



*Class Ring on Civil War
Rifled-Brass Cannon
Daniel Melnikov*

A Letter from the Editor-in-Chief

Dear reader,

It is with great honor that the Editorial Staff presents to you the 29th edition of *The Gold Star Journal*, The Citadel's most prestigious academic publication. *The Journal* features nonfiction papers from a variety of disciplines, along with photostories, photographs, and artwork submitted by Citadel students. Building on the experiences of the past, the 29th Edition strives to carry forth the legacy of *the GSJ*, combining academic prestige and modernity to showcase the best minds within our institution.

The heart of the 29th Edition's staff formed in the Fall of 2022, when Andrew and I were eager sophomores, while Noah and Niki endured the struggles of Knob year. Following the addition of John in 2023 and the arrival of our resident sophomores, Quinten and Kaitlyn this Fall, the 2024-2025 AY's staff was finalized, working tirelessly over the last few months to bring to you the 2025 edition of *The Gold Star Journal*.

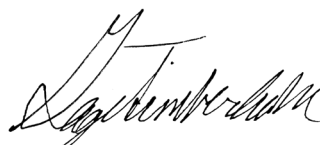
This staff is the very reason why I returned for my third consecutive year. Through serving as Editor-in-Chief, I have been blessed with the opportunity to work alongside the brightest minds and most determined cadets on our campus, all while building personal relationships that will last a lifetime.

Special recognition must be given to my Assistant Editor-in-Chief, Noah Miller. There has yet to be a moment where he was not prepared to support me in any way necessary

and I could not have asked for a better man to work alongside these past three years. Likewise, the success of the *Journal* is possible only through the dedication of Dr. Suzanne Mabrouk, the GSJ's faculty advisor since its inception in 1996. Through her mentorship and care, twenty-nine different groups of staff have flourished, producing the finest academic publication in the nation. Additionally, I would be remiss not to mention our esteemed donors, without their generosity none of this would be possible.

My time as Editor-in-Chief has taught me more about myself than I could ever have imagined. I hope you delight in reading this year's edition as much as we enjoyed its creation. I extend special thanks to F-Troop and the cadets I had the opportunity to lead for my final year at our institution. You all make each day worth the time and energy it takes to make this possible. Have fun reading and remember, Perfection is the Standard.

Yours,



Gage Timberlake

Editor-in-Chief

The Gold Star Journal

Class of 2025



STAFF SHOWCASE



*L to R: Dr. **Suzanne T. Mabrouk**, Advisor; **Quentin Walsh**, Editor; **John Cappello**, Communications; **Noah Miller**, Assistant Editor-in-Chief; **Gage Timberlake**, Editor-in-Chief; **Kaitlyn Hatchew**, Editor, **Kanjanika Kincaid**, Marketing, and **Andrew Palmer**, Editor.*

THANK YOU TO OUR DONORS:

**The Office of the Provost
LTC and Mrs. Albert G Bauer II '72
Dr. and Mrs. James F. Boyd, '71
Mr. John S. Clark, '18
LTC and Mrs. Paul S. Hodges, '63**

**Friends of the Daniel Library
Dr. Suzanne T. Mabrouk and
Mr. Stephen S. Jones
Mr. and Mrs. Grant N. Miller, '18
Mr. and Mrs. Daniel Vallini, '95**

THE GOLD STAR JOURNAL INTERNSHIP COURSE



L to R: Joshua Jackson, Abigail Sitarik, Olena Fedinova, Aaron Candreva, Hana Uraizee, Nathaniel Erwin, and Brett Roache

A SPECIAL THANK YOU TO



MEGAN GARVIN
Graduate Assistant



DR. SUZANNE T. MABROUK
Founder and Advisor



IN HONOR OF



SERGEANT MAJOR YAGLE

The twenty-ninth edition of *The Gold Star Journal* is proudly dedicated to Sergeant Major Andrew L. Yagle, United States Marine Corps (Retired). After 31 years of selfless service to his nation in the Marine Corps, Sergeant Major Yagle is an irreplaceable figure within the Commandant's Department, having now served the South Carolina Corps of Cadets (S.C.C.C.) for 11 years and counting as the college's Command Sergeant Major.

Sergeant Major Yagle credits his experience as a drill instructor while a young Marine to the longevity and success of his military career. He has carried this with him here at The Citadel. Sergeant Major preaches that "training another human being is one of the most important things you can ever do." This spirit of mentorship has left an indelible impact on the lives and careers of thousands of Citadel cadets. A consummate professional and the model of ideal proficiency, Sergeant Major has shown the way for cadets to take pride in their work, remain true to themselves, and uphold a life of virtue by the way he lives. For these reasons, Sergeant Major has inspired many cadets in ways that are not easily forgotten.

Sergeant Major is ubiquitously respected and appreciated by the S.C.C.C., especially the editors of *The Gold Star Journal*. He is a great friend to us and has graciously supported our operations through the years by approving cadets to wear patches, ribbons, and pins that represent *The Journal*. The Corps of Cadets and *The Gold Star Journal* are eternally grateful to Sergeant Major Yagle for his value of high achievement and a job well done.

Sergeant Major's message to "be true to yourself and demand of yourself always," transcends the S.C.C.C. and the Marine Corps. This lesson will continue to lead cadets to greater heights. It is with our great respect and admiration that we, the editors of *The Gold Star Journal*, dedicate the twenty-ninth edition to Sergeant Major Andrew L. Yagle: the magnanimous man, the Marine, The Citadel legend.



TABLE OF

CRYPTOLOGY IN THE SECOND WORLD WAR

8

TYLER KELLY

During World War II, Cryptology was used by both the Allied and Axis powers in attempts to gain an advantage over their enemy. The impacts of these efforts greatly influenced the operational efficiency of whomever held the upper hand and played a key role in the Allies' eventual victory.

CORPORATE SOCIAL RESPONSIBILITY: TEMU AND THE GLOBAL ECONOMY

14

ANDREW HARRINGTON

Temu, a rapidly growing e-commerce platform under the company Pinduoduo, has a large role in the global economy. This analysis highlights concerns regarding Temu's environmental sustainability claims, transparency issues, and logistical challenges. While Temu promotes itself as environmentally conscious, its lack of detailed data regarding its carbon footprint raises questions. For Temu to maintain credibility, it must update its Environmental, Social, and Governance (ESG) report with quantifiable data.

SOCIAL WELL-BEING AND THE IMPORTANCE OF A THIRD PLACE

18

ROBERT ISAAC WILLIAMS

What makes us happy? The data is shockingly simple. "Third places," or a place other than home or work, is vital not only to our social connectedness, but also our overall happiness. Come explore the facts and benefits of getting out of your house.

THERMAL MANAGEMENT SYSTEMS IN HIGH-SPEED AIRCRAFT

22

KYLIE COULSTON

Thermal management systems are crucial in regulating the temperature of critical components within aircraft. Elements such as solar radiation, electronics, and air friction negatively affect the plane's performance by creating heat. As planes increase in speed and on-board electrical components, the heat load continues to increase making these current systems ineffective.

CONTENTS

INFRASTRUCTURE UNDER ATTACK: CYBER THREATS TO TRANSPORTATION

28

MATTHEW PINCHBECK

The U.S. transportation system plays a critical role in our nation's infrastructure, and its supporting subsectors are under attack by cybercriminals. How can the U.S. defend against these threat actors? The answer may surprise you.

AN UNTAMED LIFE: A PHOTOSTORY OF YELLOWSTONE NATIONAL PARK

36

CHAD SOUDERS

In recent history, our society has become plagued with social media. We crave dopamine hits from strangers viewing our social media posts, only increasing our desire to remain online: addicted, tamed, soulless. I came to this sad realization in summer 2022, and proclaimed that I would live a life worth living, a life that was untamed. After meticulous planning, I found myself embarking on a journey to live in Yellowstone National Park to enjoy the most beautiful aspects of our everyday lives: the great outdoors.

CYBERATTACKS: WHO IS AT FAULT?

38

KIRIN CHAPLIN

Cyberattacks are an increasing threat in today's digital landscape to individuals, organizations, and governments. Should organizations or governments be held responsible for a cyberattack, or should the sole responsibility of a cyberattack be placed on whomever carried out the attack?

NANOPARTICLES TO THE RESCUE: DEVELOPMENTS IN CANCER TREATMENT

44

JESSICA BAILEY

Chemotherapy is a drug-dependent treatment used to stop the growth of cancer cells. However, chemotherapy cannot distinguish between healthy and cancerous cells. Nanotechnology is an increasingly popular delivery system used to help the drug target the unhealthy cancer cells while protecting healthy cells. Understanding the multifunctionality of nanoparticle treatment will result in a more individualized healthcare plan for those with cancer.

HIDDEN THREATS: THE ETHICS OF ZERO-DAYS

48

SEBASTIAN KLINCEWICZ

U.S. National Security increasingly relies on digital platforms, yet many systems remain vulnerable to unaddressed security flaws. Widely referred to as zero-day vulnerabilities, these security flaws are weaknesses in the source code of software or hardware products unknown to the vendor, allowing adversaries to exploit a system without detection. Ethical concerns regarding the stockpiling of zero-day vulnerabilities have become a pressing topic.

CRYPTOLOGY IN THE SECOND WORLD WAR

TYLER KELLY

While many know that cryptology, the use of codes and cyphers, influenced the outcome of World War II, the extent of this impact is rarely explained in depth. This is often because schools teach the factors that lead to war and its results rather than the reasons behind the outcome. The curriculum leaves out the importance of the war of communication fought by the Allied and Axis powers. Understanding how the Allied and Axis powers created and cracked codes, and specifically how the Allies were more successful, allows people to understand how the war ended with an Allied victory. This paper examines the use of cryptology by both the Axis and Allies. During World War II, both sides used cryptology to shape their actions. Cyphers are a form of coded messages, used to prevent information from falling into enemy hands ("Cypher," n.d.). Decryption, the countermeasure to cyphers, is the conversion of a cypher into the true message ("Decryption," n.d.). By decrypting lines of communication, an army acquired vital information. I will explain how the Allied information gathering led to an Allied victory and highlight some developments immediately after. First, I will present the Allied and Axis cryptologic efforts. I will then shift to an analysis of the Target Intelligence Committee (TICOM), which operated in the closing days of the war, and influenced cryptology in the period immediately following the war. Lastly, I will explore the limitations of the research and recommendations for future research.

Allied Cryptologic Efforts

1.1 The Enigma Machine

Infiltration of the Enigma machine may be the most well-known decryption of the war, as well as one of the most influential. The Enigma was a German cypher machine that would couple a message with a key and derive a scrambled message and would periodically shift cyphers. The Enigma also worked in reverse by combining a message with the key to decrypt it (Welchman, 2017). The machine would have been useful to the Reich for secure military communication, had it not been infiltrated years earlier. In 1931, future spy Hans-Thilo Schmitt sold details on the Enigma machine to the French, allowing France to begin the work of cracking the cypher (Kahn, 2009). Because the French used linguists as their cryptologists, they failed to crack the machine, so they sent to Poland in hopes that their expertise could solve the machine (Kahn, 2009). After Poland and France fell, efforts to crack the Enigma had to find a new home in Britain, at Bletchley Park. While describing Bletchley Park, the estate that headquartered Allied code-breaking, Maurizio Catino (2015) explained that "its task during World War II was to penetrate the secret communications of Britain's enemies" (p. 547), which included the Enigma and many more. One important figure within Bletchley Park was Dr. Alan Turing. He used a machine called the BOMBE that cracked the Enigma (Severance, 2012).

1.2 Other Successes of Allied Cryptology

Other Allied achievements included further decryption of Axis cyphers and efforts to deceive

the Axis into thinking their cyphers were secure. One such cypher that proved extremely valuable to the Allied war effort was Purple, a high-grade Japanese cypher. Purple was cracked by William Friedman, a man who revolutionized the field of cryptology and is regarded as the “father of cryptography” (Goldman, 2017, p. 1). He cracked Purple by counting how often the same letter occurs in the same place on different encrypted texts and used that to find out how other texts should be decrypted (Goldman, 2017). Another prominent figure in the world of cypher machines during the war was Thomas Harold Flowers, who made the Colossus, which was used to efficiently intercept messages for decryption (Haigh, 2018). It could process fifteen messages a day, while The Robinson machine, The Colossus’s predecessor, could only yield one (Haigh, 2018).

The Allies also succeeded at deceiving the Axis into believing their lines of communication were secure. One example was Britain only sending interceptors when bombers could be detected by other methods beyond the cracked cypher. This made it appear that they had not known about the raid ahead of time. Additionally, Britain sent patrol aircraft to locations where submarines would be surfacing so that the aircraft would “get lucky” and spot it (Mount, 2006). These methods fooled the Germans into believing that their communications had not been infiltrated.

1.3 Failures of Allied Cryptology

While the Allies had many successes in the use of cryptology, there were some failures at the hands of the Axis. For example, the Japanese challenged Britain’s cryptological efforts in the early war. By 1940, “Japan had an advantage over Britain in the codebreaking war” (Kotani, 2005). At that point, Japan was far more efficient at decrypting British cyphers than the British were at decrypting theirs; Japan could decrypt in one to four days while Britain took three to six days (Kotani, 2005). Given how time-sensitive some of these messages were, Britain suffered a heavy disadvantage. An example of such a disadvantage was how the British intercepted a message on September 14, 1940, stating that the Japanese would push into Indochina on September 22, 1940, but only decrypted it two days before the attack (Kotani, 2005, p. 313),

leaving no time for preparation. Moreover, Britain’s Naval Cypher No. 3 was cracked by the Germans in mid-1942, and despite knowing this almost immediately, the British did not replace the cypher until 1943 (Erskine, 2013). Consequently, Germany read communication that allowed their U-boats to intercept vessels for much longer than otherwise possible. Britain was fully capable of replacing the cypher in less time but prioritized different objectives (Erskine, 2013). The Allies failed in some aspects of cryptology, which ended up being left open for Axis success. Despite their failures, the Allies’ accomplishments resulted in a far greater impact on World War II.

Axis Cryptologic Efforts

Similar to the Allies, the Axis used cryptology during World War II, which drove some of their decision making. Some of these decisions were small, such as when and where to strike a convoy. Others were larger, such as which nation to attack. At points, their gathered intelligence led to poor decisions that hindered the Axis’ efforts. One point of note is that the difference in cooperation between the Allied powers and Axis powers can explain some differences in the operational efficiency of both.

2.1 Successes of the Axis Powers

Axis cryptological efforts produced results in both theaters. For instance, B-Dienst, the German Naval cryptology service, cracked Naval Cypher No. 3 (Erskine, 2013). Germany’s infiltration into the Naval Cypher No. 3 allowed them to send U-boats on missions to disrupt convoys to great effect. On the other side of the world, Japan found great success in their decryption of low-grade Allied cyphers. Originally, the Axis planned for Japan to advance in the north and into the Soviet Union, but when Japan decrypted a series of messages that confirmed the Allies would not be able to assist French Indochina, Japan made that region their new target. The cyphers Japan decrypted allowed them to take Indochina through diplomatic means prior to a military occupation (Kotani, 2005). Thus, the Axis powers were able to find a good bit of success in their respective theaters that heavily influenced their part of the war.

Thingvellir
Zih-Syun Fu



KELLY

technology. Unfortunately, the last goal was left unfulfilled as Japan and Germany had little cooperation in the cryptology field (Rezabek, 2012).

3.3 The New Mission of TICOM

While carrying out operations across Europe, a new threat was on the rise prompting a new mission: finding anything useful against the Soviet Union. First, the T-52 allowed for more Russian cyphers to be intercepted by the Allies (Rezabek, 2012). It allows for cyphers that were cracked to be decrypted, and those that had yet to be deciphered could be studied (Rezabek, 2012). The Allies eventually came across a castle that housed the German

Foreign Service Signal Intelligence archives (Rezabek, 2012). Among the archives were some deciphered Soviet messages, allowing the Allies to better understand how to decrypt the Soviet communication channels (Rezabek, 2012). Because this castle was in an area that would soon be handed over to the Soviets, TICOM Team 3 was sent to bring the archive back to Britain to keep it safe. Therefore, while TICOM was only active at the end of the war, it was able to rapidly increase Allied understanding of cryptology, leading to an advantage in the first days of the Cold War.



Post War Cryptology

The US and Britain continued to use cryptology after the war, but due to the lack of an enemy it was used in different ways. In this regard, cryptology was used to keep an eye on nations that seemed to be a potential threat. As time passed, there were still slight problems with cryptology, which only grew more numerous at the end of the war. Nevertheless, cryptology persisted as a vital tool for intelligence.

