THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

MOTIVATIONS AND ENABLERS PRESENT IN DECEPTION OPERATIONS: HISTORICAL CASE STUDY EXAMPLE - OPERATION FORTITUDE

GABRIELLE EBERHARDT
SPRING 2018

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Security and Risk Analysis
with honors in Security and Risk Analysis

Reviewed and approved* by the following:

Colonel Jacob Graham
Professor of Practice of Information Sciences and Technology & Coordinator, BS in Security and Risk Analysis
Thesis Supervisor

Dinghao Wu
Associate Professor of Information Sciences and Technology
Honors Advisor

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

Deception is a means to gain a favorable advantage. Whether practiced as statecraft (nation state against nation state), tradecraft (spy versus spy) or as part of a criminal enterprise (against groups or individuals), it is a tactic that is used every day, and in every part of the world. Motivations, methods, and objectives all vary by user group based largely on the desired outcome. There are two commonalities shared across all deception operations: 1) some elements of truth are what deceptions are based on; and 2) all deceptions prey on some form of bias. Biases can be cultural, personal, organizational, cognitive, or combinations thereof. To know which bias to exploit, the deceiver must have some understanding of the deception target, its behaviors, tendencies, and expectations. Then, armed with this understanding, the deceiver feeds a deception story or message to the deception target in an attempt to guide the victim to adopt a course of action that is favorable to the deceiver. This paper will examine the elements of deception through the context of a World War II military deception operation - Operation FORTITUDE. In doing so, it will highlight the component parts of deception-- how the parts were employed and when the parts were employed; and what made them successful or not. While Operation FORTITUDE was largely statecraft, that is, deception between nation states, it involved deception across a wide continuum and was comprised of multiple tactical-level deceptions within the larger deception theater. In similar fashion, the individual deception targets and their associated biases varied based on the role played by targeted individuals or groups in the overall operation. In Operation FORTITUDE, the British intelligence services represented the deceiver group and the German high command represented the primary target group. In between, there were multiple other deception targets (individuals & groups), with varying biases exploited and multiple stages of deception - each stage had to be completed successfully before the next step and next target could be engaged. One can gain much value by exploring deception through the lens of history and through the analysis of a real deception operation. First, analyzing this historic deception case provides an opportunity to tease out the elements of deception through the post mortem of history. Next, it enables one to view the entire deception continuum, from inception and planning through implementation. Additionally, such an examination hopes to provide the reader an insight into current-day activities and a better understanding of the role of deception in the modern context of a technology-enabled society. Finally, it will help intelligence and security professionals to be more aware of those things that make us vulnerable to deception and provide insight to help guard against it.

Keywords: deception, entities, motivations, biases, enablers, Operation FORTITUDE, exploit, aware, vulnerable

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would first like to thank Colonel Jacob Graham, my thesis advisor, for his patience and help throughout this process. Colonel Graham was willing to meet with me whenever I needed and always gave me critical feedback to make this paper the best that it could be.

I would also like to thank Professor Dinghao Wu, my honors advisor, who worked with me on a complex subject matter and gave me necessary advice.

I would also like to thank Professor Trisha Travers, an English Lecturer from Penn State Abington and Professor Linda Miller, a distinguished Professor of English from Penn State Abington who took time out of their busy schedules to look over my paper regarding grammar, tense, and everything else.

Last but not least, I would like to thank my mom and dad. Both of you have given me the inspiration and drive to do my best. I cannot thank you both enough for that.

Chapter 1

Introduction

As explained by Bennett & Waltz (2007) deception "is the deliberate manipulation of the target's perceptions and beliefs in order to distort his knowledge of the situation and to affect his decisions and actions in ways that benefit the deceiver" (p. 71). Deception occurs at grand-scale, as well as in everyday life. It takes place between nation states and between peers and coworkers. Many do not stop to think about why deception is utilized, whether they as individuals are susceptible, or even whether they have already been or will be a victim of deception. In principle, deception is used to gain some form of an advantage. The New York Times Editorial Board (2014) describes the ways the Federal Bureau of Investigation used deception to gain information to build cases for prosecution. Deceivers vary in size and complexity – from individual deceivers to criminal groups to nation-states. One example of tactical deception between nation-state armies as described by Latimer (2003) is when Napoleon Bonaparte's French army successfully deceived Johann Beaulieu and the rest of the Austrian army. Napoleon's tactical approach required the crossing of the River Po at a particular location. However, to ensure the crossing's success required some misdirection. Believing the Austrian commander expected the French crossing to happen at Valenza, Bonaparte dispatched forces in that direction. In doing so, Bonaparte accomplished two tactical maneuvers; first, a successful river crossing at a place of his choosing; and second, a successful positioning of fighting forces behind the Austrians line so as to surprise them from the rear (Latimer, p. 24). Deceivers employ varying means, depending on the deception target and the deception objective. Deception can be characterized largely by methodology as technical deception, physical deception, and administrative. Of the sub-type, technical deception, this can further be broken down into tactical and operational sensory deception. Underneath this umbrella of technical deception is the tactic of camouflage. Camouflage can be defined as, “the use of natural or artificial material on personnel, objects, or tactical positions with the aim of confusing, misleading, or evading the enemy” (Bennett & Waltz, 2007, p. 115). Camouflage is a way for the deceiver to “blend in” with their surroundings to make themselves less visible to the target/enemy.

Deception actors use deceptive tactics because they have a goal or objective that they need and want to reach. Deception actors are motivated when they carry out and employ deceptive operations and acts. Motivation shapes deception operations. Motivations vary based on the desired outcome of the deception. Typical deception motivators are monetary gain, knowledge, political or military advantage, amongst others. As motivations vary, so too do the enablers that make deception possible in the first place. The enablers are those conditions that, when present, allow the deceiver to perform the deceptive act, and those conditions that make the deception target or victim susceptible to the deception itself. In simple terms, enablers fool the deception target and the deceiver is able to gain the desired advantage. While deception operations vary by motivation, target, means and objective, there are certain commonalities that all deception operations share: appearance of truth and the exploitation of bias. According to Bennett & Waltz (2007), “deception works because most of what we observe and experience in the real is world is non-deceptive” (p. 59). A real world example of making deductions is a friend approaching another friend and is smiling, from past personal experiences it can be deduced that the smiling friend is happy to see the other. A deceptive example of using this tactic is a salesperson who smiles at a customer while mentally planning how they can swindle the customer out of money. In the context of deception, what is presented as truth is enabled through the eyes of the beholder (the deception victim) through the exploitation of bias. Bias in its simplest form is defined as “systematic errors in perception, judgement, and reasoning that contribute to the target’s distorted knowledge of reality” (Bennett & Waltz, 2007, p. 71). In the context of deception, biases are those characteristics of behavior that the deceiver seeks to exploit in order to frame the deception to the victim’s perception of truth in the hopes of causing a corresponding reaction. It is important to note that the deception activity itself is not the objective of the deception. The objective is the action taken on the part of the deceived in response. Typical biases used in deception include cultural, personal, organizational, or cognitive, and in many cases, different combinations of these. However, not all biases can be exploited equally. Deceptions at a grand scale, such as Operation FORTITUDE require extensive knowledge and insight and may require an in-depth understanding of individuals, groups, and organizations. Some biases can be more universally applied and thus suitable for generalized use. For example, a parent of school-aged children upon hearing of a violent incident at the child’s school might automatically drop everything and go to the school, thus providing an opportunity for a robber to break into the home. Alternatively, in similar fashion, cyber deceivers attempt to exploit user behavior by sending out hundreds, if not thousands of phishing emails in hopes that some will download malware onto their computer. The literature review first analyzes scholarly articles to identify the enablers and motivators present across the various deception domains, which include nation states, organizations, and individuals. The next area will discuss the different enablers (bias, opportunity, technology, etc.) and motivators (monetary, knowledge, power, influence, political, military, etc.) present in deceptive acts. The area following will discuss deception through the context of a World War II military deception operation - Operation

