Dedicated in Honor of Sergeant 1st Class Christopher A. Celiz,'08

The 26th Edition of *The Gold Star Journal* is dedicated to Sergeant 1st Class Christopher Celiz. Sergeant 1st Class Celiz's actions will forever cement him among the United States and The Citadel's greatest heroes. He was awarded the Medal of Honor for his actions during Operation Freedom's Sentinel, where he served as a batallion mortar platoon sergeant with Company D, 1st Battalion, 75th Ranger Regiment, in Afghanistan. The Editors of *The Gold Star Journal* express our admiration to Sergeant 1st Class Celiz along with our gratitude to his family and friends.

A Letter from The Editors

To the members, family and friends of The Citadel community,

It is with great honor and distinction that we present to you the 26th Edition of *The Gold Star Journal*. *The Gold Star Journal* provides an outlet for the publication of cross-disciplinary nonfiction papers, photographs, and artwork from members of the Corps of Cadets and the Graduate Program. This edition of the journal highlights the challenging and forward learning of our peers. The Citadel's students are continuously developing their academia, leadership skills, and purpose while establishing themselves as experts in their field. The mission of this journal is to examine and to display their initiative to the readers.

Following the 25th Edition of *The Gold Star Journal*, we inducted an entirely new team of editors. This presented our Editorial Staff with the task of developing a specific and unique mission for the journal. It is owed all to the ambitious minds of our fellow editors as their consistency and dedication to our mission led to the production of this publication. They have worked tirelessly throughout the year, and it is clearly demonstrated in the following pages.

The journal features eight scholarly papers that represent distinctly different disciplines within The Citadel's academic environment from International Affairs to Computer Science. We highlight Charles Geiger who is being awarded The Boyd Family Distinction Award for his paper, Carbon Nanotube Types and Application. Harry Charles' paper, The Opioid Crisis and its Connection to Dentistry, is given the Best Undergraduate Paper Award. *The Gold Star Journal* highlights six photographers for their display of scholarship through the lense of a camera. We congratulate Eric Wilson Jr. with The Best Photograph Award for his photograph, The Flag Bearer, and Matthew Smith for The GSJ Distinction in Photography Award for his photograph, Lunar Winter.

The publication of *The Gold Star Journal* embodies much more than meets the eye. We extend gratitude to our faculty advisor, Dr. Suzanne Mabrouk, for her steadfast commitment to the success of *The Gold Star Journal*, our editorial team, members of this publication, and The Citadel community. We recognize a member of the Multimedia Services, Mr. John Whitten, as he has continuously supported the endeavors of this publication through mentorship and Indesign expertise. We also thank our donors, Dr. and Mrs. James F. Boyd, '71, LTC and Mrs. Albert G. Brauer II, '72, Dr. Suzanne T. Mabrouk and Mr. Stephen S. Jones, Mr. and Mrs. William G. Rasberry, '19, LT. Grant N. Miller, '18, and the Friends of the Daniel Library. Their contribution to *The Gold Star Journal* is essential to our publication, and it would not be possible without their generosity. Our appreciation extends to The Provost, Dr. Sally Selden, The Commandant of Cadets, Colonel Thomas J. Gordon, and other members of the Commandant's Department due to their guidance in documenting the success of the Corp of Cadets and the Graduate Program.

The Commandant of the Corps of Cadets, Colonel Thomas J. Gordon, has repetitively stated his leadership philosophy as, "Do right, and fear no man." Members of The Citadel community have used these words as a documentation of integrity and purpose in their continuous development of leadership. However, these words are true to academia as well. As young members of our nation, it is imperative that we grasp onto every opportunity to educate ourselves and to expand our minds. The power of knowledge is undeniable, and it provides each member of our campus with the ability to fulfill their purpose. The students published in this journal are a testament to this statement.

The Gold Star Journal is a staple to the academic community of The Citadel, and it has continued to do so for twenty-six years. By uplifting and promoting the multidisciplinary work of our peers, our Editorial Staff hopes to continue this tradition. Thank you to all who devote their time to reading and supporting the 26th Edition and those elite students included in it. We hope you are able to expand your knowledge and power as those within the journal have demonstrated.