4.1 Cryptology in the Aftermath of the War

While the war was over, there were still uses for cryptology operations to be carried out on a variety of targets. After the war, the United States and Britain obtained various documents through TICOM that allowed decryption of communications from nations previously left untouched (Rezabek, 2012). Rather than discard this potential for intelligence, they began to read these newly infiltrated lines of communication, along with those that had already been cracked. Alfred McComack, an attorney hired to reorganize Army intelligence after Pearl Harbor, "explicitly refused to exempt any countries from surveillance" (Alvarez, 2007, p. 868), as the information could potentially be useful if

there were to be any conflict. One nation heavily monitored was France. They were in a position of global power before the war and there was concern they may cause conflict in attempts to reclaim the position (Alvarez, 2007). The Allies soon realized that France would not prove problematic, and concerns shifted.

4.2 The Rise of the Cold War

As World War II ended, the Cold War was on the horizon prompting increased efforts against the Soviet Union. A focus on Russian cypher systems emerged in the summer of 1945, even though the war in the Pacific carried on until mid-August (Alvarez, 2007). Through the efforts of TICOM, German efforts against Soviet cypher systems proved useful for the United States and Britain who otherwise struggled to crack Soviet cyphers (Rezabek, 2012). The discovery of the German Foreign Service Signal Intelligence archives improved the decryption efforts of the United States and Britain (Rezabek, 2012). The T-52 also proved useful as it allowed for an increased amount of Soviet radio transmissions to be intercepted (Rezabek, 2012). Unfortunately, the Soviets changed all of their cyphers in 1948, leading to a 30-year blackout of Soviet communication (Rezabek, 2012).

4.3 Persisting Hardships with Cryptology

While many advancements were made during the war, there were still some shortcomings that proved problematic with cryptology. Firstly, it was always difficult to provide real-time information on enemy communications (Alvarez, 2007). This was evident when Japan planned on invading Indochina and Britain found out through decrypted messages just two days before the attack, leaving no time to prepare for the invasion (Kotani, 2005). Another concern that occurred is high costs, as an increase in the number of targets comes with an increase in the number of resources needed to sustain the operation (Alvarez, 2007). This led to further issues as individual cryptological efforts had to be prioritized, and it was hard to discern which targets yield useful intel (Alvarez, 2007). Sometimes, countless hours and materials were put into deciphering a nation's encrypted messages, just to find out that the messages had no use. (Alvarez, 2007). Eventually, in the 1970s, most nations switched over to computer encryption and decryption systems, rendering most of the skills and techniques, along with almost all the machines invented during the war obsolete (Rezabek, 2012). Despite the persistent troubles with cryptology, it was able to provide intelligence in the post war period that shaped actions of major powers.

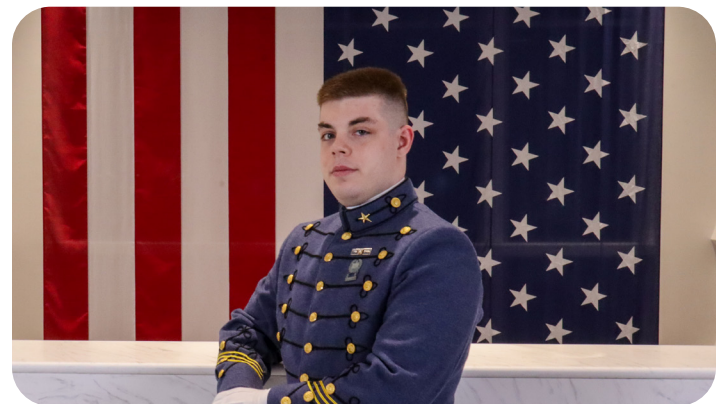
Conclusion

The outcome and immediate fallout of World War II was heavily influenced by both the Allied and Axis efforts in cryptology. The Allies encountered great success in decrypting the Enigma along with other cyphers that ended up proving vital to intelligence gathering, though they did suffer some failures. Similarly, the Axis found success in decryption, but they failed to cooperate in meaningful ways. Their extreme division of resources restricted them from making any meaningful gains in cryptology which caused their failures to impact the war more than their successes did. In the closing days of the war, the Allies were able to gather the archives and machines of the German cryptology units, which led to breakthroughs and even further success as Germany fell. This information was employed after the war against a variety of countries, but

eventually, the Soviet Union was targeted as the Cold War kicked off.

There were limitations within the scope of this research. For example, while many of these documents were declassified in the 1970s, some were kept hidden from the public until as late as 2009. Therefore, it is likely that some documents pertaining to this topic have yet to be released out of concern for national security. Future declassifications may reveal more information regarding cryptology in the war. The topic of cryptology in World War II is important because anyone who wants to understand the outcome of the war and those interested in the developments that occurred directly after its conclusion must first understand how cryptology affected the conflict.

About the Author - Tyler Kelly



Tyler Kelly is a senior cadet from Delta Company. He is majoring in Mechanical Engineering and will be going into the Navy as a Nuclear Officer after graduation.

References

- Alvarez, D. (2007). Trying to make the MAGIC last: American diplomatic codebreaking in the early cold war. *Diplomatic History*, 31(5), 865–882. <https://doi.org/10.1111/j.1467-7709.2007.00657.x>
- Cotino, M. (2015). Decoding organization: Bletchley park, codebreaking and organization studies. *Public Administration (London)*, 93(2), 547–549. <https://doi.org/10.1111/padm.12129>
- "Cypher - Dictionary definition." (n.d.) Vocabulary.com, <https://www.vocabulary.com/dictionary/cypher>
- "Decryption - Dictionary definition." (n.d.) Vocabulary.com, <https://www.vocabulary.com/dictionary/decryption>
- Erskine, R. (2013). Tunny reveals b-dienst successes against the "Convoy Code." *Intelligence and National Security*, 28(6), 868–889. <https://doi.org/10.1080/02684527.2012.746414>
- Goldman, I. L. (2017). William Friedman, geneticist turned cryptographer. *Genetics (Austin)*, 206(1), 1–8. <https://doi.org/10.1534/genetics.117.201624>
- Haigh, T. (2018). Thomas Harold ("Tommy") Flowers: Designer of the colossus codebreaking machines. *IEEE Annals of the History of Computing*, 40(1), 72–82. <https://doi.org/10.1135/ahc.2018.0005>
- Kahn, D. (2009). The fonds de moscou, TICOM, and the nerve of a spy. *Intelligence and National Security*, 24(6), 865–875. <https://doi.org/10.1080/02684520903320477>
- Kotani, K. (2005). Could japan read allied signal traffic? Japanese codebreaking and the advance into French Indo-china, September 1940. *Intelligence and National Security*, 20(2), 304–320. <https://doi.org/10.1080/02684520500134065>
- Mount, G. S. (2006). Delusions of intelligence: Enigma, ultra, and the end of secure ciphers. *Canadian Journal of History*, 41(3), 579–580. University of Toronto Press.
- Rezabek, R. (2012). TICOM: The last great secret of world war II. *Intelligence and National Security*, 27(4), 513–530. <https://doi.org/10.1080/02684527.2012.688305>
- Severance, C. (2012). Alan Turing and Bletchley Park. *Computer (Long Beach, Calif.)*, 45(6), 6–8. <https://doi.org/10.1109/MC.2012.197>
- Weichman, G. (2017). Ultra revisited, a tale of two contributors. *Intelligence and National Security*, 32(2), 244–255. <https://doi.org/10.1080/02684527.2016.1253221>

CORPORATE SOCIAL RESPONSIBILITY: TEMU AND THE GLOBAL ECONOMY

ANDREW HARRINGTON

The recent development of Colin Huang, CEO of Temu and of Pinduoduo, becoming the richest man in the People's Republic of China (PRC), has put the international spotlight on the rapid growth of Temu. With Pinduoduo operating as the parent company within the PRC and Temu as the American subsidiary, this creates a convoluted dynamic concerning their Corporate Social Responsibility (CSR) and transparency. (Fortune, 2024 p.2) Globally, Temu has seen a rapid growth pattern based on its ability to provide cheap products sourced from China along with utilizing an app-based system to entice consumers to purchase their products by offering "discounts" and "rewards". Pinduoduo, as the parent corporation, regulates Temu's Corporate Social Responsibility policy. It is believed that the company is able to hide many facets of their operation. By allowing direct shipping from mainland China, the company Temu has undergone scrutiny regarding their Corporate Social Responsibility policies, specifically in aspects of the environment.

Temu has publicly stated and acknowledged many different points that seemingly fit into a traditional Corporate Social Responsibility (CSR) policy. Their development of a next generation production model along with their efforts to foster a relationship between mindful buying practices are meant to offset their massive carbon emissions, but it gives cause for speculation. Their stated goal is to speed up production, reduce the waste coming from the supply chain cycle, and instill a sense of environmentally focused production among its consumers. The massive volume and variety of products offered within the Temu app provides consumers with

the ability to purchase and receive goods with a fast fulfillment cycle. In many cases it can entice consumers to visit and purchase more goods due to its purposeful and tactful app design. The design encourages an addictive mind-frame for the consumer that intentionally keeps them scrolling and coming back. Though they claim to lower their carbon emissions through the supply chain, one can certainly question their dedication to these responsibilities. Coupled with the fact that they are based in the PRC, factual and relevant information can be hard to obtain making Temu's true carbon footprint data difficult to quantify. Calin Van Paris states, "Thus far, Temu has offered little in terms of transparency around practices. The brand lists four values—"empowerment, inclusion and diversity, integrity, and socially responsible"—on its site, but with no details as to how those terms apply to the brand or its business model". (Brightly, 2024 p. 2) These four values can be found on their website after getting through a blistering number of ads, pop-ups, and other features to entice you to "buy now". (Temu, 2024) Considering all of this and Temu's Corporate Social Responsibility policy, their "environmental sustainability" is the most pertinent focus as it is a global company with a massive supply chain, logistical hurdles, and shipping challenges to overcome.

The Sustainable Development Goals (SDG) of 2023, enacted by the UN, outlines seventeen obtainable goals for companies to ensure they are within the bounds of sustainable environment practices. They are enumerated within the SDG and provide a level of protection to the global populace, all of which is aimed to be achievable by the year 2030. (UN, p.14) Temu's CEO Colin Huang, through Pinduoduo has stated, "We support the United Nations'

Sustainable Development Goals to end poverty, protect Earth and bring peace and prosperity to everyone around the globe. We continue to do our part to contribute toward these goals through our day-to-day initiatives.” (Pinduoduo, 2020) The Consumer-to-Manufacturer (C2M) policy is a stated goal within Temu and Pinduoduo’s Environmental, Social and Governance report. Its purpose is to change the way in which procurement and distribution is organized throughout the People’s Republic of China. Temu’s SDG plan seeks to “digitize” the supply chain which theoretically will streamline the traditional supply chain models, in turn benefiting the manufacturers in reaching their consumers. Pinduoduo aims to meet six specific goals outlined in their 2020 CSR to change the current strategy in regard to supply chains and distribution networks.

The goals Temu and Pinduoduo wish to achieve are thus:

Goal 7. Ensure access to affordable, reliable, sustainable and modern energy for all

Goal 8: Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all

Goal 9: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation

Goal 12: Ensure sustainable consumption and production patterns

Goal 13: Take urgent action to combat climate change and its impacts (Acknowledging that the United Nations Framework Convention on Climate Change is the primary international, intergovernmental forum for negotiating the global response to climate change)

Goal 17: Strengthen the means of implementation and revitalize the Global Partnership for Sustainable Development

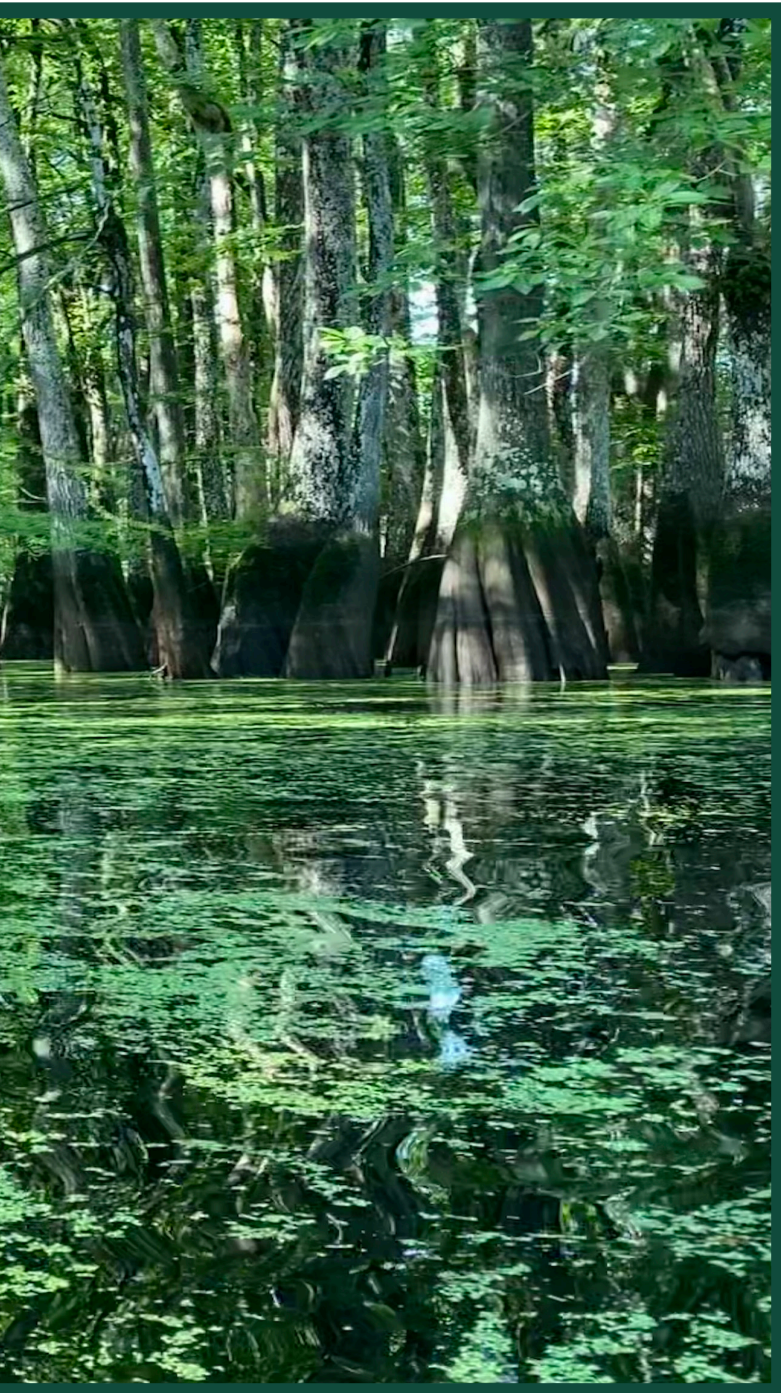
By eliminating specific steps that are environmentally unfriendly within their supply chain, Temu strives to cut down on excess packing with hazardous materials and create a more cost-effective distribution network. By focusing on goals eight, nine, and twelve, Temu is striving to change the mentality of consumers “from how much we can produce, to how much we should produce.” (Pinduoduo, 2020)

Utilizing their applications, Temu and parent company, Pinduoduo, can provide and share with manufacturers the specific information needed to cut out the unnecessary factors that cause environmental damage. By aggregating this information, companies will now be able to tailor their products specifically to meet their consumers’ demands. Much of this information is gathered from the Temu application by gathering data, analytical trends, and any other data point consumers may be unaware of. Packaging is a significant point of focus within Temu’s ESG from their stated focuses. Going paperless, in terms of billing and using biodegradable packaging materials is a major focal point of the company. Data collected within the company’s systems are also being utilized to plan much more efficient routes to cut down on their carbon footprint. (Pinduoduo, 2020) In theory, many of these policies seem feasible and practical but, Temu’s ESG lacks any data regarding their numbers and environmental impact. (Greenpeace, 2023, p.1) This lack of transparency is troublesome because it is not included within their report. This unfortunately leads to consumers being unaware of the true environmental impact of their purchases. In a society where consumers demand transparency and typically opt for an environmentally conscious brand, it is odd that consumers do not show concern while using Temu’s application. (Carrol et al. 2018) Based off Temu’s rapid growth, the success of their app, and the reveal of the Colin Huang as the richest man in the PRC, Temu appears to be continuing their successful trends despite the glaring lack relevant, factual, and necessary data. (Fortune, 2024)

The sustainability model of a company such as Temu that competes with other e-commerce companies such as Amazon, creates a sense of contradiction between what the consumer desires concerning transparency but also desiring the concept of “fast fulfillment and cheap.” Temu claims transparency in the quality of their products that they ship but has been scrutinized because of their inherent lack of upfront honesty. Products searched under “eco-friendly” populate with arguable listings that would be considered harmful to the environment due to the level of plastic, compounding with the amount of plastic waste already in the United States and many other western countries. (Brightly, 2024 p.3) Searching within the application, the term “sustainable”, it

and the influence of the Chinese Communist Party, Temu is able to hide a distribution and supply chain behind this political and geographical barrier. Temu's rapid rise in success and understanding of the e-commerce powered world we now live in does provide the company with the opportunity to become transparent and to act on their promises within their Environmental, Social and Governance report. The US based Temu e-commerce platform and company provides a perfect platform for the company to start focusing on their environmental impact, allowing consumers to view relevant data,

to streamline the site to be more transparent of their goals, and align itself to their promises within their ESG. As the global spotlight has shown upon Colin Huang as CEO, it is now more important than ever for Temu to start focusing on its global responsibilities. With the increased media coverage surrounding the announcement of Colin Huang's place as the richest man in the PRC, hopefully it becomes the catalyst in which a much needed and honest response is given not only to consumers but also the world. For a company to be ethical in today's global economy, these are standards that should be met by brands and demanded by consumers in principle.