FORTITUDE, including the various individual, group and organizational deception targets and the corresponding enablers and the motivations exploited along the way. The final area will summarize the discussion and highlight the importance of understanding deception in the context of a technology-enabled society.

Chapter 2

Literature Review

Deception, its motivators, and the corresponding enabling forces employed to carry out deception in society have been studied and documented by many scholars. The starting point for the literature review is an examination of the major deception domains (deception actors), and a corresponding discussion of the motivators and enablers for each. The major deception domains covered herein include nation state, organizational (including business & crime), and individuals. It is important to note that each deception actor is guided by its own set of motivations and that the enablers for each will vary based on the scale and effort of the deception practice. For example, a nation-state may dedicate huge amounts of resources (labor, money, and time) in order to undertake a large-scale deception operation. Whereas, an individual, would likely lack the technical expertise and sophistication to pull-off a deception on a grand-scale.

Deception Domains

Nation States

A nation state is a state that joints the political entity of a state with the cultural entity of the state, thus providing political legitimacy (New World Encyclopedia, 2015).

Internally Directed Deception. It is not uncommon for nation-states to apply deceptive tactics against its own citizens. Mervin (2000) explains that one motivation that governments have to use deception is to make their citizens believe that “foreign policies outline with their preferences” (p. 25). That is, elected government officials will deceive their citizens to make them believe that their foreign policies are shaping up to be what they promised their citizens before they took office. When campaigning for office, an official may take a stance on a certain foreign policy, like international trade, and may say that they are going to fix those trade agreements if elected. After taking office, those campaign promises have different outcomes: officials could fix the trade agreements as promised, they can try to fix them but fail, or they may not try to fix them at all. The citizens (in this scenario) want to see change, so the government officials may deceive the public to make citizens believe that they are doing what they said they were going to do. Other literature has discussed instances where government officials may deceive the public about the country entering into an armed conflict. Napolitano stated, “It is commonplace in America for our leaders to lie in order to enter or initiate armed conflicts” (Christman, 2010, p. 61). Christman (2010), on Napolitano’s treatise, “Lies the Government Told You: Myth, Power, and Deception in American History,” explains that even in early American government, it was commonplace for government officials to lie and deceive the public about the what, who, and why, when nation-states go to war.

Enablers of Deception. Government officials are able to deceive the people that they rule because enablers are present within the target. An enabler is defined as something and or someone that “offers help and perpetuates rather than solves a problem” (Khaleghi, 2012). In the instance of a government official deceiving his/her citizens into believing that they have accomplished things that they said they would accomplish throughout their time in office, this would be a very small-scale operation. While the deceiver (the government official) is targeting a large group of people (citizens), they can achieve their goals easily if they lie and citizens believe their lies. In this example, government officials would be using anchoring bias to their advantage. The anchoring bias as defined by Shonk (2017) “describes the common tendency to give too much weight to the first number put forth in a discussion and then inadequately adjust from that starting point or ‘anchor’”. When presidential candidates campaign, they explain to the public all of the things that they are going to do when in office, like lower taxes. Once people hear that these officials want to lower taxes, for example, citizens will latch and anchor onto that statement and believe that the official will actually do what they say they were going to do.

Military-Strategic deception. Military-strategic deception involves deception at its highest form. Strategic operations are those that bring to bear or make available all of a nation’s capabilities, at a high level, and for long range national objectives; this differs from tactical deception, which is focused at a much lower level and usually for a short duration and for limited objectives. When nation states use deceptive techniques in strategic military operations, it is for gaining military-political advantage over their adversary – at a high level. Ronald Reagan’s Strategic Defense Initiatives (SDI) is an example of this. Dubbed “Starwars” Reagan publically announced his SDI program as a program to develop and employ a defense umbrella over the U.S. to protect the nation from a Russian nuclear strike. In reality, the program was less successful for its scientific-military achievement than it was as a means to have the Russians spend themselves into bankruptcy in an effort to keep up with their perceptions of U.S. military advancements. Usborne (1993) described:

> The two missiles had secretly been fitted with radio beacons to guarantee their meeting in space. This small but vital detail was apparently withheld as part of a general policy of 'strategic deception' at the heart of the SDI - the feeding to the Soviet enemy of lies about the project's progress and technological content.

If the military is able to gain an advantage, they are able to pursue their agenda within a certain area in any way they want. Gradev (2014) explains, "Logic to mislead your adversary is efficient and the payoff from it can be implemented very quickly" (p. 117). Gradev (2014) later explains that deception is "inherent to all human relationships; it is an intentional activity to gain advantage over the adversary" (p. 117). The focus of his paper is relating deception use to war practices. Nation-states, when going to war, want to win and push their agendas in whichever country they are trying to fight or invade. To do this, they need to stay one-step ahead of their adversary/ target. Being ahead of the target means that the deceiver is one step closer to "winning" (in whatever capacity that may be). "Winning" is whatever the deceiver wants to gain by deceiving the target.

