaccessible websites or services of companies, individuals, or government entities that they are protesting the actions of. Generally these attacks are announced within the hacktivist group to ensure the effectively of the attack, as these attacks require the mass action of many systems at once. Statements to give the particular hacktivist cause publicity generally accompany these attacks. Denial of service attacks, like many common hacker exploits, are prosecutable under U.S. Federal Law (18 USC Sec. 1030).

SQL injections are a technique designed to exploit security flaws in a website in order to gain access to, modify, or destroy parts or the entirety of a website's database. In this type of exploit, hackers exploit the vulnerability when websites do not properly filter user input to only allow specific types. If the vulnerability exists on the site, hackers can type SQL commands into any user input field and gain direct access to the database of an application. This attack is often used to gain information such as usernames and passwords as well as other personal information for distribution (Junjin; Kieyzun et al.).

Of the methods hackers use, the least technical is social engineering. Social engineering is the manipulation of people to either divulge information or carry out certain actions. According to Kevin Mitnick, an infamous social engineer, it was very easy- he "could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it" (Mitnick, 2002).

Many security professionals consider the user to be the most vulnerable part of any system, and rightly so; human instinct is to trust and give information to those who appear to have the proper right to that information. One type of social engineering is phishing, a practice wherein users are widely targeted through fake, yet authentic looking, e-mails requesting sensitive information. Often hacktivists use a more high-level version of phishing, spear-phishing, which is when specific people are targeted for their information, and the attacks are tailored to obtain the information they want. This information may be as specific as a password to access the system, or as general as a supervisor's name in order to continue the attack upwards. Social engineering is the hardest of all methods to safeguard against because it depends heavily on user awareness and alertness (Allen).

Research Objectives

It is important to comprehend the development of the hacktivist culture and mindset in order to examine the implications of this emerging trend for both cybersecurity professionals and for the public at large. Examining the historical trends of social activism gives a similar roadmap to compare with the current hacker activist movement. By combining this with academic and media viewpoints, this thesis establishes current perceptions on hacktivists. Examining these perceptions allows cybersecurity professionals to understand how the public, including those responsible for the funding of cybersecurity, view hacktivism.

This thesis will examine the history of the evolution of hacker communities and their activism roots further allows the paper to examine the development of the hacker and digital social activist community in order to further understand what direction this emerging trend is heading. After examining hacktivism as an emerging trend, this thesis will focus on the implications of said trend for cybersecurity professionals and the public as a whole. This thesis will conclude with a summary of key findings and suggested solutions to tackle the developing trend.

Perceptions of Hacktivism

One of the most valuable perceptions that literature on hacktivism has graced the academic community with is the name hacktivist itself. It accurately conjures up the parallel between the online movement that exists today and the activists of the non digital world. In many ways, the growth and development of activism offline created, influenced, and interacted with the hacktivist movement. Movements such as Students for a Democratic Society used a combination of low key, socially approved tactics such as the publication of literature and flyers about their causes, and newer, more controversial tactics such as sit-ins and non-violent protests to get their point across. Throughout the 1960s and 1970s, these movements became more and more radical. Students for a Democratic Society eventually folded and in its dust rose the Weather Underground, a more radical group intent on getting its message across through bombings and robberies.“There is no example of a peaceful road to fundamental social change,” one of the group’s co-founders declared (qtd. in Suddath). Academic and media sources did not know how to handle these groups; they were torn between covering them as fighters for change and as terrorists (Suddath). This confusion has carried over into the coverage and perceptions of the hacktivist movement.

Hacktivism in Academia

Perceptions within academia have been mixed as the phenomenon receives more media and public attention. Academia is attempting to feel out the beginnings of research on hacktivism, sticking to smaller definitions and dissecting their movements in anticipation of larger research down the road. Each researcher approaches the issue of hacktivism slightly differently. In a research article published in *Computer Fraud and*

Security, Tim Jordan divides the actions of hacktivists into two separate categories: mass virtual direction actions (MVDA) and individual virtual direction actions (IVDA). MVDAs are the simultaneous digital actions of many protesters across the internet, while IVDAs are actions that do not rely on mass action and can be undertaken by an individual. Both forms of protest, and their nomenclature, are linked to the offline protest movement of the 1990s. This research supports the establishment of hacktivists as their own separate entity within the Internet society, establishing their electronic civil disobedience as a growing trend while also warning of the complicated nature of the hacktivist groups (Jordan).

Academics have also chosen to examine the potential staying power of the hacktivism movement. Paul Taylor argues that the social construct's reliance on the technological infrastructure of the internet and speed of word of mouth is a pitfall that might prevent hacktivism from every truly realizing its full potential as a radical social movement. However, he also points out that the true advantage of hacktivists is that they are part of a movement that understands the potential of combining traditional resources and causes with technology-based techniques and outreach. He chooses to keep his conclusions inconclusive, instead spending time focusing on the fact that hacktivism is a double-sided sword, with great potential but great problems to overcome, and points out that the newness of hacktivism makes it difficult to predict the prospects and nature of the movement going forward (Taylor).

Other academic research has focused on whether hacktivist actions can truly be defined as electronic civil disobedience or if it is terroristic in nature. In order to align with other actions of civil disobedience, Mark Manion and Abby Goodrum concluded that hacktivism must act within five conditions: The attack must cause no damage to persons or property, must be non-violent in nature, not for personal profit, have a strong underlying ethical motivation, and the hacker must be willing to take responsibility for the outcome of their actions (Manion and Goodrum). This conclusion struggles with the same issues that policymakers face when determining how to categorize actions by non digital activist groups, particularly activist groups of the 1960s and 1970s.