About the Author - Andrew Harrington



Andrew Harrington is from Minneapolis, Minnesota. He earned his BA in History and Geography and is about to complete his Masters in Business Administration. After he graduates in 2025, he plans to continue in the business field with an emphasis on operations and supply chain management.

Works Cited

Brightly. (n.d.). Is Temu sustainable? A look inside the online marketplace. Brightly. Retrieved August 9, 2024, from <https://brightly.eco/blog/temu-sustainability>

Carroll, A. B., Brown, J. A., & Buchholtz, A. K. (2018). Business & society: Ethics, sustainability, and stakeholder management (10th ed.). Cengage Learning.

Fortune. (2024, August 9). PDD founder Colin Huang overtakes Zhong Shanshan to become China's richest person. Fortune. Retrieved August 9, 2024, from <https://fortune.com/asia/2024/08/09/colin-huang-pdd-founder-pinduoduo-temu-china-richest-person-overtakes-zhong-shanshan/>

Greenpeace. (2023). The deals behind Temu: Its hidden environmental price and climate silence. Greenpeace. Retrieved August 9, 2024, from <https://www.greenpeace.org/international/story/64710/the-deals-behind-temu-its-hidden-environment-price-and-climate-silence/>

Pinduoduo. (n.d.). Corporate responsibility. Pinduoduo. Retrieved August 9, 2024, from <https://en.pinduoduo.com/responsibility>

Pinduoduo. (2020). Environmental, social, and governance report 2020. Pinduoduo. Retrieved August 9, 2024, from https://global-uploads.webflow.com/5f068604be4f9d3890933b65/5f9900d519c42ee17894f189_PinDuoDuo-ESGReport_2020.pdf

Temu. (n.d.). About Temu. Temu. Retrieved August 9, 2024, from https://www.temu.com/about-temu.html?_x_sessn_id=s7s4zby3fs&refer_page_name=home&refer_page_id=10005_1723402495862_zcdgh4vr4h&refer_page_sn=10005

Transforming our world: The 2030 Agenda for Sustainable Development. (10/21/22015). [Resolution]. United Nations General Assembly. https://docs.un.org/en/A/RES/70/1Pcom/5f068604be4f9d3890933b65/5f9900d519c42ee17894f189_PinDuoDuo-ESGReport_2020.pdf

Temu. (n.d.). About Temu. Temu. Retrieved August 9, 2024, from https://www.temu.com/about-temu.html?_x_sessn_id=s7s4zby3fs&refer_page_name=home&refer_page_id=10005_1723402495862_zcdgh4vr4h&refer_page_sn=10005

Transforming our world: The 2030 Agenda for Sustainable Development. (10/21/22015). [Resolution]. United Nations General Assembly. <https://docs.un.org/en/A/RES/70/1>

SOCIAL WELL-BEING AND THE IMPORTANCE OF A THIRD PLACE

ROBERT ISAAC WILLIAMS

I. Introduction

Today the modern world suffers from social disconnect. We are unbalanced, we are unfulfilled, and we are unhappy. The solution to this social disconnect and unhappiness is a person's involvement in a "third place". A "third place" is a location where individuals will spend their spare time doing things they enjoy in a community. This could be a bar, a group of friends, a library, a club or intermural sport, or other locations. Naturally, there are three types of places that a person has in their life and a person's involvement in their "third place" is directly linked to their personal wellbeing and a society's social wellbeing. One's home and place of work does not count as these are "first places" and "second places" respectively. The research I present will measure the social disconnectedness of a person through five independent variables: Evenings spent at bars, with friends, with neighbors, religious service attendance, and the amount of social media a respondent uses. I analyzed the data produced from the Statistical Package for Social Sciences (SPSS) General Social Survey (GSS) data set and the variables above. Additionally, I will pursue the hypothesis that there is a positive relationship between the amount of time spent in a "third place" and a person's social connectedness.

II. Literature Review

I conducted literature reviews to provide a framework for this paper to pursue. In the Cornwell & Waite (2009) paper, "Social Disconnectedness, Perceived Isolation, and Health among Older Adults", they argue that the indicators of social

isolation vary across disciplines however they cite social networks and participation in events such as volunteering or religious attendance as measures of social isolation (p. 3). Furthermore, they identify a lack of integration in a community and companionship as factors in one's social disconnectedness (p. 4).

In Steptoe et al. (2013) paper, "Social Isolation, Loneliness, and All-Cause Mortality in Older Men and Women", the group analyzed the causes of mortality in the older generation. They found that social isolation was a main cause while identifying contact with friends, family and one's participation in organizations as measures of social isolation. Additionally, they discussed financial wealth and stability as a measure of welfare (p. 5).

The Parigi & Henson (2014) research, "Social Isolation in America", asked the question "Are contemporary Americans more isolated than ever before?" (p. 3). To measure this, they focused primarily on one's social media and internet usage. They argue that community should be the most important part of one's social life. In reference to a past article, *Bowling Alone*, they cite "contemporary Americans are participating less frequently in associational life, thereby undermining their connections with their neighbors and communities." (p. 5). With less participation in face-to-face socialization and a growing number of online interactions the paper argues that poor social health and disconnectedness is growing.

Finally, in the Larson (1996) paper, "The World Health Organization's Definition of Health: Social versus Spiritual Health", he addresses the World Health Organization's definition of health. They define health as "a state of complete physical,



Light of Men
Tyler Jacobs

mental and social well-being". From this Larson states that health "now includes mental and social dimensions." (p. 2). He goes on to argue that spirituality is a major part of one's social health (p. 9) and that spirituality is not exclusively one's participation in a religion but instead one's source of meaning through a community such as organized religion (p. 10).

III. Theory

After reviewing the literature above, I have identified five key variables as previously mentioned. While the literature mentions factors such as family this paper does not consider family as a "third place" because most family interactions happen at home. Additionally, they mention one's wealth and financial stability as a factor in one's health. I will not include these variables in my research as there are too many social economic variables that might affect one's social wellbeing. This paper will measure one's interactions with friends, neighbors, and communities as well as one's participation in social media and religion.

My final hypothesis is this: our social disconnectedness is positively related to one's use of social media but inversely related to one's participation in a religious organization and participation with friends, neighbors, and social spaces such as bars. The more that we use social media the unhappier we are while the more we attend "third places" the happier we are.

IV. Data and Analysis

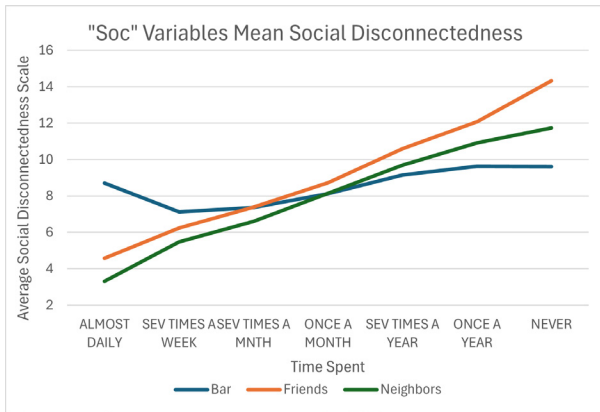
Using the SPSS GSS data set the dependent variable used for this paper will be *social_disconnect*. The dependent variable is an interval level variable scaled from 0-18 with higher numbers being a higher level of social disconnectedness.

The independent variables used in this paper also come from the SPSS GSS data set. They are: *socbar*, *socfriend*, *socommun*, *attend*, and *num_of_social*. The "soc" variables, *socbar*, *socfriend*, and *socommun*, all ask how often respondents spend evenings at bars, with friends, or neighbors respectively. The variable *attend* asks how often the respondent attends religious services. Finally, *num_of_social* is a computed variable made of the GSS variables, *snapchat*, *twitter*, *tumblr*, *facebook*, and *vine*, all of which measure if a respondent uses the respective social media. This variable is measured 5-10 with 10 being no usage and 5 being usage of all five applications. All variables will be weighted by *wtss*, the GSS weight variable.

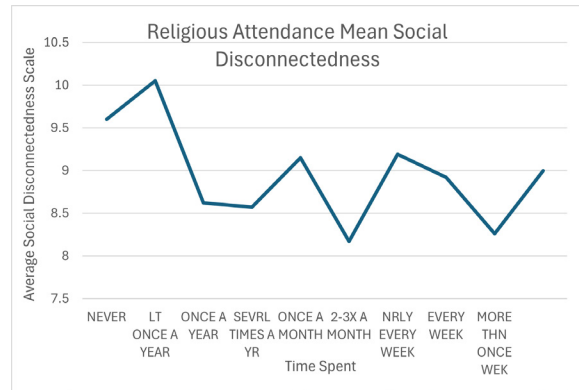
V. Bivariate Analysis

First, we will begin by comparing the relationship between the

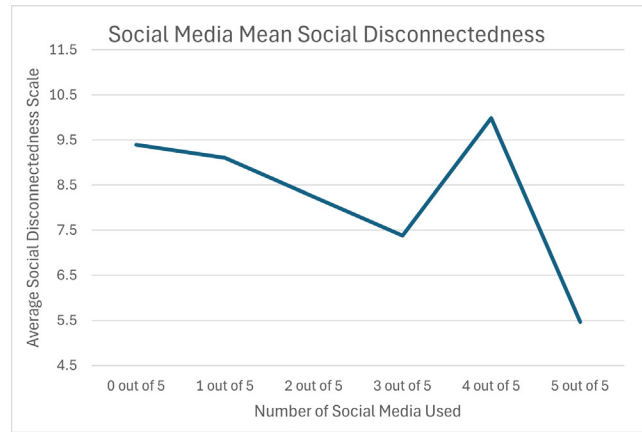
“soc” variables and social disconnectedness. When comparing the relationship between evenings spent at bars, with friends, or with neighbors and social disconnectedness the below graph and correlation was created:



As seen, on average, the less time one spends at a social location the higher they score on a social disconnectedness scale. When comparing the relationship between religious attendance and social disconnectedness the below graph and correlation was created:



When viewing the graph, it may be seen that there is no direct correlation between the variables. Someone who attends church more than once a week is more likely to score similarly to someone who attends once a month. The same may be seen for social media usage. Someone who uses no social media may score the same as someone who uses four of the five measured social media applications. Furthermore, if one uses all five of the social media applications, they, on average, score lower on social disconnectedness. When comparing the relationship between social media usage and social disconnectedness the graph and correlation below was created:



VI. Multivariate Analysis

Following the bivariate analysis, a multivariate analysis was conducted. This would work to determine the relationship between one’s social disconnectedness and the independent variables tested. In the first table, Model Summary, the value “Adjusted R Square” is a measure of how well a model reflects the data. It is measured on a scale of 0-1, the greater the value the better. In the second table, Coefficients², the value “Sig.” is a measure of statistical significance. A value that is less than 0.05 is considered good as it indicates 95% confidence in a measurement. Following the analysis the results were found below:

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.894 ^a	.799	.798	1.522

a. Predictors: (Constant), num_of_social, How Often R Attends Religious Services, Spend Evening With Neighbor, Spend Evening At Bar, Spend Evening With Friends

From the Model Summary table above, it is shown that the Adjusted R Square value of 0.798 is well above the standard 0.5 for statistical significance. Because of this the multivariate analysis should be considered over the bivariate analysis. Additionally, from the Coefficients table all values are statistically significant except for num_of_social which is under the statistically significant value of 0.05 with a value of 0.323. This shows there is no relationship between the number of social media used and social disconnectedness.

Model		Coefficients ^a					95.0% Confiden Lower Bound
		Unstandardized Coefficients B	Std. Error	Standardized Coefficients Beta	t	Sig.	
1	(Constant)	-.706	.513		-1.376	.169	-1.714
	Spend Evening At Bar	-.088	.036	-.044	-2.424	.016	-.159
	Spend Evening With Friends	1.160	.042	.514	27.909	<.001	1.078
	Spend Evening With Neighbor	1.063	.029	.639	36.130	<.001	1.005
	How Often R Attends Religious Services	-.057	.021	-.046	-2.665	.008	-.099
	num_of_social	.057	.057	.017	.988	.323	-.056

a. Dependent Variable: Social disconnectedness scale

VII. Results

The bivariate analysis worked to provide support for my hypothesis through viewing each variable separately. These analyses however did not consider other variables or how each individual variable may interact with each other. Meanwhile, the multivariate took these factors into account.

For the “soc” variables I hypothesized that they would all have a negative relationship. The more one spent time socially in “third places” the less social disconnectedness they would feel. I was correct in the hypothesis for the bivariate analysis, all variables, *socbar*, *socfriend*, and *soccommun* were significant at the .001 level. However, in the case of *socbar*, the multivariate analysis found significance at the .016 level which is not significant. Because of this result, there is no evidence to find a relationship between the time one spends at bars and their social disconnectedness. For the variables, *socbar* and *socfriend* the multivariate found both to be significant at the .001 level.

In the case of religious attendance I hypothesized that there would be a negative relationship. The more one attended a religious event the less social disconnectedness one would feel. The hypothesis was correct as bivariate analysis found the variable significant at the .001 level and the multivariate analysis found significance at the .05 level.

For the number of social media used I hypothesized a positive relationship. The more social media one used the more socially disconnected they would feel. While the bivariate analysis found no compelling evidence to support a positive or negative relationship it did find that no relationship was significant at the .001 level. However, the multivariate found that this was not significant, well above the

.05 level with a figure of .323. There is no evidence that social media affects one’s social disconnectedness nor is there evidence that it is significant.

VIII. Conclusion

We asked if one’s participation in a “third place” has any effect on one’s social disconnectedness and thus one’s wellbeing. Following the research, I found evidence that the more one spends time with friends, neighbors, or in social locations like bars and religious gatherings the less socially disconnected they will be. Additionally, despite the paper’s hypothesis, there is no relationship between those who use more social media and their social disconnectedness. There is evidence that a “third place”, a social life outside of what is required for basic function in modern society, is vital to one’s happiness. Thus, it is proven, all work and no play makes Jack a dull boy.

About the Author – Robert Isaac Williams



Robert Isaac Williams was born in Charleston, SC and hopes one day to work for the State Department. He is a junior in Palmetto Battery and political science major.

Bibliography

Cornwell, Erin York, and Linda J. Waite. “Social Disconnectedness, Perceived Isolation, and Health among Older Adults.” *Journal of Health and Social Behavior*, vol. 50, no. 1, 2009, pp. 31–48, <https://www.jstor.org/stable/20617618>. Accessed 23 Apr. 2024.

Larson, James S. “The World Health Organization’s Definition of Health: Social versus Spiritual Health.” *Social Indicators Research*, vol. 38, no. 2, 1996, pp. 181–192, <https://www.jstor.org/stable/27522925>. Accessed 23 Apr. 2024.

Parigi, Paolo, and Warner Henson. “Social Isolation in America.” *Annual Review of Sociology*, vol. 40, 2014, pp. 153–171, www.jstor.org/stable/43049530.

Stephens, Andrew, et al. “Social Isolation, Loneliness, and All-Cause Mortality in Older Men and Women.” *Proceedings of the National Academy of Sciences of the United States of America*, vol. 110, no. 15, 2013, pp. 5797–5801, <https://www.jstor.org/stable/42590308>. Accessed 23 Apr. 2024.

THERMAL MANAGEMENT SYSTEMS IN HIGH-SPEED AIRCRAFT

KYLIE COULSTON

1. Introduction

The influence of heat on aircraft plays a major role in the design and overall performance of high-speed aircraft. Many factors such as solar radiation, electronics, mechanics (i.e. heat from the engine), and air friction negatively affect the performance of the plane [1]. As modern-day fighter and supersonic jets increase in speed and electronic components, the heat produced from both friction and energy puts a greater strain on the aircraft. The implementation of thermal management systems (THMS) can reduce this problem and decrease a portion of the heat generated by the aircraft.

This report examines the current strategies for addressing the challenges posed by heat. It starts by explaining how heat impacts aircraft performance and safety. Then, it explores two heat-reducing solutions: thermal management systems (TMS) and thermal protection systems (TPS). The report also analyzes the limitations of these systems and concludes by considering potential future solutions.