Enablers of Deception. Enablers apparent within a target allow military-strategic deception to take place. For the deceiver to stay one step ahead of the adversary/target they can take advantage of different biases. Confirmation bias is one type of bias that can be exploited in this type of situation. Confirmation bias as defined by Nickerson (1998) is "the seeking or interpreting of evidence in ways that are partial to existing beliefs expectations or a hypothesis in hand." (p. 175). Most people, as well as militaries, tend to believe the simplest explanation of something. If the deceiver knows the attitude and culture of their adversary, they can intentionally play on this to feed to their target or put them in a situation where the target may "seek evidence in a way that is partial to their existing beliefs" (p. 175). Therefore, if the deceiver alludes to the target that they are planning to invade their country using the simplest and shortest attack route, the target may believe this to be the truth because of the simplistic nature that most people tend to have. The deceiver exploits the target's bias so the target will be prepared to meet the deceiver by the simplest route, but the deceiver will actually end up attacking using a harder and longer attack route to surprise the adversary.

Military-Tactical deception. Tactical operations are those that focus on the art of organizing and deploying armed forces, and different techniques used to engage and use weapons during battle. On the battlefield, nation-states employ deception to achieve tactical advantage. Deception is used within war to mislead the adversary for various reasons, the most common reasons are friendly intent, capability, and intelligence. Deceiving the target for these various reasons allows the deceiver to gain a tactical edge over their counterpart. Hutchinson (2006) states that:

> As the nature of conflict changed to being an almost ongoing situation, control over mass communication became a high priority task for governments as well as the military. As such, the manipulation of information became an essential function. Thus, the world of deception became an integral part of official communications between governments and their constituency (p. 213).

Information warfare is becoming more prevalent with the evolution of technology. Technology and its evolution is the primary driver for the changes within the use of deception as well as the evolution of deception itself as a practice. Having the upper hand over the adversary requires information that the deceiver may not have readily available. Adversaries know that their counterparts will be looking for information, and they are able to distort messages and send out fake information to try to get the target (adversary) to act in a way that is predetermined by the deceiver.

Enablers of deception. To employ military-tactical deception, the deceiver takes advantage of enablers that are present within the target. One bias that can be exploited within this type of situation is the automation bias. The automation bias as defined by Goddard et al. (2011) is “the tendency to over-rely on automation” (p. 121). During World War II, the use of technology like satellites and radio transmissions were utilized frequently. Countries used these devices to relay important information between armies and between satellite or communication stations. This information was sent over radio and satellite waves, and the adversary and other parties started to listen in on those channels. Most nation-states who would listen in on the other party’s communications would assume the information they overheard was accurate. These groups were over relying on the use of this type of automation and did not think about the possibility of the adversary purposely feeding false information.

Organizations

An organization can be defined as an individual person or group of people who come together to work on and achieve a common goal or objective. Organizations can range dramatically in size. Some can have 50 people while others can have 3,000.

Business

Deception between Business Competitors. Money and influence can help determine whether businesses succeed or fail. Because of this, deception is commonplace between business competitors. No new startup business wants to fail due to the wealth and power that larger and more distinguished businesses have. Smaller firms will resort to deceptive practices to try to stay afloat in the cutthroat business world. Even larger firms, who want to beat the competition, will resort to deceptive practices. Pech & Stamboulidis (2010) conclude that businesses engage in this type of deception practice. Throughout their work Pech & Stamboulidis state:

> One entrepreneur deploys a strategy designed to hide his success, giving the impression that his (very large firm) is only a very small family entity; the second entrepreneur takes this strategy further by completely hiding himself and his web of business interests from sight (p. 37).

This paper looks at the acts of two different business people who are in charge of different companies. They were able to document and see the results of when these two business people deceived their fellow business competitors. Pech & Stamboulidis (2010) noticed that large businesses are able to make it look like they are smaller in size, and it allows them to go unnoticed by larger firms. Larger firms are not necessarily worried about the influence and capabilities of small firms in that their larger firm has more employees, contacts, products, and offices. This allows the "smaller" company to do a lot more business transactions and gain more clients without the target firm realizing it is happening. By the small company hiding in plain sight, they are able to expand, create, and get more clients without other companies noticing.

Enablers of deception. Enablers are present within the targets of business-to-business deception. One bias (enabler) that can be exploited within this type of situation is the believability bias. The belief bias can be defined as "the tendency to be influenced by the believability of the conclusion when attempting to solve a syllogistic reasoning problem" (Morley et al., 2004, p. 666). If a larger business corporation sees numbers on paper for smaller firms within the same line of business, they will tend to believe these numbers. If it is a list of each company's revenues for the past quarter, and one small company made $3,000, hypothetically, the larger company will tend to believe that the other company is a small firm and is of no competition to the larger firm. They reasoned that because of the small numbers, they are not a competitor to be concerned about. The smaller companies can play on this bias.

Deception in the Office. Deception occurs between employees or between an employee and manager internally within companies themselves. A study conducted by Lindsey, Dunbar & Russell (2011) shows some interesting results. They found that “the perceived power difference between supervisors and subordinates was substantial, power impacted perceptions of deception in the workplace and how deceptive messages were crafted, and very few of the reported lies were detected” (p. 55). Within the corporate world power and influence are necessary to excel and succeed. People within the business world will use deceptive practices to gain more power and influence within their company. The desire of power influences how people interact with one another and how people communicate and send/receive messages to and from one another. The results from a study done by Lindsey, Dunbar & Russell (2011) showed that 44.86% of their total sample reported that they used deception within the workplace (mixture of supervisors and subordinates). Both parties participate in the use of deception and primarily do it through the channels of face-to-face conversations or over the phone.

Enablers of deception. Numerous enablers are present within targets when using deception internally within a company. One bias (enabler) that can be exploited within this type of situation is the hindsight bias. The hindsight bias as defined by Roese & Vohs (2012) is “when people feel that they ‘knew it all along,’ that is, when they believe that an event is more predictable after it becomes known than it was before it became known” (p. 411). It is commonplace for employees within any business organization to want to be promoted. If they believe the only way gain the promotion is by deception, hindsight bias is a way that an employee could potentially get there. If an employee believes that their co-worker is not fit for a promotion, but they feel that they are, they may start to slack off and act less motivated around the other employee. The other employee (target) will start to believe that they are no threat and not trying to be promoted. Every time something like this happens (the deceiver doing something to show he/she is unfit for a promotion), the target will tend to rely on experiences of when the same type of situation happened before. When looking in hindsight, the target knew all along that the other employee was a slacker (the deceiver). All the while, the deceiver is only acting deceptive in front of the target to push their agenda.

Crime

Group to individuals. Criminal groups have differing motivations for deceiving individuals, but they will target individuals because an individual person is easier to convince and manage than a group of people with differing thoughts and opinions. Some motivations seem more farfetched than others do but in the minds of the criminals, their motivations are relevant and make sense. Humphreys & Peelo (2013) describe in detail different cases in which criminals used deception and why it was used (according to the individual and their personal underlying motivations). In one case, they described a gang of people who sent out fake job ads directed at young Polish people. The ads explained that there were jobs available within the UK and that the group would help get them to the UK and get set up with a new job. In reality, there were no jobs available in the UK. This gang asked young kids to pay them money to help them get to the UK and once they received the money, they would stop the communication. The British police found financial gain to be the motivation behind this criminal act. The gang received numerous payments from vulnerable and naïve Polish kids. Their only reason for doing it was to gain more money.