Very respectfully,
The Editors of *The Gold Star Journal*

Editorial Staff

Elissa Reckdenwald, Editor-in-Chief

Elissa, a third-class student from Hotel company, comes from Andrews, South Carolina. She is a Second Battalion legacy as her father graduated from Hotel, Class of '93. Elissa is an Intelligence and Securities and Spanish double major with a double minor in Cyber Interdisciplinary Studies and Leadership Studies. She has excelled in the classroom, receiving Gold Stars every semester, President's List and Dean's List. Academically, Elissa is a member of The Citadel Distinguished Scholars Program, The Citadel Leadership Scholars Program, and The Yawkey Scholars Program. She was recently inducted into the Honor Society of Phi Kappa Phi, known for being the nation's oldest and most selective multidisciplinary collegiate honor society, and Sigma Delta Pi, the Hispanic Honor Society. Over the summer, Elissa was an intern at the Georgetown County Sheriff's Office, and during the fall semester, Elissa was a congressional intern for Congresswoman Nancy Mace's Charleston office. In her free time, Elissa enjoys going to the beach, listening to music, and watching investigational-related media. Following graduation, Elissa hopes to be accepted into a prestigious post-graduate program, where she will study Foreign Relations and International Affairs.

Kenneth Galsgaard, Assistant Editor-in-Chief

Kenneth, a junior within Sierra company, is from Los Altos, California. Kenneth is a Political Science major and English minor with a focus on Pre-Law. He has excelled in the classroom, receiving Gold Stars or Dean's List honors every semester, as well as President's List and Commandant's List his sophomore year. Kenneth is a member of The Citadel's chapter of the Political Science Honor Society. Over this past summer, Kenneth interned at a prestigious law firm in the Silicon Valley. Upon graduation, Kenneth hopes to attend a top-tier law school in Southern California and pursue a career in privacy law. Outside of The Citadel, Kenneth enjoys working part-time as a lifeguard, being around friends, and participating in multiple clubs at The Citadel.

Trey Stevens, Communications Editor

Trey is a senior from Charlie company. He hails from Blythewood, SC. He is currently pursuing four degrees, a B.S in both Computer Science and Cyber Operations and a B.A in both Intelligence and Security Studies and Criminal Justice along with a double minor in Cybersecurity and Fine Arts. Trey has obtained Gold Stars and Dean's List throughout his cadet career while performing multiple extra and co-curricular activities. Trey was just recently selected to serve as Charlie company's Honor Representative and Charlie company's Company Community Engagement Council Representative. Trey currently holds the position of Treasurer and Secretary of The Citadel's Omicron Delta Kappa Leadership Society Chapter. He has served as a cyber mentor to a high school and middle school during his time as a cadet and is the most senior member of the Citadel's Cyber Unit. As a Department of Defense scholar, Trey will serve in the federal space after graduation. He plans on obtaining a master's degree and eventually his Ph.D. Trey will continue to give back to those who have helped him along the way.

Jesse Quimby, Logistics Editor

Jesse is a junior from Band company. He is from York, South Carolina, where he graduated from York Preparatory Academy. Jesse is a dual major in Physics and Mathematics with a minor in Fine Arts. Jesse is a legacy, because his brother, James Quimby, was an editor for the 2018 and 2019 editions. He recently served as Band company's Academic NCO. Jesse is the Vice President of both the Math Club and the Society of Physics Students. He is currently employed by The Citadel Chapel and as a physics tutor for the Student Success Center. This past summer, Jesse was an intern for NASA at Clemson University, where he worked to develop carbon nanoparticles. Jesse feels a calling to pursue a Masters in Divinity in seminary after completing his undergraduate degree.

Editorial Staff

John Morris, Marketing Editor

John Morris comes from Myrtle Beach, South Carolina. He is a junior at The Citadel studying Political Science on a Pre-law track with a minor in Philosophy. He is a part of The Citadel Honors Program and The Citadel Distinguished Scholars Program where he learns through research, tutorials, and service-oriented projects. While serving as the Marketing Editor in a remote capacity during the fall, John was in Washington, D.C. working for the Senate Budget Committee. In addition to his academic and professional pursuits, he is also passionate about nonprofit work and has served as the lead grant writer for an Australian NGO helping refugees and asylum-seekers since January of 2021. John is passionate about pursuing knowledge and experience, and is always looking to deliberate. John hopes to get a law degree to practice international law to help reform immigration practices across the globe.

Dylan Young, Scribe Editor

Dylan, a sophomore, is in Sierra company. He hails from North Myrtle Beach, SC. He is currently pursuing a degree in Intelligence and Security Studies and plans to minor in Psychology. Dylan has obtained Dean's List and Gold Star status throughout his cadet career while engaged in various organizations on campus. He is an athlete on the Citadel Rifle Team. He has been selected to serve as the Vice Chairman on the Company Community Engagement Council and is a member of the Student Diversity Council along with the Student Life Council. He is the founder and the President of the Citadel Intelligence Club and is the President of the National Coalition Building Institute chapter on campus. He currently holds the position of Secretary for the Judo Club. Dylan has served as a Summer SUCCEED fellow and AmeriCorps Vista for the Krause Center for Leadership and Ethics. He is passionate about leadership and in his free time, Dylan is heavily engaged with his dutys as a Squad Corporal. He also participates in community service to give back to the local area and sharpen his servant leadership skills. Upon graduation, Dylab plans on commissioning as an Intelligence Officer in the United States Army and attending night school to obtain his master and doctoral degrees.