2. Issues With Heat

Air friction, mechanics, and electronics make up the majority of the heat loads that affect aircraft. The heat produced by these elements results in high temperatures which act on aircraft walls and systems [2]. Heat loads are a common problem for all types of aircraft regardless of speed. Loads on subsonic planes, however, are drastically less when compared to their supersonic counterparts. Since the plane deals with a small load, engineers can utilize simpler

methods of cooling. As planes begin to go faster, and speeds increase to supersonic, the heat from air friction drastically increases causing temperatures to rise [1]. At the same time, the stress placed on engines for increasing speeds also produces more heat. For example, a plane traveling at Mach 6 (6 times the speed of sound) experiences a temperature increase in the body of around 600 °C (1,112 °F). If flight speeds are increased to Mach 8, the engine can experience temperatures of about 3,000 °C (5,432 °F). To put this in perspective, spacecraft reentering Earth's atmosphere can reach speeds of up to Mach 25, generating extreme temperatures that, "far exceed the working limits of standard combustion chamber materials" [2]. In such conditions, the fuel-air mixture within the engine cylinders becomes preheated and causes "combustion before the desired time" [3]. The extreme conditions often lead to the degradation of the aircraft's shape, structure, and material strength, increasing the possibility of aircraft system failure.

3. Thermal Management Systems (TMS)

Engineers use thermal management systems (TMS) to counteract unwanted heat [4]. Essentially, these systems transfer unwanted heat from the core components of the aircraft and distribute it to another source: the most common sources are heat sinks and thermal protective systems (TPS). Heat sinks work by gradually withdrawing heat away from the component and is usually made out of a conductive material or element that can easily absorb heat [5]. The heat sinks typically used in supersonic aircraft are fuel-to-air and air-to-air heat sinks. Thermal protective systems

4.2 Ablative Materials

Ablation is a form of energy management through the controlled consumption of materials [6]. When put into context as a thermal protective system, materials are made ablative to act as a sacrificial cover for high-heat situations. Materials are chosen based on their ability to absorb and re-radiate heat. Composite materials, which combine different chemical and physical properties, are often favored for their broad versatility and adaptability.

As the surface of the aircraft begins to heat to high temperatures, the heat is either reradiated or absorbed by the ablative material [6]. Multiple layers or materials are used to ensure that the aircraft is fully protected from the heat. Eventually, enough heat is absorbed by the outside layer and the material begins to decompose by burning up. Gasses formed by the burned material are pushed deeper into the other layers, thickening them and reducing heat transfer.

5. Limitations

Each thermal management and heat-protecting system has several limitations. Firstly, no single system can fully manage the heat produced by the aircraft, especially at high speeds; multiple systems must work in tandem to provide the cooling necessary to maintain operations. Additionally, many of these systems rely on consumable materials which will diminish over time or run out in the long term. For example, fuel-to-air heat sinks require fuel, transpiration requires coolant, and ablative material needs replacement due to wear.

Future aircraft design requirements may further constrain these systems. Advanced aerodynamics and stealth will drive new design choices that impact thermal management. For instance, fuel tanks may need to be downsized to account for weight-impacting fuel-to-air heat exchange while specific shapes for stealth may limit the availability of ram air holes within the body [11]. With the increase in electronic components and flight speeds, the current thermal management and protection systems may become inadequate. As a result, the development of more efficient systems is needed.

6. Emerging Technology

In tackling the challenge of increased heat loads, two main strategies stand out as potential solutions. The first approach focuses on utilizing intelligent management systems such as artificial intelligence (AI) to actively optimize thermal management systems in real-time. Using AI could allow for greater efficiency within the system to help mitigate heat. It would help make corrections when they are needed rather than using up resources to provide constant cooling. The second way would be to create a new system to manage heat. One example of this would be the use of nanofluids. Nanofluids are a type of coolant that contains nanoparticles. These particles create higher cooling capacities allowing for more heat to be absorbed. This system would most likely improve transpiration cooling and possibly act similarly to the fuel-to-air heat sink.

Each thermal management and protection system cannot fully sustain the heat produced by aircraft alone. They must work in combination with each other tackling different areas and heat sources within the plane. With today's current technology, heat can be managed, however, as aircraft technology continues to improve a better, more efficient system is needed.

7. Conclusion

Heat management is a critically important issue for high-speed aircraft. If not properly managed, damage to the aircraft and possibly injury to the pilot could occur resulting in a loss of funds, resources, and possibly a life. Using thermally managed systems and thermally protective materials, the heat felt on the aircraft can be reduced allowing for safe operation.

With the steadily increasing improvement of technology, current systems may not be able to sustain the load brought on by heat. Additional research is needed to improve heat conductors to further mitigate this issue.

About the Author – Kylie Coulston

Kylie Coulston is a sophomore cadet from Enola, Pennsylvania. She is a mechanical engineering major with a minor in aerospace sciences. After graduation, she plans to commission into Army and branch into Aviation.

References

- [1] "Aircraft thermal management: Practices, technology, system architectures, future challenges, and opportunities – ScienceDirect." Accessed: Oct. 14, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0376042121000701>
- [2] K. Li et al., "Evaluation of high-speed aircraft thermal management system based on spray cooling technology: Energy analysis, global cooling, and multi-objective optimization," *Appl. Therm. Eng.*, vol. 229, p. 120632, Jul. 2023, doi: 10.1016/j.applthermaleng.2023.120632.
- [3] "Aircraft Reciprocating Engine Cooling Systems and Maintenance," *Aircraft Systems*. Accessed: Oct. 23, 2024. [Online]. Available: <http://www.aircraftsystemstech.com/2017/04/engine-cooling-systems.html>
- [4] Y.-F. Mao, Y.-Z. Li, J.-X. Wang, K. Xiong, and J.-X. Li, "Cooling Ability/Capacity and Exergy Penalty Analysis of Each Heat Sink of Modern Supersonic Aircraft," *Entropy*, vol. 21, no. 3, Art. no. 3, Mar. 2019, doi: 10.3390/e21030223.
- [5] D. N. P. Group, "What are Heat Sinks? | Column | Solutions/Products/Services | DNP Dai Nippon Printing," Dai Nippon Printing Co., Ltd. Accessed: Oct. 16, 2024. [Online]. Available: https://www.global.dnp.biz/column/detail/10162228_4117.html
- [6] R. A. S. Beck, "Ablative Thermal Protection System Fundamentals," Jun. 15, 2013. Accessed: Oct. 15, 2024. [Online]. Available: <https://ntrs.nasa.gov/citations/20140000874>
- [7] M. R. Moroney, "Ram-air cooling systems for aircraft generators," *Trans. Am. Inst. Electr. Eng. Part II Appl. Ind.*, vol. 76, no. 4, pp. 217–221, Sep. 1957, doi: 10.1109/TAI.1957.6367231.
- [8] T. Scherer, R. Schmidt, and A. Solntsev, "Ram air based cooling and ventilation system for an aircraft," US8707721B2, Apr. 29, 2014 Accessed: Oct. 23, 2024. [Online]. Available: <https://patents.google.com/patent/US8707721B2/en>
- [9] "Thermal Protection Systems," *Tex Tech Industries*. Accessed: Oct. 23, 2024. [Online]. Available: <https://textechindustries.com/thermal-protection-systems/>
- [10] Q. Mi, S. H. Yi, D. D. Gang, X. G. Lu, and X. L. Liu, "Research progress of transpiration cooling for aircraft thermal protection," *Appl. Therm. Eng.*, vol. 236, p. 121360, Jan. 2024, doi: 10.1016/j.applthermaleng.2023.121360.
- [11] J. Wang, Y. Li, X. Liu, C. Shen, H. Zhang, and K. Xiong, "Recent active thermal management technologies for the development of energy-optimized aerospace vehicles in China," *Chin. J. Aeronaut.*, vol. 34, no. 2, pp. 1–27, Feb. 2021, doi: 10.1016/j.cja.2020.06.021.

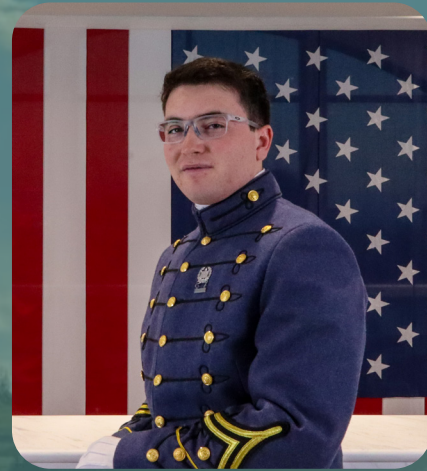


Vanta Glacier Blue Ice Cave
Zih-Syun Fu

PHOTOGRAPHERS



Chad Souders
2025
Marketing Major



Alexander Glover
2027
Supply Chain Management Major



Nicholas Paul
2025
Business Major



Daniel Melnikov
2025
Mechanical Engineering Major



Tyler Jacobs
2026
Intelligence and Security Studies Major



Anna Mart
2025 Graduate Student
Counselor Education, Art Education

AND ARTISTS

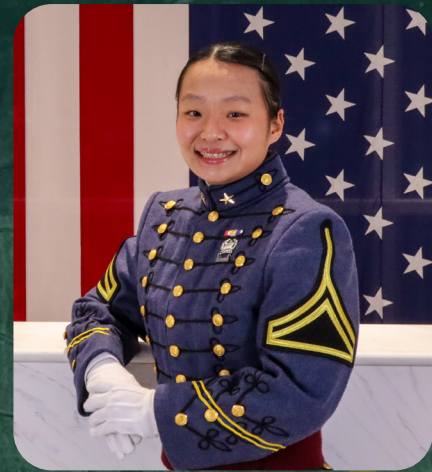


Wildflowers
Chad Souders

Jasmine Franklin
2026
Chemistry and Spanish Major



Wei Shan Lu
2027
Math Major



Zih-Syun Fu
2026
Math and Psychology Major



Michael Behrends
2025
Business Major



Gianna Marlow
2027 Graduate Student
School Psychology

INFRASTRUCTURE UNDER ATTACK: CYBER THREATS TO TRANSPORTATION

MATTHEW PINCHBECK

Keywords—Threat Actors, Transportation, Critical Infrastructure

I. INTRODUCTION - CRITICAL INFRASTRUCTURE

Critical infrastructure encompasses the systems and assets whose compromise would significantly impact national security, economic stability, public health, or safety within the United States. Such attacks can occur through physical means or cyber threats. The critical infrastructure framework is divided into sixteen key sectors, including Chemical, Commercial Facilities, Communication, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture,

Government, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation Systems, and Water and Wastewater Systems. Each sector plays a vital role in maintaining societal function, and an attack on any of them could have far-reaching consequences. Among these, the Transportation Systems sector stands out due to its interconnectedness with other critical sectors such as Food and Agriculture, Healthcare and Public Health, Emergency Services, Commercial Facilities, and Critical Manufacturing, highlighting the potential for cascading effects in a disruption [1].

II. TRANSPORTATION SYSTEMS AND SUBSECTORS

The Transportation Systems Sector encompasses the movement of various assets, including individuals and goods, from one location to another. This sector facilitates a wide range of travel methods, from subway systems for passenger transport to cargo transport in airplanes and the movement of materials through pipelines. It is organized into seven subsectors: Aviation, Highway and Motor Carrier, Maritime Transportation, Mass Transit and Passenger Rail, Pipeline Systems, Freight Rail, and Postal and Shipping. Each subsector is critical in ensuring efficient and safe transportation, supporting economic activities, and everyday mobility for the public [2].

1. Aviation

The aviation sector consists of a comprehensive network of approximately 5,193 public and 14,776 private airports, heliports, and landing strips, with around 500 designated for commercial aviation at civil and military facilities, including seaplane bases. It encompasses both commercial and recreational aircraft, both manned and unmanned, along with vital support services such as aircraft maintenance, refueling operations, navigation systems, and pilot training schools. Air traffic control systems are essential for coordinating this complex ecosystem, ensuring safe and efficient operations within the industry [2],[3].

2. Highway and Motor Carrier

The transportation network includes approximately 4.161 million paved and un-paved miles of roads, approximately 620,762 bridges, and over 500 tunnels, supporting a variety of vehicles such as trucks—some of which carry hazardous materials—as well as commercial

vehicles like motorcoaches and school buses. This extensive system also encompasses vehicle and driver licensing frameworks, traffic control systems, and cybersecurity measures to ensure effective operational oversight and safety across the network [2],[4],[5],[6].

3. Maritime Transportation

The maritime transportation system includes approximately 95,471 miles of coastline including Hawaii, Alaska, Pacific Islands, and Caribbean Islands. With over 300 ports, and over 25,000 miles of navigable waterways, supporting the efficient movement of people and goods. It also features intermodal landside connections that enhance accessibility and streamline transportation across water routes, ensuring effective integration with other modes of transport [2],[7],[8].

4. Mass Transit and Passenger Rail

The public transportation system includes terminals, operational frameworks, and infrastructure necessary for various passenger services such as transit buses, trolleybuses, monorails, heavy rail (subways or metros), light rail, and vanpool/rideshare options. In 2023, these services collectively facilitated around 10.8 billion trips, highlighting their crucial role in providing accessible transportation for the public [2].

5. Pipeline System

The pipeline network spans over 2.5 million miles across the country, transporting nearly all the nation's natural gas, about 65 percent of hazardous liquids, and various chemicals. This extensive system is supported by above-ground facilities, including compressor and pumping stations, which are essential for maintaining its operational efficiency [2].

6. Freight Rail

The rail transportation system is comprised of seven major carriers and numerous smaller railroads, featuring more than 138,000 miles of active track, over 1.33 million freight cars, and around 20,000 locomotives. Approximately 12,000 trains operate daily, while the Department of Defense has identified 30,000 miles of track and

infrastructure as essential for the mobilization and resupply of U.S. forces [2].

7. Postal and Shipping

The mail and package delivery system processes about 720 million items daily. It includes major integrated carriers, regional and local courier services, postal services, mail management companies, and specialized chartered delivery options. This extensive network ensures efficient handling and distribution of mail and packages across various regions [2].

III. THREAT ACTORS

The term "threat actor" refers broadly to any individual or group that poses a risk to cybersecurity, encompassing a variety of malicious entities. These actors, including cybercriminals, hackers, cyber terrorists, insider threats, and script kiddies, intentionally harm digital systems by exploiting vulnerabilities in computer networks and software to carry out attacks such as phishing, ransomware, and malware incidents. Sophisticated cyber actors, particularly nation-states, seek to steal sensitive information and disrupt essential services, making robust defenses critical for national security. Protecting cyberspace is a collective responsibility that includes individuals, families, businesses, and government agencies. By effectively preventing or swiftly mitigating attacks, the influence of these threat actors can be diminished, as even minor cyber incidents pose significant risks that must be identified and addressed [9],[10],[11],[12].

There are six distinct types of threat actors: cybercriminals, nation-states, hackers/ideological, thrill seekers/script kiddies, insider threats/competitors, and cyberterrorists. Each type exhibits varying levels of capabilities, motivations, and financial backing, which influence their methods and goals in the cyber landscape [9],[10],[11],[12].

1. Cybercriminals

Cybercriminals are individuals or groups that exploit digital technology to commit crimes primarily for financial gain, using tactics like

phishing, ransomware, and identity theft to target individuals and organizations. They often employ social engineering techniques to deceive victims into revealing sensitive information or transferring money. These threat actors may operate independently or as part of organized crime, and their attacks can lead to significant financial losses, particularly in sectors like finance and healthcare. Cybercriminals adapt their methods as technology evolves, increasingly using AI tools and fileless malware to bypass security measures. To counter these threats, organizations and individuals need to maintain updated systems and adopt strong cybersecurity practices, including complex passwords and awareness training [10],[11],[12].

2. Nation-state

Nation-state actors are sophisticated threat actors conducting cyber activities on behalf of specific governments, motivated primarily by political or economic objectives. Backed by significant financial resources and advanced technological capabilities, these actors pose serious risks by targeting critical infrastructure, conducting espionage, and interfering in elections, as seen with Russian hackers in the 2016 and 2020 U.S. elections. Their tactics include advanced persistent threats (APTs) that

allow them to infiltrate networks undetected for extended periods and supply chain attacks targeting defense contractors and third-party providers. To mitigate these risks, organizations

must implement robust monitoring, threat intelligence, and rapid incident response strategies to protect national security and sensitive information [9],[10],[11],[12].

3. Hacktivists / Ideological

Hactivists / Ideological are politically motivated threat actors who use hacking to promote social change, targeting individuals, organizations, or government agencies they view as opposing their beliefs. Unlike ethical hackers, hactivists operate independently and often employ tactics such as website defacement, data exposure, and distributed denial-of-service attacks to make political statements, as the group Anonymous advocates for free speech. While they do not seek personal gain, their disruptive actions can severely damage an organization's reputation and operations, necessitating effective public relations strategies for recovery. Often working with limited resources, hactivists exploit security vulnerabilities and utilize open-source tools to carry out their campaigns [10],[11],[12].

4. Thrill Seekers / Script Kiddies

Thrill seekers and script kiddies are opportunistic threat actors primarily motivated by boredom and the desire for amusement rather than political or financial gain. Script kiddies lack

5. Insider Threats / Competitors

advanced technical skills, relying on existing scripts and tools to hack into systems, while thrill seekers engage in hacking for personal enjoyment and notoriety. They typically target organizations with weak security, using distributed denial of service (DDoS) attacks or website defacement to create chaos rather than cause significant harm. Although often seen as less sophisticated, their activities can still disrupt operations and pose security risks, necessitating proactive cybersecurity measures like strong authentication, regular software updates, and continuous monitoring to mitigate potential damage [10],[11],[12].