Enablers of deception. Criminal organizations exploit enablers within individual targets to deceive them. One bias (enabler) that can be exploited within this type of situation is the outcome bias. The outcome bias as defined by The Interaction Design Foundation (2016) “enables us to judge our decision making based on the results of the process rather than the quality of the process itself.” The people who relied on this gang to get them jobs in the UK were assuming they would receive what they thought they were paying for and have a better life in the UK. The gang preyed on this bias within the young kids. They knew most of the kids would not be able to pass up that type of opportunity.

Terrorist group to nation-state. Terrorist groups will attack groups of people within nation-states to ignite fear within the citizens that reside there. There are numerous reasons terrorist groups will deceive. In another example explained by Humphreys & Peelo (2013) they explain that the motivation behind the attacks on September 11 were to promote terror and fear within the American people. Their motivations were not around money. They acted criminally by having false documentation that presented them as different people than they actually were (p. 6). Here, these terrorists were acting criminally but their motivation behind it was much different than the motivation of the gang of people who targeted young Polish kids. There are many different crimes that can be committed, hence, numerous kinds of deception that can be executed, and various kinds of motivations around why they are committing the criminal act.

Enablers of deception. Terrorist groups will exploit enablers within nation-states to promote fear and terror within the nation-state’s citizens. One bias (enabler) that can be exploited within this type of situation is the believability or belief bias. Terrorists can use this bias. In the instance above, the terrorist was able to show documentation that had false information on it. This was to try to show people that the terrorist was the “fake” person on the papers. Most people will believe what is in front of them on paper, and most people do not assume that somebody is a terrorist. The terrorist in this situation played on the fact that most people will assume that the documents are not falsified and that they (the terrorist) wish no harm on anybody.

Individuals

Employee to Customer. Employees within a company will deceive customers for different reasons depending on the situation. Research done by Payne (2008) explains the deceptive strategies and motivations behind part time workers. Payne conducted a study where he told students the definition of deception. The students then had to fill out review logs after two shifts at work. They were told to write down any instances where they heard or participated in deceptive acts. The data showed that the majority of student part time workers deceived in order to “evade work, cover up their mistakes, and mislead customers to increase their sales or commission.” (p. 5).

Enablers of deception. When employees targeting customers use deception, there are numerous enablers apparent that the deceiver can exploit within the adversary to deceive them. One bias (enabler) that can be exploited within this type of situation is the availability bias. The availability bias can be defined as a “cognitive heuristic through which the frequency or probability of an event is judged by the number of instances of it that can readily be brought to mind.” (Colman, 2008). If an employee lies to a customer on the phone and explains that they are very busy or that they do not have the item they are looking for in stock (and it is around the holiday season), most customers will believe what the employee says. Customers know that the holiday season is busy. Customers also know that numerous other people will be looking to purchase similar items compared to them. All of this information is available to them in their recent memory. The customers will look back on these memories and believe what the employee tells them. All the while, the employee was deceiving them so that they did not have to do extra work to look for the item in storage.

Individual to individual online. The world of technology and its constant evolution allows people to deceive other people while online and there are numerous motivations behind why it occurs. Research done by Utz (2005) explains why people on the internet deceive each other. In some cases, people pretend to be the other gender; in other cases people try to change their looks or personalities so more people seem to like them. Utz explains that the motivation for this type of deception is for “idealized self- preservation, fun, privacy, or malicious intent” (p. 51). People using online forums for communicative purposes and for relationship purposes may deceive for these reasons. Meeting people online allows for the two individuals interacting to not show their true selves. Looks are one of the first things that a potential partner may judge about them. In contrast, it also allows people to be cat fished when meeting potential friends or partners. The term “cat fish” refers to people posting fake pictures, posting fake things onto the internet or their social media profiles, and using this persona to make friends and gain people’s trust. The majority of what this person is posting is false, but the people who are convinced by the “false” information think they are talking to a real person and everything they post is accurate and correct.

Enablers of deception. Individuals will deceive other individuals online and exploit enablers present within the targets. One bias (enabler) that can be exploited within this type of situation is the confirmation bias. Deceivers in online forums can utilize this bias, already defined above, very easily. Most individuals want to see the best in people. If somebody reaches out to them online to start a relationship, the “target” will tend to latch onto pieces of information that are most likely to be true and use that information to judge the whole person. If the deceiver explains that they used to work at the same restaurant as the target, the target will tend to believe this to be true. Because that one piece was accurate, they judge the person (deceiver) to be telling the truth at all times. They are using small pieces of information to latch onto the fact that this person (the deceiver) is real and being truthful.

Chapter 3

Enablers of Deception

Enablers of deception are the elements that make deceptive acts successful or unsuccessful. One of these elements is biases. Bennett & Waltz (2007) define bias as “an inclination to judge others or interpret situations based on a personal and often sometimes unreasoned point of view” (p. 71). In regards to deception Bennett & Waltz (2007) explain that bias means “Systematic errors in perception, judgment, and reasoning that contribute to the target’s distorted knowledge or reality” (p. 71). Deceivers are able to exploit these biases to their advantage, to make the target behave in a certain way. There are four different types of biases that are relevant within deceptive practices. They are cultural biases, personal biases, organizational biases, and cognitive biases. The rest of this section will explain these types of biases in detail, and how deceptive practices utilize them.

Bennett & Waltz (2007) explain that cultural bias is “attempting to make judgments and decisions based on beliefs from cultural or social experiences” (p. 72). These beliefs can come from a specific place or country, they can come from preconceived ideas about a certain place or type of people, and they can come from habits or routines that are apparent within a certain environment. Being able to understand the cultural biases that the target has will help make the deception story more believable to the target. An example of this is that in America, the population views direct eye contact while speaking with somebody as a sign of respect and attentiveness, whereas in some Asian countries eye contact is considered disrespectful. If an American is a target in a deceptive act then it is in the deceiver’s best interest to make eye contact with whomever they are speaking. If the deceiver was to avoid making eye contact the target may become suspicious. The same thing can be said if the target of a deceptive act is from an Asian country. It would be in the deceiver's best interest to not look the target in the eye. This would avoid the chance of angering the target and the target feeling disrespected.