Hampton Dennis, Editor

Hampton is a junior with an English major and a minor in Biology. He is currently in Echo company. He comes from McClellanville, South Carolina. Hampton is a legacy from 1952 graduate, William Robert Spillers. He is a member of the Citadel Episcopalian group and the Huguenot Church. He is a local to the Charleston area, living here all his life. Hampton enjoys hunting and shad fishing every spring in Moncks Corner, as long as the fish are swimming. He also enjoys music, collecting CDs and records to create a sizable collection. His aspirations range from working for SCDNR to teaching English, but his future is always in the making.

Dr. Suzanne Mabrouk, Advisor and Founder

Dr. Mabrouk earned her A.B. from Wheaton College (Norton, MA) and her Ph.D. from the University of Massachusetts (Amherst, MA). She has been a faculty member at The Citadel since fall 1993. She enjoys teaching organic chemistry, introductory chemistry for non-science students, and the chemistry of art. She cherishes her time in the classroom and lab, watching students master chemical concepts and laboratory techniques, respectively. She also treasures working with the Editors of *The Gold Star Journal* as they craft a new edition. She gained experience working on school publications as a high school student. For four years, she wrote articles for the school newspaper. Senior year in high school, she was Editor-in-Chief of the literary magazine, Copy Editor of the yearbook, and News Editor of the newspaper. She has published several scientific articles in the chemical literature, since an undergraduate. In February 2022, she published a paper in the *Journal of Chemical Education* on the chemistry of art course that she teaches in the Master in Education Interdisciplinary STEM Education online program.

Disclaimer:The views and opinions expressed in this publication are solely those of the authors. They do not necessarily reflect those of The Citadel and the Editors.

The History of *The Gold Star Journal*

The Gold Star Journal has distinguished itself as the most prestigous student publication at The Citadel since its inception in 1996. The tradition has continued for twenty-six years as members of the Corps of Cadets and The Citadel Graduate College have, from various disciplines, published high quality, stimulating, and intellectually challenging scholarly papers, unique photographs, and creative artwork. As the 26th Edition has been designed by the current Editors and reaches the hands of The Citadel community, it is important to recognize the time-honored traditions and continuous development of the publication.

In May of 1996, Dr. Suzanne Mabrouk was enrolled in a gradute course focused on responding to student writing at The Citadel. She was astonished that most students' papers do not live past a simple letter grade. To develop an opportunity for students to recieve additional recognition for their academic achievement, Dr. Mabrouk discussed the idea of *The Gold Star Journal* with the Vice President for Academic Affairs, Major General Roger C. Poole, '59. Following the meeting, *The Gold Star Journal* was given a budget and permission to begin production in July of 1996.

The 1st Edition was published for Corps Day 1997 with an original hand drawn cover and three sophomores as the founding editors. They continued to serve as editors the following year. From its founding until 2008, the journal was published on campus by the staff of The Citadel Print Shop. Members of The Citadel community had a distinct role in developing the publication such as campus photographer, Mr. Russ Pace, whose photography was featured each year on the covers of the 1998 to 2004 editions. Since 2005, only photographs taken by Citadel students have been included. The developement of *The Gold Star Journal* has continully evolved as the Editorial Staff has striven to produce the highest quality publication.

In 2005, the Editorial Staff established a new tradition of featuring the stars and bars, the name of the journal, the year, and The Citadel seal on the cover. To celebrate the 10th anniversary of *The Gold Star Journal* in 2006, it was printed for the first time completely in color. Since the 20th Edition, the publication has continued to be printed completely in color. In 2008, previous member of The Citadel's Multimedia Services, Mr. Kevin Metzger, Dr. Mabrouk, and the Editorial Staff designed a seal for the publication. The original seal has been re-designed twice, in 2015 and now for 2022. The seal includes one star for each year that the journal existed prior to its design. This seal serves as a symbol of academic excellence at The Citadel, distinguishing all GSJ-associated students with a unique scholarly badge of honor.