A Snowy Sunset
Alexander Glover

Insider threats pose significant challenges for organizations as they originate from individuals within the network, such as employees, contractors, or board members, who may misuse their privileged access. These threats can be categorized into malicious insiders, who intentionally harm the organization for personal gain, and incautious insiders, who inadvertently cause data breaches through negligence. According to the 2021 Verizon Data Breach Investigations Report, insider threats account for over 20% of data breaches, primarily due to privilege abuse. Additionally, competitive intelligence and corporate espionage can involve malicious tactics to steal sensitive information from competitors. To combat these risks, organizations must implement strong access controls, employee training, and monitoring solutions like "Teramind," which offers real-time activity tracking, sensitive data classification, and auditing features to detect and prevent insider threats effectively [9],[10],[11],[12].

6. Cyber terrorists

Cyber terrorists aim to inflict harm and disruption through politically or ideologically motivated cyberattacks, targeting businesses, state machinery, and critical infrastructure to further their agendas. These threat actors can be individuals, non-governmental groups, or nation-state actors, and their actions often threaten or lead to violence, mirroring the goals of physical acts of terrorism [10],[11],[12].

IV. COMMON TYPES OF CYBER ATTACKS ON THE TRANSPORTATION SECTOR

1. Ransomware Attacks

Ransomware attacks involve encrypting data and demanding a ransom for its release. High-profile incidents have affected railways and shipping companies, disrupting operations and causing significant financial losses.

Ransomware attacks have increasingly targeted critical infrastructure, including logistics, rail, and government entities, with malicious actors evolving their techniques to extort ransom by encrypting files and demanding payment for decryption. Effective detection and analysis during such incidents involve promptly isolating

impacted systems to contain the spread of the malware, prioritizing the restoration of critical systems, and conducting thorough forensic investigations to identify precursor malware and unauthorized activities. In the case of cloud resources, tools should be used to prevent modifications to key security resources and automate responses to suspicious changes.

Incident response should be guided by a clear communications plan, ensuring timely updates to internal and external stakeholders, including relevant authorities such as CISA, FBI, or local law enforcement. Containment and eradication efforts focus on identifying and disabling known ransomware binaries, securing systems from unauthorized access, and preventing further data exfiltration. Following containment, recovery steps should prioritize critical services and data restoration from clean backups while ensuring that systems are not re-infected. The post-incident phase involves documenting lessons learned, updating cybersecurity policies and procedures, and sharing relevant findings with the broader security community to improve future defenses. This structured approach enables organizations to respond effectively to ransomware incidents and minimize long-term operational impact.

2. Social Engineering Attacks

Manipulation of employees or individuals causes them to reveal sensitive information or grant access to secure systems. Social engineering attacks come in a variety of forms, including: phishing, fake emails or websites to solicit personal information by masquerading as legitimate organizations; whaling, a targeted form of phishing, focusing on high-level executives after conducting thorough research; vishing, leverages phone calls to impersonate trusted parties and extract sensitive data; baiting, promises rewards to lure victims into divulging personal information or installing malware; diversion theft, where attackers redirect packages or information; Business Email Compromise (BEC), which targets organizations by impersonating executives to request financial transfers or change payment details; smishing (SMS phishing), which takes advantage of text messages to lead users to malicious links; quid pro quo, where HACKERS attack through

offering services in exchange for credentials; pretexting, which creates a plausible scenario to convince victims to reveal sensitive information; honeytrapping, where exploiters utilize personal relationships via dating sites to gain financial or personal data; and tailgating/piggybacking, where attackers gain physical access to secure facilities by following authorized personnel.

Social engineering attacks remain a significant cybersecurity threat despite being less frequent than technical attacks. These attacks manipulate individuals into revealing sensitive information, sharing credentials, or granting unauthorized access to devices or systems. Since many attacks begin with personal interactions that exploit human error, they can pave the way for more severe compromises, particularly in organizations. Cybercriminals often invoke emotions like empathy, fear, and urgency to trick individuals into disclosing valuable information. Common types of social engineering attacks include phishing, whaling, baiting, business email compromise (BEC), and smishing, each exploiting different communication channels (email, SMS, voice) and psychological tactics.

To prevent social engineering attacks, individuals and organizations must stay vigilant, maintain robust security practices, and educate users on recognizing suspicious activities. Common indicators of phishing include unusual sender addresses, generic greetings, spoofed links, poor grammar, and unsolicited attachments. Employees should verify suspicious communications directly with the source and avoid providing sensitive information unless they know the requester's identity. Using multi-factor authentication (MFA) and maintaining updated security software can also reduce the risk of falling victim to such attacks.

If an individual suspects they have been targeted, they should report the incident to internal security teams, change passwords immediately, monitor financial accounts, and, if necessary, contact law enforcement. Recognizing signs of social engineering—such as urgent requests for personal information or incorrect links—resisting the urge to click on suspicious links and deleting questionable messages are key steps to staying safe.

3. Distributed Denial-of Service (DDoS) Attacks

Attacks are aimed at overwhelming transportation websites and services, disrupting ticket sales, and causing operational delays.

A Denial-of-Service (DoS) attack occurs when a malicious actor disrupts access to network resources, such as websites or online services, by overwhelming the target with excessive traffic. This results in service unavailability for legitimate users, causing operational disruptions and financial losses. Common DoS techniques include flooding a server with requests, Smurf attacks (where broadcast packets are sent to multiple hosts with a spoofed target IP), and SYN floods (which exploit the transition control protocol handshake to occupy server ports).

Distributed Denial-of-Service (DDoS) attacks take this a step further, using a network of compromised devices—often part of a botnet—to launch a coordinated attack, increasing the volume and impact of the traffic. DDoS attacks are more complex to trace as they involve multiple sources and can leverage vulnerable Internet of Things (IoT) devices.

To prevent being part of a DDoS attack, organizations should secure their internet-connected devices, implement firewalls, use DoS protection services, and develop disaster recovery plans. Symptoms of a DoS or DDoS attack include slow network performance, inaccessible websites, and system unresponsiveness. Detection can be facilitated by monitoring network traffic through firewalls or intrusion detection systems. In case of an attack, it is critical to involve technical professionals to mitigate the attack, communicate with service providers for support, and monitor other systems to avoid secondary attacks.

4. Supply Chain Attacks

Targeting third-party vendors to compromise larger networks is becoming more prevalent but is still a smaller percentage overall.

5. Malware Infections

Malware infections are used to infiltrate systems, allowing attackers to steal information or disrupt operations.

6. IoT Vulnerabilities

The increasing use of IoT devices in transportation has created new attack vectors where vulnerabilities in these devices can be exploited.

V. KNOWN THREAT ACTORS

1. Threat Actors Targeting Transportation

a. FIN7

A financially motivated cybercriminal group has been active since 2013, primarily targeting industries such as retail, hospitality, finance, healthcare, and transportation. Initially, they focused on point-of-sale (POS) malware to steal payment card data, often operating under the facade of a front company, Combi Security. Since 2020, FIN7 has shifted to a Big Game Hunting (BGH) approach, leveraging sophisticated ransomware operations, including REvil and its own Ransomware-as-a-Service (RaaS) platform, Darkside. While it may be linked to the Carbanak Group, multiple groups use Carbanak malware, which results in separate tracking. FIN7's operations focus on high-value targets for financial gain, often through large-scale ransomware campaigns.

b. Leviathan

Leviathan is a Chinese state-sponsored cyber espionage group linked to the Ministry of State Security (MSS), specifically the Hainan State Security Department, and an affiliated front company. Active since at least 2009, Leviathan has targeted a wide range of sectors, including academia, aerospace, biomedical, defense, government, healthcare, manufacturing, maritime, and transportation. Their operations span globally, with activity reported in the U.S., Canada, Europe, the Middle East, and Southeast Asia. The group focuses on intelligence gathering and cyber espionage, typically supporting Chinese national interests.

c. TA2541

TA2541 has been a cybercriminal group active since at least 2017, primarily targeting industries such as aviation, aerospace, transportation, manufacturing, and defense. The group's campaigns are typically high-volume and involve the use of commodity remote access tools (RATs), which are often obfuscated using crypters. TA2541's attacks commonly feature themes related to aviation, transportation, and travel, likely to increase the likelihood of successful social engineering and phishing efforts. Their operations are focused on broad-scale intrusions aimed at stealing sensitive data and compromising networks.

d. Tropic Trooper

Tropic Thunder is a threat group active since 2011. The group has been known for conducting targeted cyber campaigns against entities in Taiwan, the Philippines, and Hong Kong. The group primarily targets government, healthcare, transportation, and high-tech industries, using a range of cyber espionage tactics to infiltrate networks and steal sensitive data. Tropic Trooper's operations are typically focused on geopolitical interests in the Asia-Pacific region, consistently emphasizing intelligence gathering and disruption of critical sectors.

e. HEXANE

HEXANE is a cyber espionage threat group that has been active since at least 2017, primarily targeting organizations in the oil and gas, telecommunications, aviation, and internet service provider sectors. Its operations have focused on companies in the Middle East and Africa, with victims located in countries such as Israel, Saudi Arabia, Kuwait, Morocco, and Tunisia. HEXANE's tactics, techniques, and procedures (TTPs) show similarities to those of APT33 and Oil Rig. However, it is tracked as a distinct entity due to differences in target organizations and tools used. The group's activities are likely aimed at intelligence gathering and disrupting critical infrastructure in the region.

f. APT33

A suspected Iranian state-sponsored threat group has been active since at least 2013. The group has targeted various industries, focusing on the aviation and energy sectors. Its operations

c. The use of single-factor authentication for remote or administrative access to systems supporting the operation of Critical Infrastructure and National Critical Functions (NCF) is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

2. Safe Practices

a. Cyber Hygiene Services: CISA offers several free scanning and testing services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

b. Elections Cyber Tabletop in a Box: A self-guided resource, CISA developed the Elections Cyber Tabletop Exercise Package (commonly called "tabletop in a box") for state, local, and private sector partners. The package includes template exercise objectives, scenarios, discussion questions, and a collection of cybersecurity references and resources.

c. Malicious Domain Blocking and Reporting: This service is available for U.S. state, local, tribal, and territorial government members of the Multi-State Information Sharing and Analysis Center and Elections Infrastructure Information Sharing and Analysis Center in partnership with CISA and Akamai.

d. Nationwide Cybersecurity Review: This free, anonymous, annual self-assessment measures gaps and capabilities of state, local, tribal, and territorial governments' cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by The U.S. Department of Homeland Security and the Multi-State Information Sharing and Analysis Center.

VII. CONCLUSION

Critical infrastructure is a colloquial term that can define many sectors, including transportation, energy, and supply chains. It may seem difficult to hack a highway, but vulnerabilities lie latent in our systems and processes. A growing rogues gallery of malign actors is constantly attempting

to degrade these sectors in the United States. These groups may be agents of a nation state or independent actors, however fundamental practices (when employed correctly and consistently) can go a long way in ensuring the cybersecurity of national critical infrastructure systems from coast to coast.

About the Author - Matthew Pinchbeck



Matthew is majoring in Computer Science and Cyber with a minor in Computer Engineering. He is from Albany, New York. After graduation in 2026, he plans to do freelance security work, enjoy being a father, and writing.

References

[1] CrowdStrike, "What is a Threat Actor?" [Online]. Available: <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/threat-actor/>. [Accessed: Oct. 30, 2024].

[2] SentinelOne, "Understanding Threat Actors," [Online]. Available: <https://www.sentinelone.com/cybersecurity-101/threat-intelligence/threat-actor/>. [Accessed: Oct. 30, 2024].

[3] IBM, "Threat Actor," [Online]. Available: <https://www.ibm.com/topics/threat-actor>. [Accessed: Oct. 30, 2024].

[4] Teramind, "Types of Threat Actors," [Online]. Available: <https://www.teramind.co/blog/types-of-threat-actors/>. [Accessed: Oct. 30, 2024].

[5] Statista, "Number of Airports in the United States from 1990 to 2023," [Online]. Available: <https://www.statista.com/statistics/183496/number-of-airports-in-the-united-states-since-1990/>. [Accessed: Oct. 30, 2024].

[6] U.S. Bureau of Transportation Statistics, "Public Road and Street Mileage in the United States by Surface Type," [Online]. Available: <https://www.bts.gov/content/public-road-and-street-mileage-united-states-type-surface>. [Accessed: Oct. 30, 2024].

[7] Statista, "Number of Road Bridges in the United States from 2000 to 2023," [Online]. Available: <https://www.statista.com/statistics/190386/number-of-road-bridges-in-the-united-states/>. [Accessed: Oct. 30, 2024].

[8] U.S. Department of Transportation, "National Tunnel Inventory," [Online]. Available: <https://geodata.bts.gov/datasets/usdot:national-tunnel-inventory/about>. [Accessed: Oct. 30, 2024].

[9] American Oceans, "Facts About the U.S. Coastline Length," [Online]. Available: <https://www.americancoastlines.org/facts/us-coastline-length/>. [Accessed: Oct. 30, 2024].

[10] U.S. Department of Transportation, "Ports," [Online]. Available: <https://www.maritime.dot.gov/ports/ports>. [Accessed: Oct. 30, 2024].

[11] U.S. Department of Transportation, "Navigable Waterway Network Lines," [Online]. Available: <https://geodata.bts.gov/datasets/usdot:navigable-waterway-network-lines/about>. [Accessed: Oct. 30, 2024].

[12] American Public Transportation Association, "APTA Update Q4 2023," [Online]. Available: <https://www.apta.com/research-technical-resources/transit-statistics/ridership-report/ridership-report-archives/>. [Accessed: Oct. 30, 2024].

[13] Cybersecurity and Infrastructure Security Agency (CISA), "Critical Infrastructure Sectors," [Online]. Available: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>. [Accessed: Oct. 30, 2024].

[14] Cybersecurity and Infrastructure Security Agency (CISA), "Transportation Systems Sector," [Online]. Available: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector>. [Accessed: Oct. 30, 2024].



Snow Capped Mountains



Bear Camp



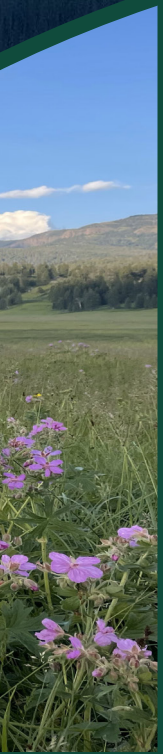
Valley of Flowers



Grand Canyon of Yellowstone



Yellowstone Views



"These photos depict just a few of some of the most awe-inspiring moments during my summer adventure. From snow-capped mountains as far as the eye can see to a mesmerizing sunset accompanied by bighorn sheep, these moments altered the course of my life for the better.

It has become my goal to share my experience with others in an attempt to rekindle our society's love for our most precious gifts: the natural environment. The tranquility and other-worldly feelings oftentimes joining these pristine lands cannot be described by words, only by experience."

-Chad Souders

Sheep and a Sunset

CYBERATTACKS: WHO IS AT FAULT?

KIRIN CHAPLIN

1 Introduction

Cyberattacks are growing in prevalence in today's digital world for a multitude of reasons. One reason is that as organizations and the digital landscape expands and increases in complexity, there is inherently more attack surface area [1]. This allows for new risks to be introduced to the digital environment and increases the possibility of systems being vulnerable. Bring Your Own Device (BYOD) policies are another reason for the increase in attacks on organizations [1]. BYOD allows individuals to deploy personal devices that may be malicious into the organization's environment. This can lead to the spread of malware across the organization's network.

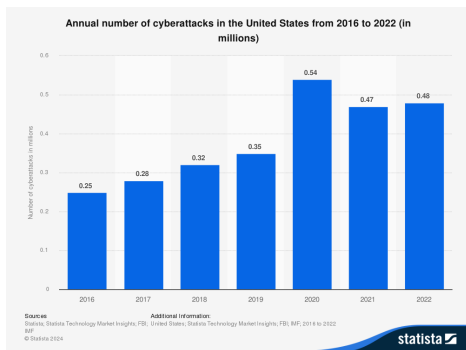


Figure 1: Number of cyberattacks in the U.S. 2016-2022 [2]

As shown in figure 1, we can infer how BYOD policies, due to COVID-19, led to an increase in attacks in 2020. BYOD policies were necessary due

to the nature of not wanting to share workspace with other employees and the high number of employees working from home or working in a hybrid environment. This environment led to an increasing number of cyberattacks within the United States. Organizations also rely on third-party vendors or commercial off-the-shelf (COTS) software, which may have vulnerabilities that are then exploited by attackers. Finally, there is an increase in the sophistication of those who would do harm. In this paper, we will discuss the intricacies of cyberattack vectors and how an attacker may commit their attack, the role of the attacker and the defender, and how fault can be determined. To determine fault, we will look to not only how famous cyberattacks found fault but also explore fault attribution within third-party vendor regulations and technologically involved industries.