Bennett & Waltz (2007) explain that personal biases are "the beliefs and ideas that a person has based on personal experiences throughout their lives" (p. 73). Most notable are the experiences that occur when a person is an infant or a toddler. Any experience, either traumatic or amazing, tends to stick within the brain of a younger child more than, if it happened to an older person. An example of this is quite simply the story of the hare and the tortoise. The hare was very overconfident and was in the lead throughout their foot race the whole time. Because the hare was in the lead the whole time, the hare became overconfident. This eventually led to its downfall because the tortoise ended up winning the race. Because the hare relied on previous experiences within the race where it was winning, it became overconfident and did not think there was any way it could lose. This same thing could be said for acts of war. Most times whenever generals hear about how the others fight, that shapes the way they think of each other. For example, General 1 is known for sneaking up from behind the enemy and attacking. General 1 has done this to General 2 before. When there are rumors circling that General 1 is going to strike at General 2 again, General 2 is expecting the strike to come from behind and plans accordingly. Based on a previous experience, General 2 does not take into account General 1 attacking from the front, and that incorrect assumption is their downfall.

Bennett & Waltz (2007) explain that an organizational bias is "the result of the goals, mores, policies, and traditions that characterize the specific organization in which the individual works" (p. 74). This type of bias can be seen throughout numerous bureaucratic, government, and even business structures. By being able to pinpoint who in the structure receives important information and how long it takes to get to them, a deceiver could easily tell the wrong information to the right people to have the targets thrown off track without them even realizing. The deceiver could also take advantage of time sensitive activities. When somebody at the top of any organizational structure needs to be briefed on an event that just occurred, staff tends to provide information as quickly as possible so they have enough time and all of the information to make a sound decision and judgement based on the data they were just briefed. The deceiver here could take advantage of the intelligence analysts by sending in numerous “fake” radio signals, telephone calls, letters, etc. The analysts need to go through all of this and make a sound decision to relay the potential important information to the head of the organization. By sending so much in a little amount of time, the analysts may not look through everything as thoroughly as they should, and that would cause them giving a potentially inaccurate reading to the head of the company. This would play right into the deceiver’s hands.

Cognitive biases are another type of bias that deceivers take advantage of to mislead their targets. Bennett & Waltz (2007) explain that cognitive biases are “the innate ways that human beings perceive, recall, and process information from the environment” (p. 76). Humans draw upon experiences and beliefs to help them make decisions within different situations. An example of this is the bandwagon effect. Whenever a group of high schoolers purchases a new pair of shoes, they start a type of “fad”. Once a couple people start wearing the shoes to school all of the other kids start to go out to buy them as well. If they do not, they will stand out of the crowd and not fit in with everybody else. This is a simple example of the bandwagon bias. An example of this more related to deception, can be seen within the research project written by The Security Blogger (2013). Within this project, a fake person was created on social media sites.

This fake person, Emily, requested to be friends with lower level employees of an unidentified company. Once a couple employees accepted the friend request, other employees followed suit because they trust their friends from work whom they follow on social media. This same thing happened when “Emily” started to request friendships with personnel higher up in the company. These people saw that trustworthy coworkers below them accepted her request, so they followed suit. The deceiver’s goal was to get to the top of the organization and that is just what they were able to do. The bandwagon effect is only one of the many types of cognitive biases that humans have and that deceivers are able to take advantage.

Chapter 4

Case Study

The paper written by Donovan (2014) describes that OPERATION FORTITUDE was the code name for a military deception operation planned by the British and executed with help from the Allied powers, and aimed at the Axis powers (specifically Germany). This Operation was a part of a larger deceptive objective codenamed BODYGUARD. The purpose of FORTITUDE was to allow the British to invade Normandy while diverting the attention of the Germans to Norway and Pas de Calais. The Ally powers used numerous deceptive tactics to allow them an uninterrupted invasion of Normandy as well as some time afterwards to delay German reinforcement.

The Ally powers implemented many deceptive tactics to create false beliefs in the minds of the Germans. Some tactics that were used were physical deception like landing “fake” planes, using fake infrastructure and equipment, and utilizing dummy airfields. Wireless traffic was also used. This traffic was used to mislead the Germans into seeing and thinking that real Ally forces were positioned and stationed in places that they really were not. The Germans had too much trust in some of their agents; The Ally forces had agents on the inside working for the Axis powers but feeing them false information about the Ally powers (whom they were supposed to be spying on). In addition, the Ally powers were able to use and publicize the names of strong and notable generals, for example General George S. Patton. Whether or not the General was actually leading an attack, the Allied powers were able to put fear in the Germans by stating that one of the greatest Generals would be leading an attack against them.

The amazing thing about these deceptive acts is that they allowed the Germans to construct a false order of battle and false invasion location for the Allies. At no point in time did the Allied forces accidentally or purposely show the Germans any battle plans. The Germans took what they heard on the deceptive radio channels, and decided that they knew what the Allies' plans were. The Allies, to make their tricks even more believable, built buildings around where the German army thought their base was. They also constructed fake aircrafts and fake landing points for these aircrafts. General Patton then travelled to these fake aircrafts and buildings. He was photographed to make it seem like he was there to train and lead his army. The Germans still did not know that all of this was fake.

The rest of this section will describe what enablers were present within this case study, as well as which motivations of deception are present within this case study. These motivations will be compared and contrasted to the motivations that the literature review presented.

Enablers Present

Operation FORTITUDE consisted of numerous elements/enablers of deception. To reiterate from above, these enablers are cultural, personal, organizational, and cognitive. All of these elements were "prey" that either the Germans or the British exploited to further their agendas and plans. By either of these two countries exploiting one of these enablers of deception, this allowed them to carry out their deception plans and ultimately, be successful. Because the British created and implemented Operation FORTITUDE, the British exploited the majority of enablers. This does not mean that the Germans did not use deception tactics; However, within the scope of this paper, the focus is on the British and their deceptive actions.

Throughout Operation FORTITUDE, the British were able to play upon the enabler of cultural bias. Throughout this time, the Germans had numerous nuances about their culture that the British were able to play and exploit to push their own agendas and have things play out the way that they wanted. When Hitler became the dictator of Germany, his laws became the supreme laws of the land. Whatever he said meant that everybody had to follow suit. The British were able to find out that Hitler was a normative person. The British were able to feed the Germans information that Hitler was bound to accept as true, and the British knew that the German army would follow whatever way Hitler commanded. The British had to focus on fooling Hitler, because anybody below Hitler would make sure to follow his commands and not stray away from his beliefs. If they tried to undermine him or second-guess him, there was a very large chance that he would execute them. In addition, the governmental culture there at the time was many groups fighting for power (given to them by Hitler) and fighting to be Hitler's "favorite". The British knew this and were able to use the same technique mentioned above in their favor. They knew any information sent to the Germans would reach Hitler, because any group would want to show him that they found the information first to gain his approval. The information would be geared towards his normative ways, and he would tend to accept the information as true. The British were able to plant the seed and the German's tendencies to want power and the respect of Hitler allowed their deception plan to work just as they wanted. It is also known that at this time the Germans believed that they were the superior country and race. By having high commanding officers on the Allied powers side, it most likely did not sit right with Hitler. If he knew the ethnicity of some of the commanders and knew some of the people transmitting messages that the Germans intercepted, he most likely believed that the inferior races were not smart enough to make sure the Germans were listening to their conversations. Therefore, everything that was played over these channels, the Germans took as accurate.