Hacktivism in the Media

Unlike academia, the media is less concerned with the how and why of the development of the movement, and more concerned about the potential impact hacktivists will have on the common person. Within the media there seems to be three perceptions of hacktivist activity: cyberactivists are not a significant threat, a threat to the individual, or a threat to the nation as a whole. Even those that think hacktivist groups like Anonymous are not a significant threat acknowledge their ability to wreak significant havoc both on and offline, but these articles are less likely to see hacktivism as a concerning trend capable of causing fundamental damage (Kearney).

The second focus that the media takes is on the victims of hacktivists more than the social construct of the group; one article warns readers that “even if you haven’t done anything obvious to provoke it, you could still be the victim of a highly-skilled attack against your infrastructure, your personnel, or your information assets” (Weir-Jones). These types of articles are reaching out to the individual reader and presenting the possible threat of hacktivism on a very personal level, unlike the third level, which focuses on the threat hacktivism presents on a larger scale. These articles look at the threat hacktivist groups present towards national targets such as the US Infrastructure, rather than the individuals (Schwartz).

The interesting thing about the media’s perception of hacktivist groups is that they tend to lose sight of the fact that cyberactivists can be all things at the same time. To some who have proper precautions or who do not engage in activities that would provoke protest, hacktivists are no threat. All individuals who maintain a presence in cyberspace risk the danger of having their information stolen or leaked, or their identity attacked. And national structures with cybercontrol mechanisms can also be targeted. Only by combining these perceptions, and examining the academia's concerns and thoughts as well, is it possible to get a complete picture of the emerging hacktivist trend.

Evolution of Hacker Communities

Although it is only recently that hacking has come to such prominence in the national media, hacking communities have been around since the creation of machines that communicated electronically. Some go so far as to claim that the first hack was in 1903, when a man by the name of Nevil Maskelyne hacked a telegraph demonstration to illustrate security flaws in the system (Marks). However, the modern hacking movement is more clearly tied with the development of the phone phreaking community.

Phone Phreaking

In the late 1950s and early 1960s, major telecommunication groups such as AT&T converted their telephone switches to full automation. This automation allowed people familiar with the how the system worked to exploit this automation and place free phone calls. At this time, long-distance phone calls were still very expensive, so it incredibly advantageous for those in the know—phone freaks, or phreaks, as they called themselves. As they explored the phone network, they developed personal relationships with the other phreakers, communicating through conference call circuits and newsletters (Orth).

The practice really took off in the late 1960s and early 1970s, with many counterculture groups embracing phone phreaking as a way to buck authority. The Yippies started a magazine called the *Youth International Party Line* (later the *Technological American Party*), aimed solely at using technology to exploit automated systems and obtain free services illegally ("Technical American Party (TAP) Subversive Matter"). Around the same time, magazines and news articles also began to draw new attention to the movement, leading to an increase in phreaking community size (Orth; Rosenbaum, 1971). Several early members of the personal computer movement, including Steve Jobs, would later credit their exposure to phone phreaking through these media sources with their later successes. With the advent of personal computers in the 1980s, some phreakers started to adventure into the world of networked computers and their vulnerabilities, in the same way they had earlier explored the telephone network (Rosenbaum, 2011).

The Hacker Hero in Film

In the same way that the media brought new members to the phone phreaking community through its magazine articles, films were on the frontlines of mainstreaming hacking among the technologically adept. The films, in most cases, not only glorified hacking, but made it cool. In 1982, *WarGames* led the charge with its protagonist David Lightman, who easily hacks into the US Government's computer systems and then spends the rest of the movie trying to prevent nuclear warfare with his computer skills (WarGames).That same year, the movie *Tron* was released, featuring a plot where a computer programmer must use his skills to triumph against the evil computer programs and a fellow programmer trying to steal his work (Tron). Both films were box office successes, and hacking burst into the public eye.

The trend continued strongly through the 1980s and into the 1990s, with movies such as *Sneakers* being released, featuring a team of computer security experts who must match wits and hacking skills against personal enemies and a government intent on spying on itself (Sneakers). The defeat of the alien invasion introduced in the film *Independence Day* depended heavily on the creation of a virus to attack the alien's network (Independence Day). These films all popularized a perception of the hacker as the heroic or anti-heroic figure, defending themselves, the United States, and even the World from great threats such as death, nuclear war, an invasive government, and aliens.

In many cases, the hacker of film used unorthodox—and sometimes illegal—methods, in the pursuit of what films portrayed as the defense of the greater good. Film, and through film, society, started to embrace a new form of hero that used a cybertoolkit.

Early Computer Hacking Communities

The rising of hacking in popular culture expanded the community brought together a myriad of people from all walks of life. Many early hacking groups, however, were former through physical proximity rather than any digital affinity. The 414s, one of the first hacking groups to be targeted by the FBI after breaking into some 60 computer systems including Los Alamos National Laboratory in 1983, were all from the Milwaukee area. The Legion of Doom was primarily American hackers, while the Chaos Computer Club's membership came from Germany. Many hackers communicated through Usenet, a popular Internet discussion forum ("The History of Hacking"; "Timeline").