Since the creation of *The Gold Star Journal*, the Editorial Staff and Dr. Mabrouk have continued to enhance the publication through the seal, student awards, and the annual Gold Star Journal Academic Conference. The conference started in 2016 to commemorate the twentieth anniversary of the journal. It has continued as an additional venue for authors to share their scholarship through the spoken word before a live audience. Current awards include, The Boyd Family Distinction Award, previously The Best Overall Submission, first given in 2011, The Best Undergraduate Submission, since 2014, The Best Graduate Submission, since 2019, The Best Photograph, since 2012, The GSJ Distinction in Photography, since 2019, and The Best Oral Presentation, since 2017. *The Gold Star Journal* has been honored several times, in 2005 by Case District III with a Special Merit Award for the the 2004, 2003, and 2002 editions and in 2021 for the 2020 edition with the Athens Paper Award for Most Creative Use of Paper and the Special Judges Award for Soft Cover Booklet by the Printing Industry of the Carolina Awards.

Twenty six-years ago, Dr. Mabrouk and three editors began a journey to highlight the academic achievements of the Corps of Cadets and The Citadel Graduate College that became known as *The Gold Star Journal*. The publication continues to recognize the importance of effective writing, research skills, critical thinking, creativity, and ingenuity. The honor and legacy of *The Gold Star Journal* will continue for years to come!

Table of Contents

China's Shadow War

Alexander Clark

Alexander Clark is a senior from Little Rock, AR. He is currently serving as the Regimental Executive Officer. Alex is double majoring in Accounting and Intelligence and Securities Studies. After graduation, Alex plans to attend graduate school for an MS in Data Analytics while pursuing a commission in the United States Navy Reserve as an Intelligence Officer.

Abstract

Over the past several decades, it is undeniable that China has greatly increased their influence in the West. For the United States, this has meant a large influx of cheap Chinese goods. As a nation, the United States has allowed the Chinese government to take advantage of generous trade incentives in hopes that further privatization of Chinese industry would foster better cooperation globally. However, without cooperation on the part of the Chinese can this exchange be considered anything other than a shrewd strategy to hide economic and military buildup?

Chinese Influence in the United States

In 1999, the United States intelligence community began to understand the gravity of China's socioeconomic actions since the fall of the Soviet Union. The primary cause for this was the release of a document drafted by two senior officers of the People's Liberation Army (PLA). This document, titled *Unrestricted Warfare*, would serve as the mold for China to overtake the United States as the most powerful nation in the world. This strategy was an extremely complex and combined military strategy with United States' politics, social theory, and economics to achieve their complex national goals.

Unfortunately, not much action was taken by the United States as a result of this chilling document. This is in large part due to just how intangible the Chinese strategy was. The Chinese people know that the best outcome for them is to win this war without firing a single shot. They even go so far as to say:

> The new principles of war are no longer "using armed forces to compel the enemy to submit to one's will" but rather are "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests" (Messel 200).

This further confirms their strategy to overtake the United States using silent ideals such as political and economic control. Finally, there is the fact that many of these strategies not only help them overtake the United States, but they also help to increase the already extremely concerning stranglehold that China has on the Asia-Pacific region.

The Chinese Communist Party (CCP) has been working tirelessly for years to destroy the American democratic lifestyle, and the truth is that only the nature of their strategy has changed. From Washington to Wall Street, it is our complacency and reliance on globalism that has allowed China to utilize this underground strategy. BGen Spalding, a former Defense Attaché to China and Senior Director for Strategic Planning for the US National Security Council, furthers this point when he wrote that "we have about three years to stop the CCP's unrestricted war" (Spalding & Kaufman 2019).

China finally seems to have perfected this Unrestricted Warfare strategy as large monetary interests allow them to influence foreign politicians, silence dissenting ideas both at home and abroad, and even purchase and develop cutting edge technology. This provides insight into President Xi Xinping's cooperative statement at World Economic Forum in 2017 where he said, "We must remain committed to developing global free trade and investment, promote trade and investment liberalization and facilitation through opening-up, and saying no to protectionism."

Perhaps the most concerning aspect of this strategy is just how many of our politicians on both sides of the aisle are unknowingly controlled by Chinese influenced lobbyists. One of the most recent examples of Chinese conflicts of interest in United States' politics involves former Senate Majority Leader Mitch McConnell and his wife Elaine Chao. James Chao, her father, served as General Secretary of the CCP from 1989 to 2002 and to this day has strong business ties with China. While it is hard to prove that she took any treasonous action while acting as the Labor Secretary under President George W. Bush, it is crucial to acknowledge the conflict of interest. We must also realize that during this critical time in America, millions of jobs began leaving the United States in search of cheaper labor in places like China. Even if one can overlook these facts, it is still concerning how much the one couple's ties to China can affect the global market (Spalding et al. 2019).

Globalism

In 1978, the Chinese government began opening up their previously state-controlled communist system to the idea of free-market enterprises within limited portions of the private sector. This "small" private sector makes up what is now ~70% of the countries total GDP (Preen 2019).