Throughout Operation FORTITUDE, the British were able to play upon the enabler of personal bias. Hitler had an experience in WWI which made him believe Germany lost because the German armies were stationed too close around Germany. The German army and navy stayed too close to home and did not branch out to surrounding areas or countries. Platt (2004) explains that when WWII started, Hitler made sure to fix the problem that happened in the past. The German navy and army branched out to protect ports in Norway. The Germans focused on the belief that the British would come westward to where there were larger ports where larger armies could invade. They failed to think about the British possibly entering smaller ports on the eastern coast (p. 53). The British were able to play upon the fact that Hitler vocally explained why he thought the Germans lost WWI. Because the British knew this, they were able play upon Hitler's beliefs to deceive him and the Germans. The British also understood that Hitler (the commander-in-chief) was very hands on when it came to intelligence and actions of war. When a commander and chief is hands on in this way, personal biases are much easier to exploit and the British were able to do this. This allowed the British to invade Normandy with no push back until late into their invasion.

Throughout this operation, while organizational bias may not have been the target bias to exploit, the organizational hierarchy employed by the Germans most definitely played a part in their downfall. Most historians and war experts believe that even if the German command and control structure was different, the Germans still would not have won the war, but there would have been easier communication and not as many casualties would have occurred (for the Germans). In a paper written by Kraetsch (2009), he explains that Hitler believed no one commander should hold all of the power, so when it came to deliberation and whom commanders reported to, it became very confusing and was not very direct. Hitler wanted to make sure that he was the only person who held all of the power. By making numerous commanders go to different people for information and yes or no decisions, this made sure that every single one of them had no more power than the next one. Because of the complexity of reporting and making decisions, there were numerous delays when it came to acting on new intelligence or actually going out and physically attacking an area or people. Because of this lag, the British were already one-step ahead (because of the deception they employed) and this time lag made the Germans fall even more behind. Because the British knew how the German's hierarchy was created, it was easy for them to feed sensitive and act-provoking information, which would force the Germans to talk to different people and different commanders and take up more of their time. Whether or not it was a goose chase the British sent the Germans on, it took the Germans very long to decide or employ anything, and that allowed the British to stay one-step ahead. Another way that the British were able to exploit organizational bias was by knowing and understanding that commanders and intelligence analysts underneath Hitler were scared of him. These analysts and commanders knew of Hitler's mindset. The British would send information through their channels that would reinforce Hitler's beliefs, and his intelligence people would agree with this information and feed to it Hitler himself. These analysts and commanders did not want to consider any alternative assumptions based on the information they were fed through their channels because of the push back that they were bound to get from Hitler himself for questioning some of his beliefs.

Throughout this operation, The British were able to play upon certain cognitive biases present within the German's minds. One such biases they played upon was the confirmation bias. The Germans stole intelligence about where the British were sending armies in the hopes of attacking. The British knew that the Germans were listening in, and stealing fake and planted information. Hitler and the Germans knew the British most likely were going to this spot. The British then sent fake aircrafts and fake troops to this area. Hitler saw these troops and his belief of where the British were landing was “confirmed”. The Germans did not go any further to look into the legitimacy of the information they were being fed. They thought the British were going to land in one spot, and the British fed them more intelligence that confirmed that belief for them. The Germans then sent troops to this area, where in fact, Britain stationed fake troops. The British knew that Hitler was a normative person and that he believed in doing things with the least utility. They were able to feed Hitler information that led him to believe that they were going to take the “easy” way and Hitler did not question it because that is what he would do.

Another cognitive bias the British played upon was the anchoring bias. General Patton was a great commander of the United States army. The British played on the fact that General Patton was a great General and respected in the army community. The British led the Germans to believe that Patton was leading some of their troops into battle. Hitler knew about General Patton and “anchored” onto this information. He was fed pictures of Patton leading British armies along with intelligence about it as well. Hitler anchored on this information and believed that the British armies were going to be very strong and ready to fight. Hitler did not look at any other information that may have made him see that the information was false and that the British armies were less prepared than he thought. Britain gave Hitler one piece of information, and he made up his mind about the strength of the British armies based on that one piece of information.

Motivations Present

Motivations are present throughout all aspects of life. Motivations are very prevalent within the realm of deception and deception operations. Within Operation FORTITUDE especially, there are numerous different motivations present. There is an underlying reason behind why the British deceived the Germans, which allowed them to invade Normandy. Because this operation was conducted by a nation state in a time of war, the motivations present for the British closely aligned with motivations present within most nation states during a deception operation. Nation states here is defined broadly. It encompasses governments and politicians, as well as the country itself in a time of war. The motivations stated within the literature review are: government officials deceive their citizens to have them believe that their foreign policies outline with their preferences; government officials lie to their citizens in order to enter into war or start war; countries deceive others in order to gain control over information and communication channels and data; countries deceive other countries to gain the advantage in any type of conflict (able to push their agenda); and countries deceive other countries to "win". The rest of this section will discuss which of these motivations are present within the deceptive acts employed in Operation Fortitude.

Operation Fortitude was successful because of the deceptive acts used by the British. If they did not use these acts, the results may have turned out dramatically different. This deception operation was focused on Germany throughout their time of war. When looking at the first motivation behind nation state deception, government officials will deceive their citizens to have them believe that their foreign policies align with their preferences; this is not a motivation present within Operation FORTITUDE. As stated before, Operation FORTITUDE was a deception operation planned and executed within the realm of war. This deception was not aimed at the citizens of Britain or Germany in any way. This is not to say that citizens were not deceived, but that this paper does not focus on that example.

The second motivation listed within the literature review was that government officials will lie to their citizens in order to enter into war or start war. This motivation has to do with the acts of war but it focuses on government officials and citizens. As stated above, Operation FORTITUDE is a deception operation deployed by Britain, focusing on the Germans. Government officials are not seen talking to or discussing with their citizens about joining WWII. This may have occurred earlier when the countries were first debating whether to join WWII or not, but the focus of this paper and the literature review is around the deception operation done when already in war. This deception operation was deployed when Britain was already in the war and fighting. Their citizens already knew their country was fighting and may or may not have supported it. That is not the focus of this operation. While that motivation may have been present before the war started, that is not the focus of this paper.