Hackers continued to publish and spread their knowledge, turning to ezines to create articles about vulnerabilities that could be exploited, international news, and, most telling, themselves. One of the earliest ezines was Phrack, first available on a message board in 1985. The zine, still in operation today, is perhaps most well known for publishing "Hacker's Manifesto", a short essay that many hackers continue to embrace today. In many ways, it characterizes the hacker as the anti-hero, claiming a moral ground for hackers above and beyond world government and laws, as it declares defiantly:

> "This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for

> what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.
>
> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for" (The Mentor).

This manifesto portrays hackers as above violence and selfish desires, and points to their use of technology as a way to expand horizons and keep the world free. This attitude continues to be present in many hacktivists today (Thomas).

By 1990, US authorities were starting to take notice of these hacking organizations, leading to Operation Sundevil the first large-scale operation aimed at hunting down hackers ("Timeline"). Throughout the 1990s and early 2000s, hacking became more and more popular, in part due to the rising popularity of personal computers, and in part due to the new access that the World Wide Web (WWW) provided. Prior to the World Wide Web protocol being introduced, internet users communicated through the text-based Usenet groups on the Unix-to-Unix Copy (UUCP) protocol; the World Wide Web protocol was a graphical interface that made the Internet even easier to navigate. With the introduction of the Mosaic browser in 1993, the Internet's popularity, and with it, the hacking community's population, soared (Stewart).

Anonymous

One of the most commonly linked names to hacktivism is Anonymous. Often characterized as a hacking group by the media, Anonymous is a decentralized, online collective acting anonymously in somewhat coordinated actions towards a loose set of goals. The collective's name originated as an internet meme, a concept which spreads across the subcultures of the internet; because many message boards allowed users to post anonymously under the pseudonym Anonymous, users found it amusing to refer to all Anonymous posts as Anonymous was a real person or being. Users on the website 4chan's random board, /b/, are identified as among the first to embrace the collectivity of the name Anonymous. Concealing their identity allowed anyone and everyone to become a member of Anonymous; by 2005, users had embraced the Anonymous concept as a hacker collective (Anonymous, 2011; Davies).

Rise of Anonymous

Early Anonymous activity had a "do as you wish" atmosphere, with many people using the moniker for a varied span of exploits. By 2007, however, Anonymous began to make a name for itself as a proactive group working for the people of the Internet with its first major protest action against the Church of Scientology (Anonymous, 2011). "[The Church of Scientology] attempted not only to subvert free speech, but to recklessly pervert justice to silence those who spoke out against them", one hacker acting for Anonymous claimed (qtd. in George-Cosh). Prior to the campaign, several individuals posted warnings against the Church, with statements boldly declaring "For the good of your followers, for the good of mankind--for the laughs--we shall expel you from the Internet" (Anonymous, 2008). This campaign also saw the first wide use of the quote that would become the rallying cry for every hacktivist action undertaken under the Anonymous group name:

> "Knowledge is free.
>
> We are Anonymous.
>
> We are Legion.
>
> We do not forgive.
>
> We do not forget.
>
> Expect us" (Anonymous, 2008).

Their protests took both digital and physical form, with denial of service attacks shutting down the Church of Scientology websites while internet denizens took to the streets and protested outside of Scientology establishments. The effectiveness of the denial of service attacks, some believe, was due to the use of harnessed botnets that added additional firepower to the activists' arsenal (Kaplan). To the hacktivists, the attack on the Church of Scientology was the first battle in their war on information suppression, and their early successes and public exposure attracted many new members and drove their attention to new causes.

The Vigilante Mindset

Hacktivists tend to associate themselves and their methods with fictional vigilantes with whom they feel they share common mission elements. Perhaps most prominent of these figures is V, from the comic book series *V for Vendetta* by Alan Moore. The story centers on an anonymous masked man, V, who fights for political reform and change in a future where the government ruthlessly restricts free thinking and speech. To hacktivists, it promotes the idea that one person can influence and bring about real change, and many focus on the fact that V's main concern lies with the freedom to spread ideas, thoughts, and actions. In particular, the Guy Fawkes mask that V wears in the comic has become a symbol for the group Anonymous; members often wear the mask when protesting in the non-digital world to protect their identity and emphasize the idea that they stand as one together. Members of Anonymous relate with V's fight for freedom of action and information.

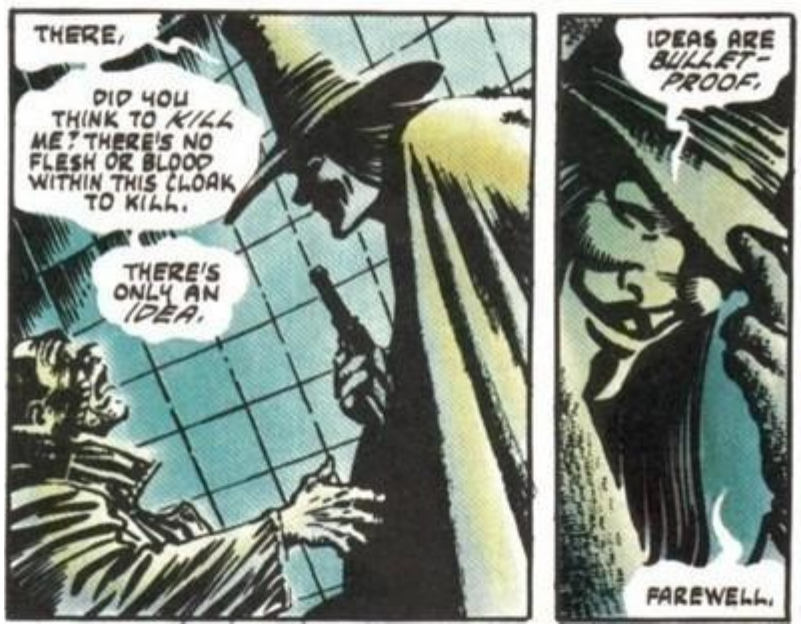
THERE,
DID YOU THINK TO KILL ME? THERE'S NO FLESH OR BLOOD WITHIN THIS CLOAK TO KILL.
THERE'S ONLY AN IDEA.
IDEAS ARE BULLET-PROOF.
FAREWELL.