China has been extremely careful in implementing this limited free market; however, through the use of their Special Economic Zones (SEZ), they have been able to gradually test out new reforms. This has led to the creation of massive manufacturing cities, such as Shenzhen, which are at the forefront of worldwide technological development.

These massive manufacturing meccas coupled with the cheap cost of labor has allowed China to take over many of the manufacturing jobs that previously existed in the United States. Its modern evidence is proven in an episode of *The Office* when Micheal Scott says, "They used to make stuff in America, Andy. But we're falling behind, did you know that? China is a sleeping dragon that is just beginning to stir." This defines the issue with China's market dominance, offset by the 2008 financial crisis showing the United States at its weakest in decades. Today, we find ourselves in recession once again due to the COVID-19 pandemic, and it continues to highlight our relationship with China ("The Office: China" 2010).

Another aspect of the cheap labor strategy is that it is not only occurring within the confines of China's border. Many Chinese companies, especially in the construction industry, have begun shipping their workers abroad to work on other nations infrastructure projects. It has led to some rather strange alliances being formed. Perhaps the most alarming of these alliances being with Egypt. Recently, Egypt has been looking to construct a new capital city in order to keep pace with many of the heavily modernizing nations around them. It has provided a perfect opportunity for Chinese state-owned construction firms to grab these contracts as the lowest bidder. The problem, however, is that the CCP is utilizing these new relationships to change the face of global trade and diplomacy. A large part of the reason that they have offered this cheap labor to Egypt is due to their massive influence by way of the Suez Canal. China sees the Suez Canal as one of their country's main strategic weaknesses and is doing everything they can to build relationships that will guarantee them long-term access (NYT 2018).

In light of the COVID-19 pandemic, many countries have begun to re-evaluate their relationship with the People's Republic of China. This has meant both good and bad for the countries moving for international leadership, but the CCP is fighting its hardest to come out of this crisis on top. It has primarily occurred in the form of humanitarian outreach, such as medical aid to be distributed primarily through the Chinese embassies of African nations.

One of the main circumstances to come out of the pandemic that has fueled this fire is the United States government's sluggish and unexperienced response. They have achieved this through several means but primarily through their threefold strategy which involves medical aid, vaccine distribution, and debt relief to smaller African states. The CCP has realized that if they are to ever garner respect on the international stage, they first need to acknowledge their failures, which is what they have attempted here. Zhao Lijian is quoted as saying, "China's signature strength, efficiency and speed in this fight has been widely acclaimed, we hope to create a new standard for the global efforts against the epidemic." It ultimately describes how the pandemic has been fit into their strategy of globalism. Beijing's dominance through production is enhanced by the fact that much of what the world depends on to fight the COVID is made in China (Campbell & Doshi 2021).

Boat in a Bottle by Kaytlynne McCord

Long Term Repercussions of Chinese "Globalism"

As we have seen throughout the course of the Coronavirus pandemic, it is clear the CCP is succeeding in their campaign to become a global leader. One of the easiest places to see this is in their aid to Italy in the earliest days of the pandemic. Even when the whole of Europe couldn't provide Italy with the masks, medical supplies, and ventilators that they desperately needed, China was there to take advantage of the situation. Their intervention helped to spread the idea that "European solidarity" was dead and that the only nation they could depend on was China (Campbell & Doshi 2021).

Now that we have seen real world examples of just how advantageous China's dominance in production can be, it doesn't leave much to the imagination when it comes to what more outsourcing could do. Not only does it provide them with long-term control over worldwide goods, but it also affords them the ability to reallocate production for wartime means.

Regional Security

China remains the biggest threat to peace in the Asia-Pacific region. The continued deterioration of United States-China relations that occurred during the Trump administration has been sustained in the early days of the Biden administration and shows no signs of changing anytime soon. One of the biggest flashpoints between United States-China relations has to be the nation of Taiwan. Furthermore, the United States continues to bolster the Taipei government. It is not guaranteed to explode into a military conflict in the region; however, we cannot rule out that possibility just yet (IISS 2020).

There is also the threat of the newly bolstered Sino-Russian relations as the two nations find themselves allied once again. These relations are primarily threatening to various ethnic groups in the region such as the Uyghur Muslims, who are currently being persecuted by the Chinese government. This is the primary reason that many of these central Asian nations, such as Kazakhstan and Kyrgyzstan, have turned a blind eye to the atrocities that the CCP is committing against their Uyghur Muslim populations (Pannier 2020).

Lastly, and perhaps the most applicable worldwide, is the threat that China may attempt to restrict trade within the South China Sea. The potential trade restriction is one of the most discussed scenarios within the region, and rightfully so. China

has continued for years to make illegitimate claims within the Sea (i.e. Nine-Dash Line) and with their current island-building activities, it can only seem that they are priming themselves for a pseudo-naval conflict. It is alarming for many of the nations of South and Southeast Asia as a majority of their goods, both import and export, will at some point travel through the South China Sea. This showcases the potential for far-reaching impacts across the globe (Council on Foreign Relations 2021).