2 Attack Vectors

Attack vectors are the methodologies attackers use to carry out their cyberattacks. There are three key types of cyberattack vectors: social engineering, malware, and cyberwarfare. These categories can then be further broken down. Attackers will oftentimes use a variety of tactics, techniques, and procedures (TTPs) when conducting an attack to carry out their actions in a covert manner.

2.1 Social Engineering

Social engineering involves sending a fake message via email (phishing), phone call (vishing), or text message (smishing or SMS phishing). Attackers may also perform a spear phishing attack, which is where the attacker specifically targets and tailors their phishing

attack to a person or organization. This attack vector relies on the victim's human nature and having empathy for others. The fraudulent message sent during a phishing attack may request that the victim provides information that they are not supposed to disclose. This illustrates why this attack vector relies on the human victim to make the mistake and disclose the information. Social engineering could also involve allowing someone who is not authorized into a building by holding the door for them. This attack is known as tailgating. To do this, the attacker could simply pose as someone with their hands full. Generally, as humans we would then hold the door open for the next person, so they do not have to set all their stuff down. While this person may have legitimate access to the building, it could also be someone trying to gain access to a room or building they are not supposed to be in. The attacker may then be able to gain physical access to cyber systems, which could allow them to directly harm the systems or put malware on the system. This cyberattack vector is more commonly used to gather more information about the attacker's target and can aid in reconnaissance.

2.2 Malware

Malware consists of malicious code that makes a computer or system act in an undesirable manner. This attack vector can be carried out through ransomware, which is the stealing and encrypting of data, where the attacker then requests something in return for the victim to get their data back. Another way to implement malware into an attack would be through a trojan horse. This kind of malware masquerades as an executable that the victim does not believe is malicious and that the machine trusts. These factors make it more likely that the malware will be run on the system. Malware can also be used via worms and viruses. A worm is malicious code that self-replicates on other computers/systems within a network and a virus is malicious code that requires user action to spread. Malware can utilize social engineering to get initial access into a computer system and malware can be embedded within a social engineering attack as a link or attachment.

2.3 Cyberwarfare

Cyberwarfare is a broad category to describe cyberespionage and cyberterrorism. Cyberespionage is the use of malware to steal data from organizations and governments [1]. Cyberespionage is done by another nation-state or entity acting on behalf of, or to further another country's national interests. Attackers committing cyberespionage typically target data related to employee records, customer data, business information, and intellectual property. Cyberterrorism is the intimidation of government or civilian population by using technology to disable critical national infrastructure to achieve political, religious, or ideological goals [1]. This attack vector is the most sophisticated and utilizes any TTPs necessary to ensure that the nation-state behind the attack either gathers the data they are seeking or inflicts the harm/fear they want to incite.

2.4 Cyberattack Case Studies

There are many famous examples of cyberattacks, but this section will focus on examples of attacks where fault attribution came into question. The first example is the SolarWinds attack, which was a supply chain attack. In this case the attackers injected malicious code (SUNBURST) into a software update. Once the systems received the malicious update, SUNBURST allowed attackers to have a backdoor into systems. Fault in this example is questioned because many argued that the SolarWinds Chief Information Security Officer (CISO) failed to secure their systems and was aware of critical vulnerabilities within their systems which further perpetuated the impact of the attack. Another example is the AT&T data breach that exposed AT&T customers' call and message records. This breach occurred by attackers exploiting misconfigured application programming interfaces (APIs), which then allowed them to query for sensitive customer details. Fault, in this example, is also a grey area because the attack was a Zero-Day exploit, meaning the vulnerability was unknown to the organization and the vendor had zero days to prepare a patch for the vulnerability, but due to the misconfigured APIs and the lack of resolution for those affected made victims blame AT&T for the breach. The final example is the flawed update from CrowdStrike. This flawed update, while not a malicious attack, disrupted many IT

systems that relied on Windows machines. Since CrowdStrike was providing a third-party service to Microsoft and then pushed it to all Windows machines it is alarming that a flawed update would cause system failures. This example brings into question contractual limitations within the area of fault since CrowdStrike provided a service to Microsoft. Overall, each of these incidents were extremely intricate attacks, or flawed security updates, and include grey area within the United States' legal system.

3 Attacker vs. Defender

To determine fault in a cyberattack we must also understand each person's role within an attack. The attacker is the person carrying out the cyberattack through various vectors to achieve their goal or gather the data they are seeking. As a defender, one must protect against cyberattacks by doing their due diligence to secure systems and the organization. In practice, that means continuously monitoring systems to prevent and detect threats while also predicting the "crown jewels" the attackers may attempt at getting access to.



Figure 2: 6-Step Cycle for Incident Response and Mitigation [3]

Within continuous monitoring and prevention, the defender should be doing risk analysis based on their findings. Not every vulnerability is a critical vulnerability, but that does not mean that it should not have a mitigation plan or a risk waiver that the organization is willing to accept. In addition to continuous monitoring, the defender must ensure that the entire workforce is properly trained in basic cybersecurity tradecraft. This means training in password requirements, phishing tactics, BYOD policies, and other social engineering tactics like tailgating.

The defender is also responsible for responding to a cyberattack, meaning the defender should have a plan or framework in place for responding to an incident. The defender needs to be able

to identify when an incident has occurred in a timely manner, then contain the malware or infected systems to prevent the further spread and impact of the attack. Next, the defender needs to eradicate not only all the malicious artifacts, but also needs to determine and get rid of the attack vectors that caused the incident. Then, the defender needs to recover from the incident by restoring the organization to normal operation and improving the organization's security posture accordingly.

3.1 Leadership

The Chief Information Security Officer (CISO) and the Chief Executive Officer (CEO) of organizations are senior executives who are responsible for developing and implementing security strategies to protect their organization's systems and information. Within this leadership role, one must be able to communicate with technical and non-technical staff, manage the security staff, oversee the development and implementation of security policies, understand network activity and potential threats, and report threats to those who need to be made aware. While the CEO/CISO is responsible for ensuring reasonable security of their organization, no one can protect against the "unknown, unknowns." In the case of SolarWinds, "The SEC's complaint alleges that Brown was aware of SolarWinds' cybersecurity risks and vulnerabilities but failed to resolve the issues, or at times, sufficiently raise them further within the company" [4]. In this example, the CISO allegedly failed to perform one of his main job responsibilities, by insufficiently raising the issues within the company. The CISO needs to perform due diligence and provide due care to protect the organization's data and systems. The securities and exchange commission (SEC) argued that insufficient cybersecurity measures, mainly the ones that led to the SUNBURST attack, led to a violation of Section 13(b)(2)(B) of the Securities Exchange Act of 1934. In August 2024, the court dropped the case saying, "the SEC is not authorized to charge internal accounting control violations that are not specifically tied to financial accounting" [5]. Additionally, the court found that "the SEC was separately incorrect in concluding that the incidents and vulnerability at issue should have been escalated under the incident response plan; while these were later found to be related to the compromise discovered in December



2020, none were objectively significant at the time, and the SEC's claim 'has traction only with the benefit of post-[incident] hindsight' " [5]. In the case of SolarWinds, it was found in court that the CISO did do the job accordingly because it is not reasonable to expect protection against something that is unprecedented and that was funded by another nation-state. Additionally, after examining how complex cyberwarfare can be, it would be unfair to punish a defender based on an attack as complex as SolarWinds.

3.2 *Determining accountability*

After reviewing the roles of the attacker, defender, and the responsibility of leadership we can begin to discuss accountability. When discussing accountability, we should keep in mind that ultimately the cyberattack occurred because the attacker decided to perform the attack, but we must also discuss if the defender should be held accountable as well if he or she fails to provide due care to secure the organization.

One benefit of holding the defender accountable would be that you are not only punishing someone who failed to provide what they said they would, but also setting a precedent to deter others from doing so as well. It would hold leadership truly responsible for any IT issue within their organization and deter not only the CISO, but those under her or him, from doing something that would be unauthorized. This, however, could not only deter people from

wanting to be in the CISO position, but also could inhibit those individuals from performing their job. If an individual is constantly worried about messing up, or over reporting insignificant incidents it could lead to more chaos than if organizations kept the status quo for accountability. Additionally, if we determine the defenders can be held accountable, then some may also misplace the blame. People should remember that the attacker should receive majority of the blame for carrying out the attack, but, depending on the scale and impact of the attack, punishing the defender could be an avenue for holding the defender accountable for securing their organization.

4 **Other players**

Many companies in today's digital age use third-party vendors or commercial-off-the-shelf (COTS) software to save both time and resources from being put into general applications. While this idea is cost-effective for companies, it also introduces a new area of risk for the defender of that organization using that generalized application. This risk comes from the fact that the defender is not in charge of the security of the application as a single part but must also ensure that it runs securely within the organization's environment as whole. The CrowdStrike outage that occurred in July 2024 is a prime example of how the usage of third-party vendors, even credible ones, can cause

software developed by Boeing, Maneuvering Characteristics Augmentation System (MCAS), was a key safety issue that was found because of the crashes. This software used data from Angle of Attack (AoA) sensors to determine if the nose of the aircraft is pitch too high. The flaws with this software controlling the Boeing 737 aircraft were that the software relies on only one sensor and that the software can override pilot input. Boeing also, allegedly, did not disclose the MCAS software to pilots and instead described it as a minor feature that pilots did not know how to disable. In 2021, the Department of Justice reached a settlement in this case and would not prosecute Boeing for fraud. But, before the deferred-prosecution agreement was set to expire, a door plug blew off a door of a 737 MAX aircraft during a flight over Oregon [11]. "That incident renewed concerns about manufacturing quality and safety at Boeing and put the company under intense scrutiny by regulators and lawmakers" [11]. Recently, a federal judge "rejected a deal that would have let Boeing plead guilty to a felony conspiracy charge and pay a fine for misleading U.S. regulators about the 737 Max jetliner before two of the planes crashed, killing 346 people" over DEI policy concerns. The judge noted that he is "not convinced ... the Government will not choose a monitor without race-based considerations" and argued that "in a case of this magnitude, it is in the utmost interest of justice that the public is confident this monitor selection is done based solely on competency" [11].

While accountability for the Boeing 737 MAX crashes has not been finalized in court, it is likely that Boeing may face fraud charges and be subject to a fine for the malpractice that was found. Additionally, Boeing's CEO did not face any criminal charges but was instead terminated from his position.

6 Conclusion

Throughout this paper, we discussed the various attack vectors that attackers may exploit when delivering their attack, examples of famous cyberattacks, and the complexity of cyberattacks. We also discussed the role of the attacker and the defender and the responsibility of leadership within the information security sector. We then discussed the pros and cons of holding the defender accountable for a

cyberattack. Next, we examined cyberattacks within third party vendors and accountability in that area, specifically looking at the CrowdStrike 2024 outage. Finally, we discussed how legal systems are handling technological malfunctions in the case of Tesla Autopilot and the Boeing 737 MAX crashes. In conclusion, it truly depends on the attack performed, but legal regulations around the defender are not likely to be taken by prosecutors. As regulations currently exist, prosecutors would have a difficult time determining fault against the defender because there is no precedence, and action would likely only take place against the organization rather than an individual. A defender cannot protect against the "unknown, unknowns," but still needs to provide reasonable security and assurance against an attacker.

About the Author - Kirin Chaplin



Kirin is a computer science and cyber operations double major. She is a junior from Lima company graduating early to work for the federal government. She is a CyberCorps: Scholarship for Service scholar.

References

[1] George Reynolds, *Ethics in Information Technology* (Sixth Edition), Cengage, 2019. ISBN: 978-1337405874
 [2] Statista. 2024. Annual number of cyberattacks in the United States from 2016 to 2022 (in millions). Statista. Retrieved February 1, 2024, from <https://www.statista.com/forecasts/1448523/us-cyberattacks-annual>.
 [3] Ryan Hammer. "Information Assurance & Computer Security" presented in CSCI327: Computer Security, The Citadel, Charleston, SC, USA, Fall 2023.
 [4] U.S. Securities and Exchange Commission (SEC). 2023. SEC Charges SolarWinds CISO with Failure to Report Cybersecurity Risks. Retrieved October 31, 2023, from <https://www.sec.gov/newsroom/press-releases/2023-227>.
 [5] Harvard Law School Forum on Corporate Governance. 2024. Court dismisses most of SEC's claims against SolarWinds. Retrieved August 3, 2024, from <https://corpgov.law.harvard.edu/2024/08/03/court-dismisses-most-of-secs-claims-against-solarwinds/>.
 [6] Bailey Schulz, Felecia Wellington Radel, and Josh Meyer. 2024. How one software update was chaotic. *USA Today*, July 22, 2024. Retrieved from Academic Search Complete.
 [7] Legal.io. 2024. CrowdStrike Faces Legal Battles After Major Outage. Retrieved July 29, 2024, from <https://www.legal.io/articles/5524395/CrowdStrike-Faces-Legal-Battles-After-Major-Outage>.
 [8] Amy Danise. 2024. Tesla Autopilot Lawsuits: Understanding the Legal Implications. *Forbes*. Retrieved November 2024, from <https://www.forbes.com/advisor/legal/accident/tesla-autopilot-lawsuit/>.
 [9] *New York Times*. 2023. Jury Finds Tesla Not Responsible for Fatal Autopilot Crash. Retrieved October 31, 2023, from <https://www.nytimes.com/2023/10/31/business/tesla-autopilot-jury-decision.html>.
 [10] Federal Aviation Administration (FAA). 2020. Summary of the Boeing 737 MAX Return to Service. U.S. Department of Transportation. Available at: https://www.faa.gov/sites/fga.gov/files/2022-08/737_RTS_Summary.pdf.
 [11] ABC News. 2024. U.S. judge rejects Boeing's plea deal in conspiracy case. *ABC News*. Retrieved June 13, 2024, from <https://abcnews.go.com/Business/wireStory/us-judge-rejects-boeings-plea-deal-conspiracy-case-116495188>.

NANOPARTICLES TO THE RESCUE: DEVELOPMENTS IN CANCER TREATMENT

JESSICA BAILEY

1. Introduction

Cancer is a deadly and complex disease in which abnormal and damaged cells multiply and create a tumor. Cancerous cells very easily travel to other parts of the body and can infect other areas of the body and form new tumors (1). Scientists and Doctors have been trying to find ways to help patients with cancer and have found ways to break down and mitigate the tumor. These treatments include surgery and chemotherapy, with chemotherapy being the more common (2).

Chemotherapy is a drug-dependent treatment used to stop the growth of the cancers cells by either killing them or stopping them from dividing. Though this treatment is preferred, the drug cannot distinguish between healthy and cancerous cells and can possibly cause significant harm to the body. This type of therapy is known to be very demanding on the patient's body and creates symptoms like fatigue, hair loss, loss of appetite, etc. (3)

Nanotechnology, or a scientific system conducted on a molecular level, is being looked at to make a drug delivery system to help the drug target the unhealthy cancer cells and/or protect the healthy cells. (4) A drug delivery system is a method or process in which therapeutic compounds can be transported to its target. Drug delivery systems can help chemotherapy pharmaceuticals target the tumor, lessen side effects and help with the efficiency on the tumor; making for a less painful experience for the patient. Different drug delivery systems can have different purposes depending on the target and the chemicals. Combining

these drug delivery systems together to make a multi-layered system can lead to "customizing the nanoparticle and its functionalities to a particular cancer or patient.