Figure 1: Panel from *V for Vendetta* often used by members of Anonymous (source: Moore)

V is an interesting character for the hacktivist community to wish to parallel, because the comic also reveals a different interpretation of the hacktivist actions. One man's freedom fighter is another man's terrorist, and *V for Vendetta* makes that clear interesting twist: the character V, the lone and powerful voice fighting against a corrupt government, is insane, and many of his methods are as cruel as the government he is fighting against. V is the quintessential anti-hero to many hacktivists, and in many ways they attempt to emulate him. They see the Internet as their territory, as theirs to defend, and, more recently, to police.

This vigilante mindset can be seen in many of the causes Anonymous touts. While Anonymous does often attack groups and corporations they see as restricting the Internet or human beings in some way, they also do fight against certain socially deviant actions. The same week that Anonymous moved to release information about Boston police in protest of their treatment of Occupy Boston protestors, they also fought to take down servers they alleged had hosted child pornography. They also published the information of the almost 1,600 active users of another child pornography site. They followed their attack with an anonymous press release decrying all who support child pornography, signing off with their We are Legion group statement (Fogarty; Kelly). The dichotomy of these two actions reveals the presence of a self-imposed ethical guidance system within the mass of users and supports the vigilante parallel; they may not always act within the laws of the government, but they support and act within the laws of society.

Flash Mob Hacktivism

Hacktivism is not limited to large groups with staying power like Anonymous; some of the most significant cyberactivist actions have been through flash mob hacktivists, groups that are created for the sole purpose of one series of attacks, and then dissolve just as quickly as they first appeared. These hackers are using their hacking as a form of activism, but strictly in the sense of a one-time event, and not a loosely formed continually existing organization like Anonymous. These flash mobs are generally reactionary to specific events.

In 2007, the country of Estonia had one of the most technologically advanced infrastructures in the world. Citizens depended heavily on the Internet for financial and government services: even their student-teacher conferences took place online. Estonia did not, however, define their Internet systems as critical infrastructure, and was missing heavy-duty defense mechanisms or emergency response systems in place to defend against any attack on their systems. This was generally not problematic for the country until the government decided to move a statue of a Soviet soldier from a prominent position in the capital to the outskirts of the city. Russians were outraged at the announcement. As riots began in Estonia's capital, a series of Russian bloggers and forums planned a digital response as well (Davis; Evron, 2008).

Aided by detailed and easy to follow instructions, as well as a detailed list of intended targets, hackers quickly took Estonia's websites and mail servers offline. Government services, schools, banks, and news outlets were all targeted. Attackers worked within their own individual systems and used botnets to create the maximum possible impact on the systems. During the digital attack, Russian language blogs continued to update the status of their successes and post new targets for protestors to focus on. While unprepared for the strength of the digital movement, Estonia eventually did mount a defense and regained their position in cyberspace, and the movement dissolved as quietly as it had began. No one has been able to pinpoint the origin of the digital movement, but it was picked up by many independent bloggers and Russian language message boards. Users successfully formed a well-organized hacktivist group for a single cause, and then dissolved back into their previously present subcultures on the Internet in a clear example of an Internet flash mob (Evron, 2008; Evron, 2009).

Hacktivist attacks can, and do, increase political tensions. In the aftermath of the Estonia attacks, Russian-Estonian relations became more strained then they were previously (Evron, 2008). This has also been the case in the escalating hacktivist war between supporters of the country Israel and other Arab nations. Citizen hackers have taken it upon themselves to engage in a series of cyberattacks, defacing or shutting down websites for government offices, hospitals, stock exchanges, and other country-affiliated services. When one affiliated party attacks, the other retaliates. These hostile actions, undertaken independently by citizen hackers on behalf of their respective countries, are hacktivist in nature. However, the governments they are antagonizing do not necessarily see it as such; attempts have been made to label the cyberactivist actions terrorism, a move that would only increase tensions in a way that only declaring another country's citizens terrorists could (Clarke).

Independent Actors

Hacktivists do not have to be organized in a group. Generally, they are, due to the nature of what they protest against, and because as they publicize their cause more participants tend to want to join. However, there have been cases of individuals working to bring awareness to a cause through hacking. In 2011, a Swedish hacktivist released the usernames and passwords of over 90,000 people who used one of the country's most popular blog portals (Harding). According to interviews, the hacktivist took action to remind people to change their passwords, stating "I dumped this information to let people know that they handle their information wrongly. Many web pages are not up to scratch. And consumers need to know they should never use the same [passwords] for different services on the web" (qtd. in Harding). This attitude is reminiscent of many hacktivists, who often claim that their attacks are to protect the information and rights of the common denizen of the Internet.