Implications for US Security Interests

The primary threat to the mainland United States comes from the possibility of a Naval blockade in the South China Sea or even small-scale police action on the part of the PLA to defend their claims. It could potentially result in massive shipping delays and have a huge economic impact on the US, as a large amount of the foreign good that we rely on come directly from China. As we saw during the Coronavirus epidemic, many of these goods are things like disposable medical supplies and other essential consumables.

The repercussions of going to war, or even sanctioning trade with, China would be far-reaching and difficult to predict. However, it is clear that the United States' economy would take a large hit as the American consumer was forced to look elsewhere, and pay more out of pocket, for essential goods. The likelihood of this, while very small based on the current climate in the region, is still very concerning especially as the United States begins to take a firmer and more definite stand on the actions of the CCP.

Conclusion

It is clear that from the actions of the Chinese Communist Party and President Xi Xinping that the Chinese government is attempting to appear friendly to the idea of globalization. However, it appears to be only a surface level attempt as we can tell from various Chinese government and PLA documents that have been leaked. These documents, like *Unrestricted Warfare*, outline a bait and switch plan for China. They pretend to be open to the idea of globalism just enough to become critical to the world economy, and then, they throw the trap and exercise their position as a global leader to achieve their long-term goals.

With China's actions over the last decade, it is abundantly clear that they have not abandoned these strategies. The United States and the International Community as a whole have ignored China's strategic posturing for years. From local border disputes to the Nine-Dash Line in the South China Sea, there is an overabundance of territory that is physically contested by China. This goes without mentioning the many ways in which China attempts to dominate through subversive means such as economy and trade.

It is critical, now more than ever, that the United States and the International Community take a hard stance on China. It is very likely that if we fail to act here that China will dominate the world as the number one superpower by the end of the decade. This, for a variety of reasons, could prove to be detrimental to United States' interests throughout the world.

Works Cited

Campbell, Kurt M., and Rush Doshi. "The Coronavirus Could Reshape Global Order." Foreign Affairs, 17 Feb. 2021, www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order.

Council on Foreign Relations. (n.d.). Timeline: China's Maritime Disputes. Retrieved December 1, 2020, from https://www.cfr.org/timeline/chinas-maritime-disputes.

"Deterioration in US–China Relations 'Deepened and Accelerated' during Trump's Presidency." IISS, International Institute for Strategic Studies, www.iiss.org/press/2020/asia-pacific-regional-security-assessment-2020.

Messel, John A. Van. "Unrestricted Warfare: A Chinese Doctrine for Future Warfare?" Defense Technical Information Center, 2005, doi:10.21236/ada509132.

"Money and Muscle Pave China's Way to Global Power." The New York Times, The New York Times, 25 Nov. 2018, www.nytimes.com/interactive/2018/11/25/world/asia/china-world-power.html.

Pannier, Bruce. "Why Are Central Asian Countries Silent About China's Uyghurs?" RadioFreeEurope/RadioLiberty, Why Are Central Asian Countries Silent About China's Uyghurs?, 23 Sept. 2020, www.rferl.org/a/why-are-central-asian-countries-silent-about-china-s-uyghurs-/30852452.html.

Preen, Mark. "China's Reforms and Opening-Up: Future Prospects." China Briefing News, 3 Apr. 2019, www.china-briefing.com/news/economic-reform-china-opening-up-future-prospects/.

Spalding, Robert Stanley, and Seth Kaufman. Stealth War: How China Took Over While Americas Elite Slept? Portfolio/Penguin, 2019.

Sullivan, Halsted, and Paul Liberstein. "China." The Office, season 7, episode 10, NBC, 2 Dec. 2010.

Properties of a Sequence Derived from Another Sequence

Richardo Henriquez

Richardo Henriquez is a senior from Harpers Ferry, West Virginia. In addition to being a first generation American, he also is the first in his family to attend college. Richardo is an Honors Program Mathematics major with a Leadership Studies minor. Upon graduation, he will commission into the United States Army as an Infantry Lieutenant. In his free time, he likes to visit Civil War battlefields with his younger brother, Michael.

Abstract

In this research, we explore the properties of a function that gives (for each input) the number of terms in a sequence greater than the input itself. We will analyze the least number of times the function is applied to a particular input until the output is constant. In particular, we explore this function for sequences of powers. This problem was proposed by Dr. Florentin Smarandache in his paper entitled "Thirty- Six Unsolved Problems in Number Theory."