The third motivation listed within the literature review was that countries deceive others in order to gain control over information and communication channels and data. This type of action can be seen throughout all acts of war, no matter the country. Tavares (2001) explains that the British had control over the information that the Germans were hearing, seeing, and had access to. More than just this, the British were able to judge how the German’s felt and reacted to the information that they received from the British. The British had dozens of double agents within the good graces of the Germans, but these agents would feed information back to the British. In addition, further into the war, the British were able to decrypt messages that the Germans were sending across different communication channels (p. VI). By the British employing these double agents, they were able to access German information as well as feed false information to the Germans. This shows that the British had control over German intelligence and communication channels. The double agents that the British had in place were able to monitor the information that they were giving to the Germans and in what quantities. They were also able to gain true intelligence about the Germans themselves. From this, the British were able to deceive the Germans. The British were able to feed information to the Germans and better understand how the Germans felt about the information they fed them. From this, the British were able to manipulate the Germans into thinking attacks would happen in places that they in fact were not. The motivation of having control over these channels led to the British to be better able to manipulate and ultimately deceive the Germans. Travers (2001) also explains that the British had control over almost all of the radio transmission in England. This allowed the British to control what was being sent across these radio channels. The Germans did not knows that the British military was controlling all of these channels, but the British knew that the Germans would try to eavesdrop to gain intelligence information. The British were able to send “fake” information across these channels to mislead the Germans. This again allowed the British to be one-step ahead and manipulate the Germans into doing something that the British wanted them to do.

The fourth motivation listed within the literature review was that countries deceive other countries to gain the advantage in any type of conflict (able to push their agenda). This type of motivation in a way compares to the motivation stated above. When trying to control information and information channels, one gains a type of advantage. Within an article written by Klein (2014), he describes that the British forces created fake groups of armies and fighting forces. This allowed the British to seem larger and better prepared for large numbers of German armies to attack. This also allowed the British to seem more prepared and more ready to take on the

German army. This in turn made them seem superior in the eyes of the Germans and perhaps make them scared for what is to come. The British also employed decoy planes and landing areas in places where they wanted the Germans to think they were stationed or would be attacking. This allowed the British to seem more prepared; at the same time have the Germans believe that the British were actually stationed or would attack from this area. Having the Germans think this allowed the British to stay one-step ahead and allowed them to know and even anticipate what the Germans would do in response. Being able to know where the Germans may attack allowed the British to be one-step ahead and have an advantage over the Germans. The British were also able to break the German's encryption mechanism so they were able to see their communications and see that the Germans believed everything that they were doing. This again gave the British an advantage in that they actually knew that their decoys worked, and they could then focus on their actual attacking plans.

The fifth motivation listed within the literature review was that countries deceive other countries to "win". In this case, "win" means win the war or successfully take control of and take over an intended location (country, city, etc.) In a report written by Tavares (2001) he describes that the British armies wanted to take control over Normandy and the South of France. The British used deception techniques to make the Germans believe that their main target was Pas de Calais. The British used deception to fool the Germans and allow them to take over and invade Normandy and South France. Because the British and their deception operations were successful, they "won". There were numerous different deception techniques that the British used to successfully "fool" the Germans and take over the intended location. Some of them have already been mentioned above, dummy aircrafts, feeding false information, double agents, etc.

Chapter 5

Summary

There are numerous reasons why different deception actors use deception. Each actor (nation-states, organizations, and individuals) has different motivations behind why they use deception. No matter the actor, every deception operation takes advantage of biases within the human mind to be successful (cultural, personal, organizational, and cognitive). By looking at the case study of Operation FORTITUDE implemented by the British, the different types of biases and motivations can be seen throughout. Because this study focuses on a war operation, the motivations for nation-states are assessed. A nation State is a state that joints the political entity of a state with the cultural entity of the state, thus providing political legitimacy (New World Encyclopedia, 2015). The motivations present within Operation FORTITUDE that are cited within the literature review are: countries will deceive others in order to gain control over information and communication channels and data; countries will deceive other countries to gain the advantage in any type of conflict (able to push their agenda); and countries will deceive other countries to "win". All of this is discussed to show the importance of understanding how deception works. It is important to understand what actors use deception, their motivations, and what biases these actors exploit within their targets. Understanding these things will allow potential targets to be more aware of their surroundings and perhaps not become fooled by the deceiver. Motivations of different deception agents remain the same today, even within a technology driven society.

REFERENCES

Bennett, M., & Waltz, E. (2007). Counter deception principles and applications for national security. Artech House.

Christman, S. (2010). Lies the Government Told You: Myth, Power, and Deception in American History. Journal of American Physicians and Surgeons, 15(2), 60-61. http://www.jpands.org/jpands1502.htm.

Colman, A. M. (2008). *A Dictionary of Psychology*(3rd ed.). Oxford University Press.

Donovan, L. C. M. J. (2014). Strategic Deception: Operation Fortitude. Pickle Partners Publishing.

Goddard, K., Roudsari, A., & Wyatt, J. (2011). Automation bias: a systematic review of frequency, effect mediators, and mitigators. Journal of the American Medical Informatics Association, 19(1), 121-127. doi:10.1136/amiajnl-2011-000089

Gradev, K. (2014). A Taxonomy of Deception Based Actions in War. Journal of Defense Resources Management, 5(2), 117-124. Retrieved from https://search.proquest.com/ezaccess.libraries.psu.edu/docview/1650984603/abstract/364C7765427E4BE7PQ/1

Humphreys, L., & Peelo, M. (2013). Understanding deception: disentangling skills from conviction. The Howard Journal of Crime and Justice, 52(1), 55-64. doi:10.1111/j.1468-2311.2012.00725.x

Hutchnison, W. (2006). Information Warfare and Deception. Informing Science: The International Journal of an Emerging Transdiscipline, 9, 213-223. doi:https://doi.org/10.28945/480

Khaleghi, K. (2012, July 11). Are You Empowering or Enabling? Retrieved November 16, 2017, from https://www.psychologytoday.com/blog/the-anatomy-addiction/201207/are-you-empowering-or-enabling

Klein, C. (2014, June 03). Fooling Hitler: The Elaborate Ruse Behind D-Day. Retrieved October 25, 2017, from http://www.history.com/news/fooling-hitler-the-elaborate-ruse-behind-d-day

Kraetsch, J. (2009, June 09). Rommel's Command in Normandy: Hitler's Interferences and Other Problems that Plagued the German Army. Retrieved October 25, 2017, from http://www.history.ucsb.edu/faculty/marcuse/classes/133p/papers/096KraetschRommelNormandy.htm#_ftnref7

Latimer, J. (2003). Deception In War. Woodstock, NY: The Overlook Press.