Implications for Cybersecurity

Many of the threats to a site's security from cyber activists are from smaller exploits; any and all websites and services are at risk because it is impossible to anticipate what will come under protest, as groups like Anonymous illustrate. While many of their methods may seem fairly harmless, hacktivists are one of the largest emerging threats to come from the Age of Information. While they are not currently the largest threat, cybersecurity policy necessitates a focus on issues such as hacktivism that draw public awareness ("Hacktivist Groups"; Schwartz). The focus that the public has given this issue is, in many ways, a positive one. Many of the hacktivist attack methods, particularly the common ones such as SQL injection and denial of service attack, are used by other members of the Internet deviant community. It is necessary to start small and ensure the more obvious vectors of attack are covered before moving on to focus on more complicated methods. Additionally, any focus on an issue that ultimately concerns cybersecurity, as hacktivist actions ultimately do, means more awareness about the need for cybersecurity, in turn leading to more funding. Hacktivists, after all, are oftentimes that most well-known part of the digital deviant community because their work, unlike the others, demands public exposure.

A large part of the risk of hacktivists comes not from what they intend to be their direct action, but the collateral damage. Social activism catches not only the targets of their ire, but many innocent users as well. Real-world implications for online actions can cause damage that in some ways, particularly financially, could possibly exceed any impact non-digital activism ever had. This is especially true of the hacktivist tactic of disclosing information. A real world thief needs to have physical proximity to the item he intends to steal; a digital thief only needs to be within logical proximity. Short of locking an off computer in a cabinet and never using it, it is impossible for a cybersecurity professional to prevent all possibility of logical access to a digital item. This is problematic to consider, particularly because on the Internet, information is everywhere—and that's mostly what hacktivists are out to get.

The information they are obtaining is not a set of Watergate tapes. It is gigabytes upon gigabytes of information. And in their haste to release that information to the public, in order to bring support to their cause, there is no way for hacktivists to sort through every piece of data they are releasing—this means that the information they are obtaining not only harms their intended attack target, but also can, and does, generate serious collateral damage. For instance, an attack by Anonymous on a law firm that defended a marine accused of killing civilians in Iraq resulted in the release of the law firm's e-mails. These e-mails included witness statements in a non-related rape case which identified by name the previously unnamed rape victims, as well as other legal documents of clients unrelated to the purpose of the Anonymous attacks (Cook).

Defacing or disrupting websites can also do their fair share of collateral damage; it can result in a loss of confidence in a corporation or government agency, leading to downsizing, financial difficulties, and even corporate shutdown. Other hackers in the deviant community have already attacked parts of the U.S. infrastructure—including power plants, and other physical systems (McGlaun; Nakashima). The methods are already established—it's just a matter of time until hacktivists have a motive that would lead them to a similar path of action. The Information Age has lead to the internet becoming an integral part of every second of our lives—it manages our social calendars, communications, news, bank accounts, and stock market exchanges, among other things—and this means that what impacts the digital world can easily crossover to the real world. Over four billion people use the Internet on this planet, and each and every one of them is generating new information every time they launch their browser. Some of those people need help protecting their pile of information and digital lives from breaches—others are contemplating which tool to use to cause the breach. A recent study revealed that out of the 177 million personal records stolen by hackers in 2011, 100 million (56%) were stolen by hacktivist groups (Greenberg).

The reality of the emerging threat coming from internet social activism shows the great need for security. It is not a matter of debate over the morality of hacktivism; in the end, cybersecurity professionals need to confront the movement in order to do their jobs. Internet social activism has revealed that a greater emphasis is needed on information security measures. Even if a firm is unlikely to be a target, security still has a vital place in their business plan; proliferation of networked systems with little or no security leads to botnets, which have played an increasingly large role in cyberactivism. Security experts also need to monitor the actions of hackers to determine the threat to the individual organization as well as to network security as a whole. According to Verizon, in almost 75% of hacktivist attacks, the target is warned beforehand that it will be targeted (Greenberg). In the case of the hacked law firm, tech news organizations were aware that Anonymous intended to, and had, hacked the law firm before the firm itself was aware of it (Biddle).

Conclusion

Hacktivism is a very relevant, emerging threat to digital security. Real-life protester predecessors of online activists have shown that action that appears non-threatening can explode; hacktivism appears to placing itself on a similar track. Hacktivism can also lead to escalation of political tensions, and possibly even state-sponsored cyberactions. Cyber social activists are becoming more and more prominent, and they are part of a social movement that is here to stay and only going to get larger over time. That is why it is vital to examine this emerging cyberthreat, which has many of its roots in historic social activism, and discuss implications for cybersecurity professionals and the rest of the world.

There is no easy way to address the cyberactivism trend; addressing their actions necessitates stepping into a moral quagmire that has no escape—their points may present some validity but their online actions have real life implications that call for action to be taken by cybersecurity professionals to secure and protect individuals and organizations from harm on and offline. The issues that hacktivists raise indicate that there is a need for social, legal, and digital reform.

Social Reform

In the here and now, though, perhaps the most important thing to focus on is social reform. Lack of security is the pandemic, but if the public is not aware of this issue, then it is impossible to take the steps to fix it. Legal and digital reforms are dependent on public outcry to gain support from public figures. The first step, therefore, is education. It is necessary ensure the public is aware of several facts:

List 1: Facts needed to inspire cybersecurity social reform

1. The current state of their personal security
2. How to improve their security to a basic cybersecurity industry standard
3. How their security relates to national security
4. The illegal nature of hacktivist groups and their activities
5. The importance of cybersecurity

The five facts would bring highly increased awareness on the part of the public for matters of cybersecurity within the nation and allow people to take part in proactive measures. It shifts some of the burden off cybersecurity professionals and lawmakers, and into the hands of the people they are trying to protect. It’s important that users be taught about what they are exposing themselves to; even requiring basic security education in schools, teaching basics such as strong passwords and updating antivirus can improve the state of the digital environment cybersecurity professionals must protect. Security education also needs to be carried over to the private sector. Companies need to realize that appropriate allocation of resources to cybersecurity initiatives is necessary. Additionally, security needs to be made user-friendly. Right now, it is difficult to discern what the best tools and practices are for the average citizen. There are many free anti-virus and anti-malware programs on the Internet; it would be very simple for a government agency to purchase the rights to some of the software and package it together to make it easier and more convenient for users to install and use to secure their computers.