1. Introduction

The problem is Number 19 from Dr. Florentin Smarandache's "Thirty-six unsolved problems in number theory" [1]. We will be using a step-by-step process to find a solution to find the smallest number for each k in a series of varying sequences. We will explain the problem, form a conjecture as an answer, and finally prove that conjecture for a particular series and attempt to apply it to others.

2. Problem

Let a_1, a_2, . . . be a strictly increasing sequence of positive integers, and $N(n)$ be the number of terms of the sequence not greater than n.

(1) Find the smallest k such that $N(N(\ldots N(n)\ldots))$ is constant, for a given n, k times"[1]. The k times is to apply to the number of iterations of $N(n)$. $N^k(n)$ is constant means that the result of $N(n)$ is 1, as once it is one, it will continue to be 1 for any greater numbers.

(2) If a_i is not 0, 1, find the smallest k such that $a_{a_{a_{\cdot^{\cdot^{a_1}}}}} \geq n$, for given n"[1] where k is the number of times that a appears.

"Particular Case: When $\{a_i\}$ is the sequence of m-th powers, for a given m: 1, 2^m, 3^m..."[1]. There are other cases given in the question but only this will be analyzed.

3. Experimentation

The question wants to solve for an equation in order to find the smallest integer for each k. This can be obtained by manually finding each interval and finding a pattern among them. The equation itself, $N(x)$ calls for a repeat function until the result becomes constant. In the sequence of squares, it will not become constant until it reaches 1. This could mean using the function repeatedly, such as $N(N(\ldots N(x)))$. For example, for the sequence of squares, the $N(x)$ function will continue to take the square root of a number until it reaches 1 and is constant. It is constant because the root of power n of any n will always be equal to 1 as n approaches ∞. Thus, the function becomes constant.

First, we will try to manually find each smallest number for each k, then find patterns in the sequence if possible. The sequence of squares will be used for

this. We have derived the following equation in order to find the other k's for sequences of squares and sequences of cubes as well. In these equations, k is the degree and s_k is the smallest number for the k.

Definition 1. *s_k is the smallest value for the number of k iterations. For example, for k=3 iterations for the sequence of squares, s_k is 4, as 4 is the smallest possible number for k=3 iterations in the sequence of squares.*

K(Iterations)	Range(Smallest and largest values)	Range Pattern
1	{1, 3}	$\{0,2^{2^1}\text{-}1\}$
2	{4, 15}	$\{2^{2^1},2^{2^2}\text{-}1\}$
3	{16, 255}	$\{2^{2^2},2^{2^3}\text{-}1\}$
4	{256, 4095}	$\{2^{2^3},2^{2^4}\text{-}1\}$
5	{4096, 65535}	$\{2^{2^4},2^{2^5}\text{-}1\}$

We will attempt to find an equation that can predict the ranges for the sequence of powers based upon the table above. We will find an equation for the sequence of squares, 2^m, and sequence of cubes, 3^m.

Squares:

$$s_2 = 2^{2^{k-2}}$$

Cubes:

$$s_3 = 3^{3^{k-2}}$$

These equations are derived from experimentation. A general solution can be derived due to results found from experimentation.

4 Main Result

The following equation is the prediction for a general solution for any sequence of powers. In these equations,

Proposition 2. *The following equation is true for all power sequences. Let $k \geq 2$, and s_k. Then the smallest number for the k, and n is the power that the sequence is raised to.*

$$s_k = n^{n^{k-2}}$$

Base Case: $k = 1$, $s = 1$ for all power series.

Proof. Prove that s_k is the smallest integer for k iterations. Show that $s_k - 1$ requires $k - 1$ iterations.

$$\mathrm{N(x)} = \sqrt[n]{x}$$
$$N(N(\dots N(n)\dots))$$

s_k is the smallest number for k iterations.

$$\begin{aligned}\mathrm{N}(s_k) &= \sqrt[n]{s_k} \\ &= (n^{n^{k-2}})^{\frac{1}{n}} = n^{n^{k-2}/n} = n^{n^{k-2-1}} \\ &= n^{n^{k-3}} = s_k - 1\end{aligned}$$

Therefore, this proves that it takes k iterations to obtain the smallest number s_k such that it is the smallest number in each interval for iteration k.

5 Conclusion

The next step in this work is to find an equation on other sequences to find similar formulas as they are found for the power series. This could be finding formulas for various other sequences. Some of the sequences we are planning to look at are the Fibonacci sequence and the sequence of all prime numbers. I would like to thank Dr. Swart and Dr. Mukherjee for their assistance in this research. It could not have been done without them.

REFERENCES

[1] Smarandache, Florentin. (2000). Thirty-Six Unsolved Problems in Number Theory, University of New Mexico. Newsroom, Orlando, FL, Aug. 06, 2020.