Lindsey, L. L. M., Dunbar, N. E., & Russell, J. C. (2011). Risky business or managed event? Perceptions of power and deception in the workplace. Journal of Organizational Culture, Communications and Conflict, 15(1), 55. http://www.instituteforpr.org/risky-business-or-managed-event-perceptions-of-power-and-deception-in-the-workplace/

Mervin, D. (2000). Deception in government. Society; New York, 37(6), 25–27. https://search-proquest-com.ezaccess.libraries.psu.edu/docview/206716950/abstract/79EC08D42F7440B3PQ/1

Morley, N. J., Evans, J. S., & Handley, S. J. (2004). Belief bias and figural bias in syllogistic reasoning. The Quarterly Journal of Experimental Psychology, 57(4), 666-692. doi:10.1080/02724980343000440

New World Encyclopedia. Nation-state. (2015, August 19). Retrieved November 15, 2017, from http://www.newworldencyclopedia.org/entry/Nation-state

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. Review of General Psychology, 2(2), 175-220. doi:http://dx.doi.org.ezaccess.libraries.psu.edu/10.1037/1089-2680.2.2.175Parkinson, R. (2017).

Payne, H. J. (2008). Targets, strategies, and topics of deception among part-time workers. Employee Relations, 30(3), 251-263. DOI: 10.1108/01425450810866523

Pech, R., & Stamboulidis, G. (2010). How strategies of deception facilitate business growth. Journal of Business Strategy, 31(6), 37-45. https://doi.org/10.1108/02756661011089062

Platt, O. (2004). Bodyguard: The Secret Plan That Saved D-day. iUniverse.

Roese, N. J., & Vohs, K. D. (2012). Hindsight Bias. Association for Psychological Science, 7(5), 411-426. doi:https://doi.org/10.1177/1745691612454303

Shonk, K. (2017, October 20). What is Anchoring in Negotiation? Retrieved November 11, 2017, from https://www.pon.harvard.edu/daily/negotiation-skills-daily/what-is-anchoring-in-negotiation/

Tavares, E. A. (2001, April). *OPERATION FORTITUDE: THE CLOSED LOOP D-DAY DECEPTION PLAN*(Publication). Retrieved March 19, 2018, from Maxwell Airforce Base website: https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/tavares_fortitude.pdf

The Interaction Design Foundation. (2016). Outcome Bias – Not All Outcomes are Created Equal. Retrieved November 12, 2017, from https://www.interaction-design.org/literature/article/outcome-bias-not-all-outcomes-are-created-equal

The New York Times Editorial Board (2014, October 31). Opinion | Deceptions of the F.B.I. Retrieved September 27, 2017, from https://www.nytimes.com/2014/11/01/opinion/deceptions-of-the-fbi.html

The Security Blogger (2013, February 20). SOCIAL MEDIA DECEPTION PROJECT: Emily Williams isn't real! Retrieved October 25, 2017, from http://www.thesecurityblogger.com/part-2-the-attack-the-social-media-deception-project-how-we-created-emily-williams-to-compromise-our-target/

Usborne, D. (1993, August 28). Reagan's great lie in the sky: Star Wars scientists may have deceived Moscow and Congress about the project, writes David Usborne in Washington. Retrieved November 16, 2017, from http://www.independent.co.uk/news/world/reagans-great-lie-in-the-sky-star-wars-scientists-may-have-deceived-moscow-and-congress-about-the-1463972.html

Utz, S. (2005). Types of deception and underlying motivation: What people think. Social Science Computer Review, 23(1), 49-56. https://doi.org/10.1177%2F0894439304271534

ACADEMIC VITA

GABRIELLE EBERHARDT

856-745-4086 | gabby.eberhardt@gmail.com

EDUCATION

The Pennsylvania State University, University Park, PA August 2016 - May 2018
Pennsylvania State University: Abington Campus, Abington, PA August 2014 - May 2016
Major: *Security and Risk Analysis – Information & Cybersecurity Option*
Honors: *Abington Honors Program| Civitas Victus Dictio Honors Program| Schreyer Honors College| Gamma Tau Phi*

AWARDS & SCHOLARSHIPS

Rookie of the Year - PSU Abington Tennis
MVP - PSU Abington Tennis
Wes Olsen Memorial Scholar Athlete Award - PSU Abington Tennis 2015-2016 Season
NEAC All-Conference Team: First Team Third Doubles and Third Singles - PSU Abington Tennis 2015-2016 Season
PNC Technologies Scholarship Fund
Provost's Award
Abington Fellows Scholarship and Grant
Top Individual Analyst – Security and Risk Analysis (Deception and Counter Deception)

LEADERSHIP

Learning Assistant (Grader) for IST 432	August 2017 – Present
Secretary of Gamma Tau Phi (IST Honor Society)	August 2017 – Present
Director of Social Media for IST Student Government	August 2017 – December 2017
Team Leader for Semester long Project in SRA 221	January 2017 – May 2017
Team Leader for Diabolical Deeds Exercise in SRA 231	August 2016 – December 2016
Athlete Services for the Student Athlete Advisory Committee (PSU Abington)	August 2015 – May 2016
First Singles and First Doubles for Penn State Abington Tennis	August 2014 – May 2015

RELATED PROJECTS

Abington College Undergraduate Research Activities (ACURA)
Cybersecurity Snapshot: Google, Twitter, and Other Online Databases

- Collaborated with team members and Dr. Bharat S. Rawal Kshatriya, D.Sc. Assistant Professor of IST, to research and create a mathematical model to help predict future cyber-attacks. The model helps predict the target, timeframe, and method of the attack. This research was turned into a paper and published in the Journal of Advanced Computer Science & Technology.

Open Basic Geo-Spatial Intelligence Boot camp (Professional Training)

RELEVANT EXPERIENCE

Erie Insurance, Erie, PA May 2017 - August 2017
Information Security Operations Intern

OTHER EXPERIENCE

Panera Bread, State College, PA August 2016 – Present
Crew Member

Wendy's, Mt. Laurel, NJ September 2013 - January 2018
Shift Supervisor (May 2015 – January 2018)
Crew Chief (January 2015 – May 2015)
Crew Member (September 2013 – January 2015)

TECHNICAL SKILLS

Working Knowledge: SQL Developer, CISCO Packet Tracer, Computer Vulnerabilities, Python, SPLUNK, Nexpose, Symantec, Stealthwatch, Absolute