Legal Reform

Security is currently in the hands of the individual and private companies, and is, as the amount of breaches shows, often poorly managed or severely underfunded.

Security, often viewed as secondary and the unfortunate add-on to business strategy, is not getting the attention it deserves. In many cases of hacks where personal information is lost, the first effort of a company is to protect its reputation, not fix the vulnerability that caused the leak in the first place. As a result, it is necessary to start to engage in a discussion about the responsibility of the government to ensure that its citizens are protected online as well as offline. Members of the legislature have begun to pick up on the need for a more cohesive national cybersecurity policy, proposing, among other things, bills that include measures that would make the Department of Homeland Security responsible for parts of national network security ("FISMA 2.0"). However, these bills tend to address only the cybersecurity of the national infrastructure. To properly defend and safeguard all of the nation's networks, a more proactive stance needs to be taken.

The lack of cybersecurity is, and should be treated as, a pandemic. Currently, it is clear that security at the hands of the individual and private company is ineffective. The United States government needs to "inoculate" its networks and interests against at least the most basic threats. One way to insure that networks and interests were properly secured would be to introduce state-sponsored security measures. Creating regulations to require ISPs to provide quality anti-virus and anti-malware services would be a good start. There is already a precedent for the creation of regulations and laws that mandate a measure of information security; the Health Insurance Portability and Accountability Act of 1996 [HIPAA] requires all organizations handling patient records to implement certain technical security measures to protect that information. Furthermore, HIPAA allows the government to implement security for individuals that are required to and want to but are unable to do so (Health Insurance Portability and Accountability Act of 1996).

Funding is also an important part of a proactive stance on improving security to be able to hand cyberactivity like hacktivism. Additional studies are needed to examine the emergence of hacktivists and how to deal with the groups. Funding should also be allocated to researching how to improve current security mechanisms and disperse them into the community. Finally, funding from the federal government could aid in social reform, which needs money in order to be enacted.

While working within the government to provide more protection to United States citizens is vital, it is important to also acknowledge that no one government can improve cybersecurity on its own. In age of globalization, solutions for cybersecurity cannot be determined solely on a country-by-country basis, because the Internet is not bound on a country-by-country basis. In order to make sites and users more secure, governments must work together. The lack of cybersecurity is a pandemic not restricted by borders, oceans, or any other physical boundary. Although international cooperation is sometimes hard to secure, the creation of an international oversight group aimed at examining internet activities and security would be a beneficial start to engaging in a serious conversation about cybersecurity. In the long term, countries could even band together to use real-world tools like trade sanctions to ensure that cybersecurity regulations and "inoculation" attempts are passed. Precedent for international cooperation against deviant cyberactivities has already been established; the Council of Europe's Convention on Cybercrime is a treatise aimed at standardizing laws that define the offense of cybercrime, providing a way for countries to cooperate in the investigation of electronic crimes, and setting up a platform to ensure international cooperation. So far, over 30 states have signed and ratified the document ("Council of Europe Convention on Cybercrime").

Digital Reform

Laws alone won't ensure better cybersecurity. An examination of the lack of boundaries within the Internet, coupled with an attempt at creating boundaries, would be beneficial as well. Within our digital society, the presence of vigilantes, who see themselves as the sole enforcers of truth, justice, and the Internet way, indicates need for enforcement or monitoring agency on the internet to take away the need for these groups existence. Vigilantes gain popularity and support when they step in to do the job that is rightfully law enforcement's. Currently, hacktivist groups gain legitimization through their actions against the digital presences of child pornography distributers, puppy mills, and known malware sites. A more definite presence of law enforcement within digital society could take over those responsibilities and pull support away from hacktivists. It's the idea that if the police force in Gotham was effective at ridding the city of crime, there would less popular support for Batman; engineering it so that hacktivists cannot perceive themselves as vigilantes governing the lawlessness of the wild World Wide Web undermines their platform and could take away some of the participants in their actions.

There needs to be a breakdown of who is responsible for what parts of the Internet, including everything from the cables transmitting the electronic signals to the servers holding the information. It doesn't have to be clear cut—no doubt it wouldn't be, considering all the nations of the world would want a stake in it—but defining any sort of boundary would be a start. The first step, in many ways, has already been taken, with the establishment of law enforcement groups aimed solely at computer-oriented crime. It's a very long-term solution, but the end game is to shape the digital world to parallel even more distinctly the non digital world. By making online represent and connect to offline even more, you not only raise the stakes for creating secure environments, but create a greater sense of responsibility that is attached to each individual entering the cyberworld, and aid in taking away the mob mentality that makes hacktivists so effective in their current incarnation. It won’t eradicate hacktivism, not by a long shot, but it could go a long way to helping subdue the damage that the movement inflicts.

There are no ideal or simple solutions to approaching the issues of cyberactivism. The Internet may be very wild and ungoverned by today’s standards, but it belongs to the world, and as a result is very difficult to regulate, particularly by a government source. In some cases, there is no known solution to how to handle the issues. Further research and investigation into the hacktivist movement is necessary to figure out how to resolve the issues in a satisfactory way, while maintaining the security of individuals in the digital world and their ability to use the Internet as a forum for social cause and change.