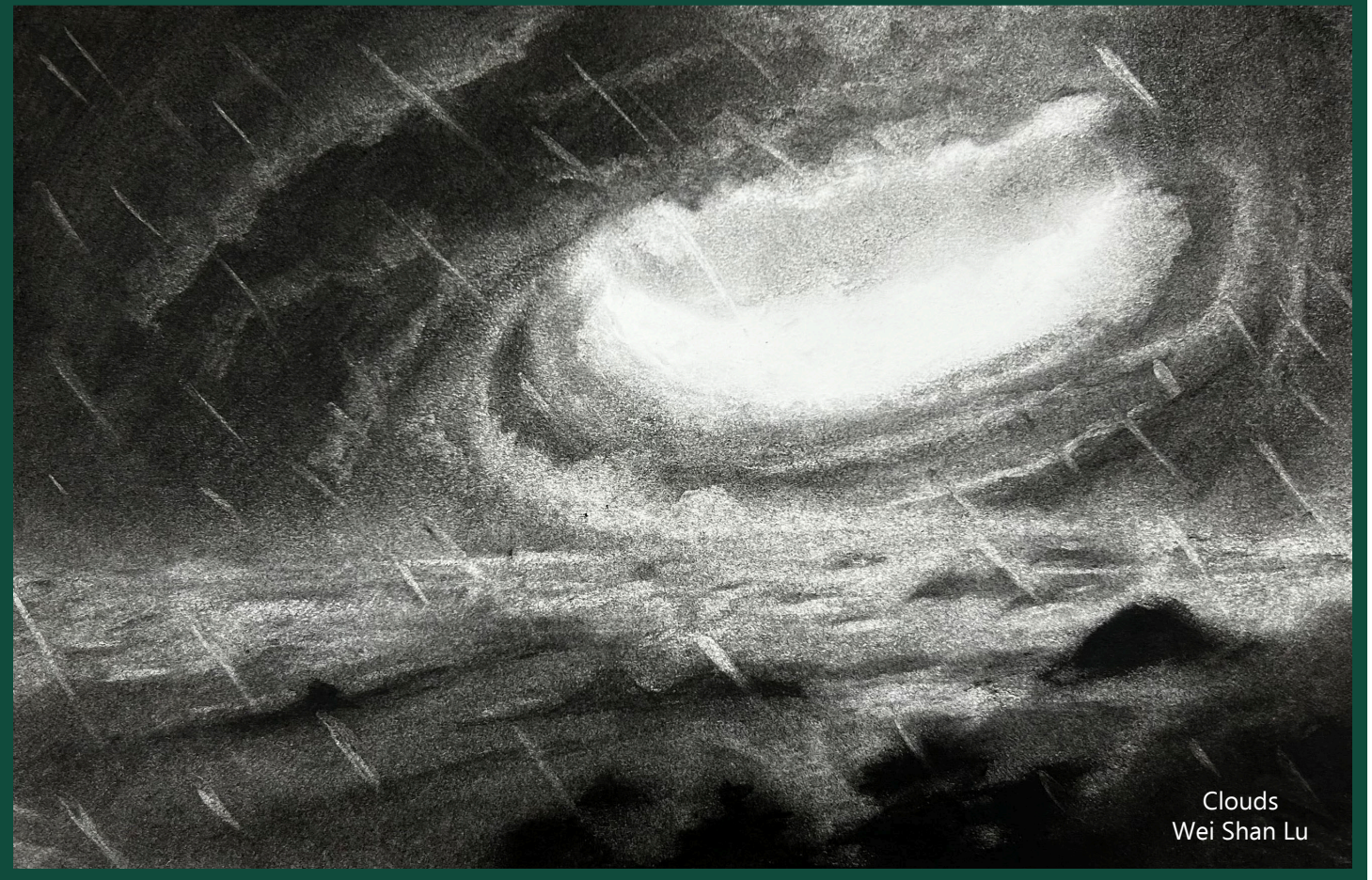
2. Advantages of multi-functional drug delivery systems

In general, there are many perks to having a drug delivery system, especially with more toxic drugs. Drug delivery systems can lessen toxic side effects, increase the drug loading efficiency, the time and target efficiency, and transporting hydrophilic drugs prolonging and targeting the release of the drug. Studies show that when a nanoparticle drug delivery system is integrated into the treatment of tumor bearing mice, results showed that the nanoparticle administration "enhances tolerability, safety, and efficacy" of the drug delivery (5). Each function has its unique sets of properties and advantages, but with a multi-functional drug delivery system there is a way to combine all the of effective ways to combat the main problems seen in nanoparticle drug delivery today; protecting chemotherapy drugs from attacking healthy cells and inefficient use of the drug (2,6).

3. Types of function/Purposes for DD systems and definitions

3.1. Targeting

The purpose of targeting in a drug delivery system is to guide the drug to the tumor site. This helps the nanoparticle transport the drug to only the cancerous cells, focusing less on the healthy cells. There are two parts to drug delivery targeting; guiding the drug through the body and to the tumor and determining when



Clouds
Wei Shan Lu

the nanoparticle should release the drug (at the tumor site). There are many methods to achieve this goal, including pH triggered release, magnets, and protein-coded nanoparticles.

3.1.1. pH Dependent Release

pH triggered release is a function in which the nanoparticle releases the drug once it is in a more acidic area. This function is significant because cancerous cells live in an acidic environment. Therefore a more acidic environment than the usual pH of blood (pH 7) can be an indicator to the nanoparticle that cancer cells are in the area. For example, PEGylated nanoparticles were made to carry paclitaxel to and release at a lower pH than 7. The nanoparticle dissolves, while the drug is released to the tumor site. This molecular mechanism is executed using the polymer polymethyl acrylate (PMA). PMA is a polymer that changes its shape with a change in pH. At pH 7, the polymer starts as a coiled shape, but when it is placed in an environment with a lower pH than 7, the shape of the polymer changes from a coiled shape to a linear shape (7).

This mechanism was proven when the particle size was measured at pH 7 and lower pH conditions. Therefore, as the pH decreases, particle size will increase.

Because of the mechanism's success, the nanoparticle does release faster in an acidic environment. The results also shows that pH 5 is the environment in which the nanoparticle is most for effective releasing (7).

3.2. Prolonging the release of the drug

Prolonging the release of the drug gives many benefits to a drug delivery system. Scientists achieve this function usually by encapsulating (or surrounding) the drug in a biodegradable and bio-compatible material (4). This encapsulation method is known as a micelle. Biodegradable (can be broken down in the body) and bio-compatible (material that does not affect the body in a negative way) are used for release studies because as the body identifies the nanoparticle a foreign objective, it will attack and degrade the particle. When the particle does break down, it does not have any negative effects on the body. A prolonged

Guardian of the Wilderness
Gianna Marlow



release helps the drug from interacting with the healthy cells, helping prevent the toxic side effects of chemotherapy drugs. It also helps with drug use efficiency, meaning that the drug will not be wasted on other parts of the body, but instead the nanoparticle will preserve most of the drug until it reaches its delivery site (tumor). Some materials that can be used for a prolonged drug release study include polymers, fibers, and cyclodextrin.

3.2.1. Cyclodextrin

Cyclodextrin is one of the many materials being used in the field of study. Cyclodextrin is a chain of glucopyranoside (a molecule derived) that is connected on either side, creating a tube-like structure. This structure creates a hydrophilic (“water-loving”) side on the outside of the tube and a hydrophobic (“water-fearing”) side on the inner part of the tube (8,9,10).

The property of this molecular structure is very beneficial for chemotherapy drugs that are hydrophobic, such as paclitaxel (10). The cyclodextrin structure acts as a buffer between the blood and the drug. The hydrophilic side (on the outside) will be compatible with blood while caging the drug in the hydrophobic side.

3.2.2. Poly (lactic-co-glycolic acid)

Another material used to encapsulate drugs is PLGA or Poly (lactic-co-glycolic acid). PLGA is an FDA-approved polymer that is bio-compatible and biodegradable. It is known to be an effective material for a NP and has been proven to withstand biological degradation in order to hold the cell. The structure of the polymer consists of lactic acid and glycolic acid. Lactic acid is naturally produced in the body and glycolic acid is found in the many plants we eat. This means the material is very compatible with our body and is a great material for encapsulating drugs (11,12).

3.3. External Assisted Therapies

External Assisted Therapies are the usage of outside instruments in conjunction with the nanoparticle and chemotherapy drug to attack the cancerous tumor site. As part of a multi-functional drug delivery system, external assistance can include something as simple as a tracking mechanism to see how far the nanoparticle travels, to helping disrupt the structure of the cancer cells for the drug to have a greater effect on the tumor (13,14).

3.3.1. Magnetite

Magnetic materials can be used as a form of therapeutic treatment with chemotherapy drugs. A multi-functional drug delivery system including a magnetic center, has other functions and doxorubicin surround the magnetic compound (14). An example of a magnetic compound is nanoparticle Fe₃O₄ also known as iron oxide. Iron oxide acts as a magnetite. Magnetite is biocompatible, biodegradable, and has many useful functions when coupled with an MRI (Magnetic Resonance Imaging) machine. One of the functions is using this NP as a therapeutic treatment in conjunction with an MRI machine to induce cell death through magnetic hyperthermia (14).

4. Conclusion

Understanding what type of functions individual parts of a drug delivery system and their benefits will provide the tools necessary to create a more personalized care plan to attack cancer. Cancer cells are mutated cells and therefore can evolve and adapt to the different methods of treatment used to treat cancer. Because of this, it is important that the treatment plan becomes more tailored to the patient's body and their cancer. Multi-functional drug delivery systems not only attack the tumor from multiple angles, but can also be customized to best combat the cancer in a way that is most beneficial for the patient. By utilizing the strengths of different drug delivery systems and combining them, we can customize the patients specific conditions and diagnosis. This personalized form of nanotechnology can create stronger and more effective treatment plans that reduce the suffering of cancer patients. This "personalized" treatment plan is the best way to protect patients and attack cancer, nanotechnology is the future of cancer treatment.

About the Author – Jessica Bailey



BAILEY

Jessica Bailey is a junior in November Company. She is a Biochemistry major and will commission into the Air Force after she graduates. This is her third year in the Gold Star Journal; she featured in the last two editions as a photographer.

References

- (8) National Cancer Institute. What is cancer? National Cancer Institute. <https://www.cancer.gov/about-cancer/understanding/what-is-cancer>.
- Ohunayo, A. S.; Elekofehinti, O. O.; Molehin, O. R.; Oyeyemi, A. O.; Ogunleye, T. M. Nanoparticles for Drug Delivery in Cancer Therapy. Elsevier eBooks 2024, 451–458. <https://doi.org/10.1016/b978-0-323-95114-2.00017-0>.
- Chemotherapy: Uses, Side Effects, and Procedure. Healthline. <https://www.healthline.com/health/chemotherapy#side-effects>.
- Nafiu Aminu; Salim Ilyasu; Mohammed Al-Kassim Hassan; Fatima Shuaibu Kurfi; Abubakar Ibrahim Jatau; Chan, S.-Y.; Deghinmotei Alfred-Ugbenbo. Applications of Nanofibers Drug Delivery System in Cancer Therapy. *Journal of Drug Delivery Science and Technology* 2023, 90, 105128–105128. <https://doi.org/10.1016/j.jddst.2023.105128>.
- Sritharan, S.; Sivalingam, N. A Comprehensive Review on Time-Tested Anticancer Drug Doxorubicin. *Life Sciences* 2021, 278, 119527. <https://doi.org/10.1016/j.lfs.2021.119527>.
- Does Nanomedicine Have a Delivery Problem? *C&EN Global Enterprise* 2016, 94 (25), 16–19. <https://doi.org/10.1021/cen-09425-scitech>.
- (6) Shen, M.; Huang, Y.; Han, L.; Qin, J.; Fang, X.; Wang, J.; Yang, V. C. Multifunctional Drug Delivery System for Targeting Tumor and Its Acidic Microenvironment. *Journal of Controlled Release* 2012, 161 (3), 884–892. <https://doi.org/10.1016/j.jconrel.2012.05.013>.
- Zhang, L.; Zhang, Q.; Wang, X.; Zhang, W.; Lin, C.; Chen, F.; Yang, X.; Pan, W. Drug-In-Cyclodextrin-In-Liposomes: A Novel Drug Delivery System for Flurbiprofen. *International Journal of Pharmaceutics* 2015, 492 (1–2), 40–45. <https://doi.org/10.1016/j.ijpharm.2015.07.011>.
- Zafar, N.; Fessi, H.; Elaissari, A. Cyclodextrin Containing Biodegradable Particles: From Preparation to Drug Delivery Applications. *International Journal of Pharmaceutics* 2014, 461 (1–2), 351–366. <https://doi.org/10.1016/j.ijpharm.2013.12.004>.
- (1) Wang, H.; Wang, K.; Tian, B.; Revia, R.; Mu, Q.; Jeon, M.; Chang, F.-C.; Zhang, M. Preloading of Hydrophobic Anticancer Drug into Multifunctional Nanocarrier for Multimodal Imaging, NIR-Responsive Drug Release, and Synergistic Therapy. *Small* 2016, 12 (46), 6388–6397. <https://doi.org/10.1002/smll.201602263>.
- Sadat Tabatabaei Mirakabad, F.; Nejati-Koshki, K.; Akbarzadeh, A.; Yamchi, M. R.; Milani, M.; Zarghami, N.; Zeighamian, V.; Rahimzadeh, A.; Alimohammadi, S.; Hanifepour, Y.; Joo, S. W. PLGA-Based Nanoparticles as Cancer Drug Delivery Systems. *Asian Pacific Journal of Cancer Prevention: APJCP* 2014, 15 (2), 517–535. <https://doi.org/10.7314/apjcp.2014.15.2.517>.
- (1) Lagreca, E.; Onesto, V.; Di Natale, C.; La Manna, S.; Netti, P. A.; Vecchione, R. Recent Advances in the Formulation of PLGA Microparticles for Controlled Drug Delivery. *Progress in Biomaterials* 2020, 9 (4), 153–174. <https://doi.org/10.1007/s40204-020-00139-y>.
- Revia, R. A.; Zhang, M. Magnetite Nanoparticles for Cancer Diagnosis, Treatment, and Treatment Monitoring: Recent Advances. *Materials Today* 2016, 19 (3), 157–168. <https://doi.org/10.1016/j.mattod.2015.08.022>.
- Da Hye Kim; Dong Wook Kim; June Young Jang; Lee, N.; Ko, Y.-J.; Sang Moon Lee; Hae Jin Kim; Kun Na; Seung Uk Son. Fe₃O₄@Void@Microporous Organic Polymer-Based Multifunctional Drug Delivery Systems: Targeting, Imaging, and Magneto-Thermal Behaviors. *ACS Applied Materials & Interfaces* 2020, 12 (33), 37628–37636. <https://doi.org/10.1021/acsami.0c12237>.

HIDDEN THREATS: THE ETHICS OF ZERO-DAYS

SEBASTIAN KLINCEWICZ

1 - Introduction

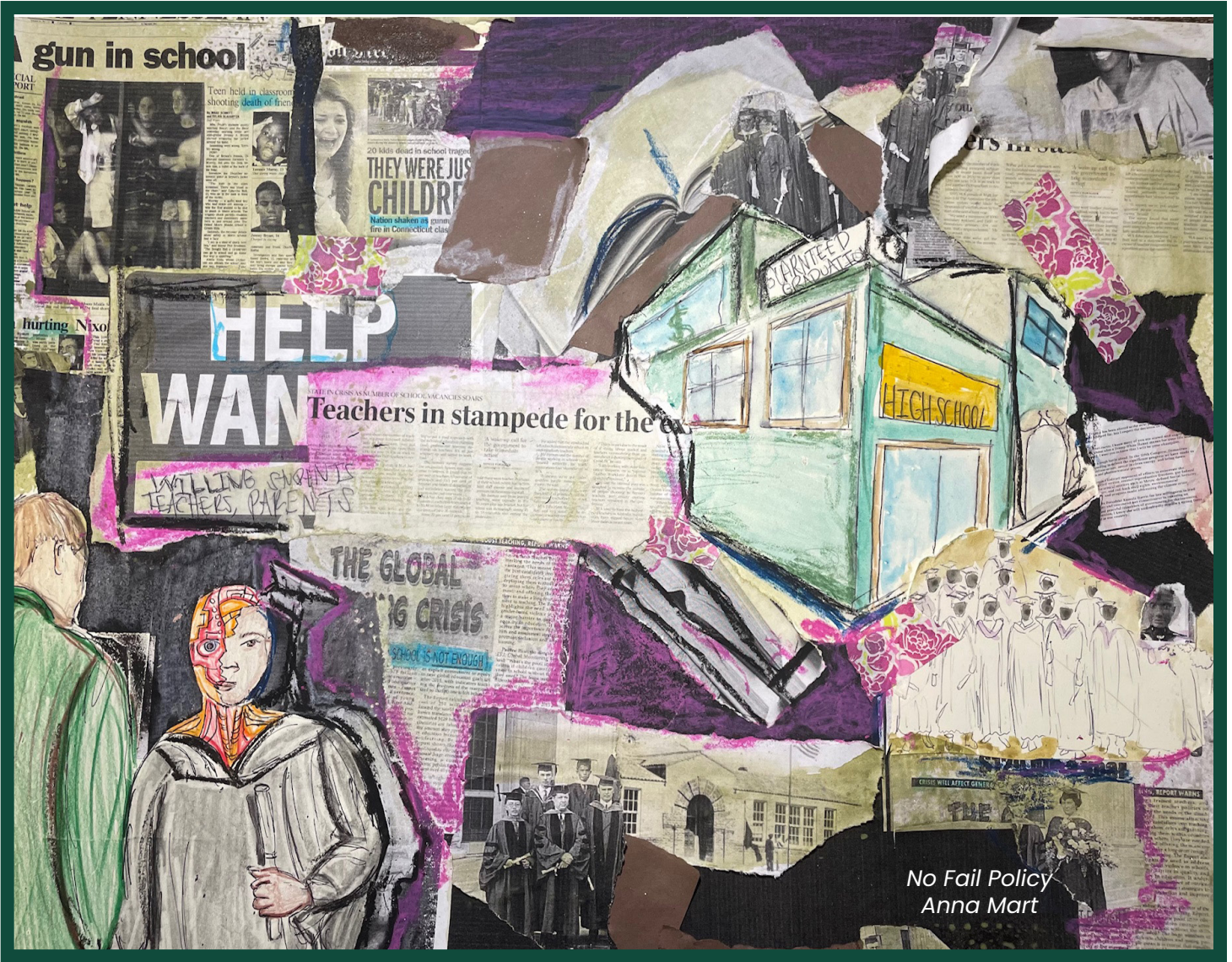
1.1- What is a Zero-Day Vulnerability?