Bibliography

18USC Sec. 1030. 2011. Web. 20 Mar. 2012. <uscode.house.gov>.

Allen, Malcolm. "Social Engineering: A Means To Violate A Computer System." SANS Institute. SANS Institute InfoSec Reading Room, Jun 2006.Web. 1 Apr 2012. <http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529>.

Anonymous."Anonymous and the global correction." Al Jazeera. 16 Feb 2011. Web. 17 Feb. 2012. <www.aljazeera.com/indepth/opinion/2011/02/201121321487750509.html>.

Anonymous."Message to Scientology" Speech. 21 Jan. 2008. YouTube. 23 March 2012.

Biddle, Sam. "Anonymous Leaks Marine Corps Massacre Case ." Gizmodo. Gizmodo, 03 Feb 2012. Web. 01 Mar 2012. <http://gizmodo.com/5882057/anonymous-leaks-marine-corps-massacre-case>.

Clarke, Richard. "Cyberattacks Can Spark Real Wars." Wall Street Journal. 16 Feb 2012. Web. 28 Feb. 2012. <http://online.wsj.com/article/SB10001424052970204883304577219543897943980.html>.

Cook, John. "Anonymous' Latest Release Includes Private Info About Sexual Assault Victims and Guantanamo Lawyers." Gawker. Gawker, 03 Feb 2012. Web. 26 Mar 2012. <http://gawker.com/5882150/anonymous-latest-release-includes-private-info-about-sexual-assault-victims-and-guantanamo-lawyers>.

Council of Europe Convention on Cybercrime, Nov. 23, 2011, Web. 28 Mar 2012. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

Davies, Shaun. “The Internet Pranksters Who Started a War.” MSN. 8 May 2008.

Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” Wired 21 Aug 2007.Web. 24 Jan. 2012. < http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all>.

Evron, Gadi. “Battling Botnets and Online Mobs : Estonia’s Defense Efforts During the Internet War.” Georgetown Journal of International Affairs (2008): 121. Print.

Evron, Gadi. “Authoritatively, Who Was Behind The Estonian Attacks?” Dark Reading Security. 17 Mar 2009.Web.14 Jan. 2012. <www.darkreading.com/blog/227700882/authoritatively-who-was-behind-the-estonian-attacks.html>.

"FISMA 2.0: Federal Information Security Amendments Act of 2012." Keep the Web Open. The office of Congressman Darrell Issa, Web. 20 Mar 2012. <http://keepthewebopen.com/open>.

Fogarty, Kevin. “Anonymous Attacks Cops, Declares War on Child Pornographers.” ITWorld 24 Oct 2011. Web. 30 Jan 2012. <http://www.itworld.com/security/216191/anonymous-attacks-copes-declares-long-term-war-child-pornography >.

George-Cosh, David. "Online group declares war on Scientology." National Post [Toronto] 26 Jan 2008. Web. 31 Mar. 2012. <http://web.archive.org/web/20080129063500/http://www.nationalpost.com/most_popular/story.html?id=261308>.

Greenberg, Andy. "Verizon Study Confirms 2011 Was The Year Of Anonymous, With 100 Million Users' Data Breached By Hacktivists." Forbes. 22 March 2012. Web. 26 Mar. 2012. <http://www.forbes.com/sites/andygreenberg/2012/03/22/verizon-study-confirms-2011-was-the-year-of-anonymous-with-100-million-credentials-breached-by-hacktivists/>.

“‘Hacktivist’ Groups Like ‘Anonymous’ Are Not the Biggest Threat to Cybersecurity, Says UB Information Assurance Expert.” *University of Buffalo NewsCenter* 2011.

Harding, Luke. “Hacker Leaks 90,000 Passwords as a Warning to ‘naive’ Swedes.” Guardian Online. 27 Oct 2011. Web. 12 Jan. 2012. <http://www.guardian.co.uk/world/2011/oct/27/sweden-hacking-twitter-hijack>.

Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191. 100 Stat. 2548. 21 August 1996. Web.< http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html>.

iMPERVA. *Hacker Intelligence Initiative, Monthly Trend Report #5*. 2011.

Independence Day. Dir. Roland Emmerich.20th Century Fox, 1996. Film.

Jordan, Tim. “Mapping Hacktivism Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) And Cyber-wars.” Computer Fraud & Security 2001.4 (2001): 8-11.

Junjin, Mei. “An Approach for SQL Injection Vulnerability Detection.”*2009 Sixth International Conference on Information Technology: New Generations* (2009) : 1411-1414. Web. 26 Nov 2011.

Kaplan, Dan. "DDoS hack attack targets Church of Scientology." SC Magazine. 25 Jan 2008. Web. 31 Mar. 2012. <http://www.scmagazine.com/ddos-hack-attack-continues-against-church-of-scientology/article/104588/>.

Kearney, Paul. “The Rise of Hacktivists.” Secure Thinking 2011. Web. 7 Oct 2011.

Kelly, Meghan. “Anonymous Disables Child Pornography Servers as Part of OpDarknet.” VentureBeat.Com 24 Oct 2011. Web. 18 Jan 2012. <http://venturebeat.com/2011/10/24/anonymous-opdarknet-child-pornography/>.

Keromytis, Angelos D. “‘Patch on Demand’ Saves Even More Time?” *Computer*. Print.