Understanding the security risks associated with modern technologies requires familiarity with how software and hardware products are built and tested. When developers create digital products, they typically conduct extensive testing to identify errors, or “bugs,” in their code to ensure the product works properly. Despite these efforts, it is not uncommon for bugs to go unnoticed, leaving digital products vulnerable to exploitation. These bugs, ranging from simple errors to complex misconfigurations, are often overlooked but can be targeted by malicious actors. When outside parties discover these flaws, they become security vulnerabilities, weaknesses that allow attackers to manipulate a system in ways not intended by the original developers [1]. To reduce the risk of exploitation, vendors use security testers who search for these bugs and create “patches” fixes to protect the system. However, a specific type of undisclosed vulnerability is called a “zero-day.” The term applies to the number of days a vendor is made aware of a vulnerability to a specific product [1]. Because the vendor is unaware of the vulnerability, there is no immediate fix. Hackers discovering these zero-day vulnerabilities may exploit them before the vendor can release a patch, proving why zero-day vulnerabilities are so dangerous. These vulnerabilities become even more threatening when they are actively used in cyberattacks, as the lack of a patch leaves systems defenseless until a solution is found. In the context of information security, zero-day vulnerabilities present a significant

challenge, as they can be used to compromise systems without warning or defense.

1.2- Who uses Zero-day Vulnerabilities, and what is their Primary Purpose?

Today, a variety of entities around the world seek out zero-day vulnerabilities. Nation-states and government actors are among the most prominent parties working to find zero-day vulnerabilities in widely distributed software products. Other entities include cyber-criminal organizations bent on disrupting corporate operations or stealing sensitive data kept secure by vendors. Notably, the U.S. government utilizes intelligence services from the Central Intelligence Agency (CIA) and National Security Agency (NSA) to find zero-day vulnerabilities ready to be transformed into exploits. The exploits are used by these intelligence agencies as tools for collection and disruption operations sanctioned by national executive leadership [2]. Though the newfound zero-day vulnerabilities are withheld from the vendor to protect U.S. national security interests and assets, the lack of communication between the federal government and product vendors creates a clear security opening for adversaries to exploit the same zero-day vulnerabilities if found. Withholding details of zero-day vulnerabilities concurrently place digital assets and allies abroad at risk should an insider threat or leak occur, exposing the vulnerabilities. Once identified, exploitative tools abusing zero-day vulnerabilities make it easy for government entities and other third parties to compromise systems, as there is little to nothing targets can do to prevent the attack [2]. To best mitigate the attacks and compromise of U.S. digital assets, the U.S. government must privately



No Fail Policy
Anna Mart

release details concerning newfound zero-day vulnerabilities to vendors without global public disclosure to protect public trust with the American people and foreign allies, enhance domestic cyber defenses, and maintain cutting edge offensive capabilities against foreign adversaries.

2- Establishing Public Trust

2.1- The Vulnerabilities Equities Process (VEP)

The American public was not exposed to covert zero-day vulnerability acquisition until unprecedented leaks exposed intelligence agency operations. The cybercriminal organization known as the Shadow Brokers revealed several classified tools and techniques developed by the NSA. Of the leaked tools,

several were identified as known zero-day vulnerabilities used in global-scale cyber campaigns to disrupt systems through an OpenSSL vulnerability referred to as Heartbleed [3]. OpenSSL is an open-source cryptographic software toolkit used for secure communications and encryption implementation. Other zero-day vulnerabilities for widely used U.S. vendor-based digital products, including Windows Vista and Windows Server 2008, were discovered within the leaks, creating widespread concern about intelligence agencies' capabilities. Calming this concern, President Barack Obama announced revamping a futile process designed to establish transparency when identifying vulnerabilities in known U.S. systems, formally known as the Vulnerabilities Equities Program (VEP) [3].

Understanding the full extent of the VEP requires knowledge of its founding, dating back to the Comprehensive National Cybersecurity Initiative

instituted by President George Bush in 2008. The initiative then paved the way for formal policy designating the VEP as a formal reviewing party as outlined by the Office of the Director of National Intelligence (ODNI) in 2010.

This new formal policy created the framework process of formal notification, decision-making, and appeals by intelligence agencies [3]. The policy further opened the door for interagency collaboration, allowing other federal entities to make decisions concerning zero-day vulnerabilities through Equities Review Boards [3]. Though clearly defined by the ODNI, loopholes within the policy continued to allow the NSA their private internal review, bringing to question whether the government was genuinely stockpiling zero-day vulnerabilities, leaving users vulnerable to attack. Leadership within the intelligence community did not face severe backlash until the Heartbleed leak, leading to the discovery of the NSA's knowledge of vulnerability for two years. The Shadow Broker's leak made many wonder what the best method would be to revamp the reporting mechanism originally established by Bush. Ethics scholars continue to contemplate whether the VEP acts in the best interests of the American people, as the Equities Review Board (ERB) does not possess proper representation for the American public. Defining distinct parameters for the VEP is essential for balancing virtuous decision-making within the intelligence community (IC) and the U.S. government.

Revising the proper reporting of zero-day vulnerabilities requires a sharp vision of what a vulnerability equities process should entail. Sharon Bradford Franklin, the acting policy director of New America's Open Technology Institute, clearly expresses in her legal journal piece that a strong VEP program brings government hacking operations within the rule of law. The same tactics and techniques used by the government can be equally exploited by American adversaries if not adequately secured, leaving millions susceptible to attack [4]. Franklin shares reasons for the significance of developing and publicizing formal VEP procedures, all based on creating international norms for handling zero-day vulnerabilities. Unlike the current methodology, the U.S. government must realize the significance of evaluating security tradeoffs in handling zero-day vulnerabilities. From a diplomatic standpoint, maintaining public trust

eliminates reservation among the international community of how the U.S. applies innovative technology and what methods of business practices will be affected by covert operations.

Furthermore, a newly revamped VEP program allows the government to secure its systems better and assist allies and intelligence partners abroad who share sensitive data. Notably, the U.K. has established a similar process but notes that if an allied partner has already evaluated the vulnerability, there is no need for formal review [4]. Lastly, the level of transparency built with a revamped VEP process will encourage technology companies to continue developing new software without fear of exploitation by state-sponsored threat actors. Reestablishing a robust VEP in the U.S. requires adequate representation from government agencies, providing unbiased and fair consideration when over-viewing reported zero-day vulnerabilities before private release to a vendor. Perspectives from the Department of Commerce and the National Cybersecurity Communications and Integration Center, along with other federal agencies, can provide the necessary perspective focused on protecting all users' digital security and rights [4]. Cybersecurity goals outlined by agencies such as the Department of Commerce were only echoed after the RAND Corporation released its dissertation over-viewing the ethics of the VEP. Based on countless case studies, researcher Lindsey Polley carefully identifies several methods of ethical reasoning the VEP program would benefit from when reviewing zero-day vulnerabilities. Her determination for public release is summed in the following three questions: [5]

1. Is the ERB "rational" in its reasoning?
2. Does the ERB have the capacity to understand daily life functions?
3. Does the ERB have the will to act in ways that optimize social good?

Though these questions only outline a generic framework for retention or dissemination, they provide an ideal framework for the ERB to institutionalize moral ethics when passing zero-day vulnerabilities through the VEP process. Further ethical questions posed by researchers such as Polley and the RAND corporation are what is needed to revamp the VEP if the U.S. hopes to establish true transparency with the

American people and the international community.

2.2 – FBI vs. Apple

Though most zero-day vulnerabilities are found and used by U.S. intelligence agencies, law enforcement agencies play a similar role when handling their zero-day vulnerability findings. As the premier federal law enforcement agency, the FBI focuses heavily on bringing criminal entities to justice through robust investigative processes, including exploiting digital devices with proper legal authority. Despite these intentions, the FBI overstepped its legal authority during the 2015 San Bernardino terrorist shooting. After the takedown of the shooter, the FBI sought adequate answers for the terrorist plot and determined who the shooter was in communication with [6]. An effort to break into the suspect’s iPhone raised several privacy concerns, given Apple’s difficulty working with the FBI. Mark Levy’s overview of the case succinctly shows that after several failed attempts to access the suspect’s phone legally, the FBI “smashed that padlock, digitally trespassing and infringing on Apple’s copyrighted software” [6]. The actions in question further revealed the federal government paying 1.3 million dollars for third-party hackers to exploit flaws in Apple’s encryption software and side-step built-in security mechanisms. Identifying a new zero-day vulnerability in the process, the FBI vs. Apple case leaves many to wonder about the genuine effectiveness of the VEP program, especially if the federal government is unwilling to offer the vulnerabilities to a review board. Regardless of the purpose, the FBI circumvented copyrighted software, ultimately violating the Digital Millennium Copyright Act (DMCA) [6]. Proper review from a separate oversight committee or conducting a formal VEP process might have mitigated legal hurdles the federal government faced after breaking into the suspect’s iPhone, leaving the transparency with the American people further tarnished. When overseeing such cases related to the delicate balance of national security, it is critical to consider the

broader ethical implications of the actions taken. Individual rights and privacy must not be at the expense of upholding public justice. A transparent and accountable process is essential to foster trust between vendors, consumers, and government agencies, ensuring ethical guidelines are upheld and security measures do not undermine the fundamental values of the Constitution. Proper accountability throughout all facets of government must be implemented to effectively reap the benefits of the VEP program and ensure mutual trust between vendors, customers actively using their products, and the federal government.

KLINCEWICZ



La Paz Waterfalls
Chad Souders

access given the institution’s inability to defend against the attack. Post-2016, data breaches continued to skyrocket, calling for immediate strategic planning to secure national assets. Notably, a separate study detailed by Stephen Wicker highlights the detriment of publicly releasing zero- day vulnerabilities by noting that the “number of malware variants exploiting [systems] increased between 183 to 85,000 times, while the number of attacks increased between 2 and 100,000 times” [1]. His observations show that while data breaches continue to increase to unprecedented levels, zero-day vulnerabilities are a mass contributor to the number of attacks occurring to national assets. As expressed through the VEP program, a proper mitigation strategy includes using internally discovered zero-days to patch systems heavily used by national institutions. The federal government must equally prioritize offensive capabilities with defensive posture to adequately diminish the number of cybersecurity incidents occurring in the years to come.

3.2 – Effectiveness of Current Cyber Defense Practices

Modern cyber defense programs within the U.S. government today include outsourcing penetration tests and vulnerability assessments to third-party contractors. Outsourcing security is not often cost-effective, as some professionals say that conducting simple penetration tests do not provide a complete picture of the security in a specific network. Many federal agencies rely heavily on firewalls, advanced encryption, and other perimeter-based security mechanisms, making internal systems susceptible to advanced attacks [8]. There is little the federal government, and civilian companies can do regarding zero-day vulnerabilities without advanced security mechanisms established to identify and patch critical and newfound vulnerabilities. Over the last ten years, the U.S. Congressional Budget Office has reported a gradual increase in cybersecurity spending, with the exception of the 2021 fiscal year. Trends over this period indicate future budget increases as the White House advances its cyber defense initiatives. With rising monetary damages and the risk of losing vital intelligence, the surge in data breaches has made cyber defense a top priority for the U.S. government.

Notably, the White House recently released

an executive order on improving the nation’s cybersecurity practices within the federal government and private sector. Formally known as Executive Order 14028, The Executive Order on Improving the Nation’s Cybersecurity highlights the significance of removing barriers between federal entities and the private sector to ensure proper communication flow [9]. Information related to active threats and apparent risks must be shared with private sector companies to patch systems used by the federal government. Specifically, the level of information sharing sought after by the White House further requires detailed vulnerability scanning reports and the identification of newfound zero-day vulnerability. Federal and corporate cooperation with policies like Executive Order 14028 establish unified and up-to-date cyber defense practices that mitigate risks associated with advanced attack methods [9]. Furthermore, information sharing between entities can also help drive down budget increases by reducing spending on defense research. Just as private contractors take heavy initiative in identifying vulnerabilities within their products, the federal government can equally assist in this effort by contributing to national vulnerability databases and notifying vendors privately.

4 – Maintaining Offensive Capabilities

4.1 – Lifespan of Zero-Days

Though critics of zero-day vulnerability disclosure argue that reporting places the U.S. at a disadvantage, specific statistics have shown otherwise. The advent of leaked zero-days and increases in nationwide data breaches drove the RAND Corporation to conduct a unique study, analyzing the effectiveness of vulnerability retention and stockpiling. The dataset used in the study spans over 14 years and contains information about more than two hundred zero-day vulnerabilities that threat actors took advantage of [10]. Notably, over half of the zero-day vulnerabilities used within the study were publicly unknown. Of the findings within the report, RAND identifies the unlikely longevity of zero- day vulnerabilities with an average life expectancy of 6.9 years [10]. This life expectancy includes the time vendors need to develop

countless U.S. digital assets. Once reported, security patches can be administered to all significant federal and civilian assets that transmit sensitive data. Further cyber defense standards will be updated to maintain uniformity when handling security incidents and keeping assets up to date with the latest security patching. Proper uniformity requires adequate information sharing between federal agencies and civilian partners. Disclosure of zero-day vulnerabilities found by the federal government still allows intelligence agencies to engage in planned offensive operations within a designated timeframe, depending on the vulnerability of choice. The long life span of most vulnerabilities and low chances of outside adversaries finding the same vulnerabilities allow the federal government to report them as needed if prior vulnerabilities were found for a target system. The U.S. can uphold national security while remaining ethical in collecting and using zero-day vulnerabilities by properly disseminating them to vendors through official channels. Dissemination and increased information sharing between the federal government and U.S. vendors are the only ways to maintain ethical superiority while maintaining dominance over cyberspace.

About the Author – Sebastian Klincewicz



KLINCEWICZ

A senior from Miami, Florida, Sebastian Klincewicz is a double major in computer science and cyber operations with a minor in Intelligence and Security Studies. Upon graduation, he will be commissioning as an Ensign in the US Navy as a Naval Flight Officer (NFO).

References

- Wicker, S.B. (2020) 'The ethics of zero-day exploits---The NSA Meets the Trolley Car', *Communications of the ACM*, 64(1), pp. 97–103. doi:10.1145/3393670.
- Soghoian, C. (2023) *Feds refuse to release documents on 'Zero-Day' security exploits*. ACLU, American Civil Liberties Union. Available at: <https://www.aclu.org/news/national-security/feds-refuse-release-documents-zero-day-security> (Accessed: 28 November 2024).
- Healey, J. (2016) *The U.S. government and zero-day vulnerabilities: From Pre-Heartbleed to shadow brokers* | *columbia journal of international affairs*, *Journal of International Affairs*. Available at: <https://jia.sipa.columbia.edu/news/us-government-and-zero-day-vulnerabilities-pre-heartbleed-shadow-brokers> (Accessed: 28 November 2024).
- Franklin, S.B. (2019) 'The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes', *Fletcher Security Review*, 6(1), pp. 45–48.
- Polley, L et al. (2022) *To disclose, or not to disclose, that is the question a methods-based approach for examining & improving the US government's vulnerabilities equities process, To Disclose, or Not to Disclose, That Is the Question A Methods-Based Approach for Examining & Improving the US Government's Vulnerabilities Equities Process*. dissertation, RAND.
- Levy, M.S. (2017) 'Holding the FBI Accountable for Hacking the Apple's Software under the Takings Clause', *American University Law Review*, 66(5), pp. 1293–1314.
- Jones, M.E. (2007) 'Data Breaches: Recent Developments in the Public and Private Sectors', *I/S: A Journal of Law and Policy for the Information Society*, 3(3) pp. 555– 580.
- The White House. 2021. Executive Order 14028: Improving the Nation's Cybersecurity. *Federal Register*, Vol. 86, No. 93, 26633–26646. Available at: <https://www.federalregister.gov/d/2021-10460>.
- Ablon, L and Bogart, A. 2017. *Zero Days. Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corporation, Santa Monica, CA. Available at: https://www.rand.org/pubs/research_reports/RR1751.html.



Cabin Views
Chad Souders

A Note on the Journal

The Gold Star Journal is set in Poppins, a versatile typeface with clean, monolinear strokes perfect for publications seeking a sharp, modern style. Our title page features the powerful font, 210 Supersize. The cover is gold foil embossed on 100# Sundance Linen Emerald Green paper stock. The interior paper is 100# Gloss Text.

The Gold Star Journal is printed and bound by Sheriar Press in Myrtle Beach, South Carolina.

The Gold Star Journal showcases the work of Citadel students outside the classroom. Submissions are open year-round, with the deadline being the December prior to the year of publication. Work can be uploaded at:
<https://www.citadel.edu/goldstar/submissions/>