Kieyzun, Adam et al. “Automatic Creation of SQL Injection and Cross-site Scripting Attacks.” *2009 IEEE 31st International Conference on Software Engineering* (2009): 199-209.

Manion, Mark, and Abby Goodrum. “Toward a Hacktivist Ethic.” October June (2000): 14-19. Print.

Marks, Paul. "Dot-dash-diss: The gentleman hacker's 1903 lulz”. NewScientist. 27 Dec 2011. Web. 24 Mar. 2012. <http://www.newscientist.com/article/mg21228440.700-dotdashdiss-the-gentleman-hackers-1903-lulz.html>.

McGlaun, Shane. "Hackers Target Power Plants and Physical Systems." DailyTech. 04 Aug 2010. Web. 20 Mar 2012. <http://www.dailytech.com/Hackers Target Power Plants and Physical Systems/article19257.htm>.

Mitnick, Kevin David, and William L. Simon. The Art Of Deception. Indianapolis: John Wiley & Sons, 2002. Print.

Moore, Alan, and David Lloyd. V for Vendetta. Vertigo, 2005. Print.

Nakashima, Ellen. "Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says." Washington Post [Washington, D.C.] 18 Nov 2011. Web. 26 Mar. 2012. <http://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html>.

Orth, Maureen. "For Whom Ma Bell Tolls Not." Los Angeles Times 31 Oct 1971. P28. ProQuest Historical Newspapers Los Angeles Times (1881 - 1985).Web. 25 Mar 2012.

Patrikakis, Charalampos, Michalis Masikos, and Olga Zouraraki. "Distributed Denial of Service Attacks."*Internet Protocol Journal*. 7.4 (2004): n. page. Web. 24 Mar.

2012. <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html>.

Rosenbaum, Ron. "Secrets of the Little Blue Box." Esquire. Oct 1971. Web. 20 Mar. 2012. <http://www.lospadres.info/thorg/lbb.html>.

Rosenbaum, Ron. “Secrets of the Little Blue Box”. Slate. 7 Oct 2011. Web. 26 Mar. 2012. <http://www.slate.com/articles/technology/the_spectator/2011/10/the_article_that_inspired_steve_jobs_secrets_of_the_little_blue_.html>.

Schwartz, Matthew. “Can Anonymous Cripple Critical U.S. Infrastructure?” *InformationWeek* 18 Oct 2011.

Sneakers. Dir. Phil Alden Robinson. Universal Studios, 1992. Film.

Stewart, Bill. "Mosaic -- The First Global Web Browser." The World's First Web Published Book. Living Internet, 10 Apr 2011. Web. 29 Mar 2012. <http://www.livinginternet.com/w/wi_mosaic.htm>.

Suddath, Claire. "The Weather Underground." Time. 07 Oct 2008. Web. 1 Apr. 2012. <http://www.time.com/time/magazine/article/0,9171,1848763,00.html>.

Taylor, Paul A. “From Hackers to Hacktivists: Speed Bumps on the Global Superhighway?” New Media & Society 7.5 (2005): 625-646. Web. 10 June 2011.

Technical American Party (TAP) Subversive Matter. Memorandum. SAC, Seattle, to SAC, New York. 1 January 1974. Bureau file 100-NY-179649.

"The History of Hacking." Focus. Focus. Web. 19 Mar 2012. <http://www.focus.com/fyi/history-hacking/>.

The Mentor. "The Conscience of a Hacker (Hacker’s Manifesto)." Phrack. 08 Jan 1986: Web. 31 Mar. 2012. <http://phrack.org/issues.html?issue=7&id=3&mode=txt>.

Thomas, Douglas. Hacker culture. Minneapolis, MN: University Of Minnesota Press, 2003. eBook.

"Timeline: A 40-year History of Hacking." CNN.COM. CNN, 19 Nov 2001. Web. 18 Mar 2012. <http://articles.cnn.com/2001-11-19/tech/hack.history.idg_1_phone-phreaks-chaos-computer-club-emmanuel-goldstein?_s=PM:TECH>.

Tron. Dir. Steven Lisberger. Walt Disney Productions, 1982. Film.

WarGames. Dir. John Badham. United Artists, 1982. Film.

Verizon RISK Team. "2012 Data Breach Investigations Report." Verizon Business. Verizon, 22 Mar 2012. Web. 25 Mar 2012. <http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf>.

Weir-Jones, Toby. “Can We Learn from Hacktivists?” Secure Thinking 2011. Web. 7 Oct 2011.

Academic Vita of Elizabeth Brennan Bartels

Education:

The Pennsylvania State University University Park, PA
Schreyer Honors College
B.S. Security and Risk Analysis, Spring 2012
B.S. Information Sciences and Technology, Spring 2012

Thesis: Truth, Justice, and the Internet Way: Security Implications of the Online Activist Movement

Technology Skills:

- C++
- Java
- HTML
- SQL
- XML
- Visual Basic
- Database Design
- Database Management

Activities:

- President of the Doctor Who Fan club
- President of the Game Design Club
- Chair, IST Student Government, Academic Committee
- IST Student Government, Academic Committee
- Member of Women in IST (WIST)
- Member of Gamma Tau Phi (IST Honors Society)
- IST Diplomat

Awards:

- College of IST Student Marshal, Spring 2012
- Winner of IST Women of Distinction Award for Service, 2012
- Dean’s List
- National Merit Finalist
- National AP Scholar
- Pennsylvania Governor’s School for Information, Society and Technology Scholar