Reflecting by Jacob Williams

Whistle Blowers: Heroes or Traitors

Will Jensen

William Jensen is a Senior majoring in Computer Science, Mathematics, and Cyber Operations. He serves as Papa company's Academic Officer and Honor Representative, the President of the Math Club, and is involved in the DoD Cyber institution. He is also a member of The Citadel Honors Program and The Distinguished Scholars Program. Upon graduation, he plans on commissioning into the Navy.

Abstract

In the present day, the digital world is for of more information than could even be imagined, ranging from the most mundane logs of temperature readings, to content that may be browsed or streamed, to classified documents. With the recent uptake in viewership of the Snowden Documentary, Available on Netflix, this paper will attempt to define what aspects of whistle blowing are good and what aspects of it are bad, determine when it might be appropriate, and explore some case studies through that framework.

Introduction

In the Summer of 2013, the collection of 3 letter agencies had their world rocked when several of their secrets were exposed to the world by whistle blower, Edward Snowden, with the NSA taking the largest hit of all. Several people have commented on the situation, from reporters and journalists, to the government and the people, both in its implications for the security and defense community, as well as whether the actions Snowden took were justified. Snowden fled the country before releasing over 9,000 documents to The Guardian and other select journalists. The US has taken the position that what Snowden did was considered treasonous, while Snowden and some other key figures that are strong proponents of governmental transparency and Freedom of Information have commended the actions, saying it was in the best interest of the American Public. Regardless of the stance taken, no one would disagree that it has had a lasting impact on both the practices of governmental agencies as well as public reception of actions that those institutions take.

We will discuss the merits of both those who call Snowden a hero, as well as those who see him as a traitor. We will then discuss the necessary conditions for whistle blowing being an ethically sound action, as well as consider the ethical impact that occurs when looking at the short and long term effects of releasing information not originally intended for the public eye. We will also analyze whistle blowing in contexts other than governmental documents, such as industry practices, and examine whether there is a different standard or impact compared to what the government considers national security and defense information.

The Snowden Perspectives

There are several facts about the Snowden situation which are important to note in order to fully understand the scenario, as well as whether or not he can be considered justified in his actions. Edward Snowden first gained experience in computer programming, becoming an expert relative to many of his peers. He dropped out of high school and instead chose to pursue his study of computers at a community college. While studying, he joined the Army reserves, where he attempted to complete Special Forces training, but suffered from a severe injury, leading

to his discharge from the Army. He ended up getting a job working with the Central Intelligence Agency, but left his work following suspicions of him accessing privileged information that was outside of the scope of his clearance. He ended up finding a job with Dell, which placed him as a National Security Agency contractor, originally in Japan eventually moving to Hawaii. He then transferred to Booz Allen Hamilton, in another role contracted with the NSA.

During this role, Snowden began copying classified documents onto a Lady GaGa CD that had the ability to both read and write. He was able to bring it with him to "listen to music" while working and take it home with him after work with several classified documents contained. Over the course of a few months, this allowed him to compile a large number of files, which bore particular interest to the Domestic Surveillance Policies of the NSA. After approximately three months working for Booz Allen Hamilton, Snowden requested a leave of absence from his employer, stating that he had recently been diagnosed with epilepsy and needed some time to get himself in order.

As opposed to using the absence for health purposes, Snowden flew to Hong Kong, where he had scheduled a meeting with journalists from The Guardian. He brought all of his files with him to the meeting, and turned some or all over to the journalists "blowing the whistle" so to speak. Shortly after, The Guardian released these documents to the public, exposing questionable and potentially illegal actions taken by the National Security Agency, again with particular emphasis on their surveillance actions linked to United States Citizens. Following the leaking of the documents, Snowden went into hiding, hoping to seek asylum in Ecuador. During this time, the United States government took swift legal action against him with charges including the theft of government property, unauthorized communication of National Defense Information, and willful communication of classified communications intelligence information to an unauthorized person to name a few. These charges all carried hefty sentences. While either in transit or in hiding, the United States also revoked Snowden's passport. As a result, he became stranded in Russia due to his lack of valid documentation, making him unable to complete his journey to Ecuador as originally planned. The US requested that Russia extradite Snowden, a request which the Russian government refused.

Snowden was granted temporary asylum and residency within Russia, and has voiced that he would come back to America and even serve time in prison if he could be guaranteed a fair trial, though he does not yet feel that a fair trial would occur. He garnered large amounts of international support. He leaked several documents showcasing the NSA and the United States spying on foreign powers through their surveillance. As of now, Snowden has been granted permanent residency status in Russia and has applied for dual-citizenship there as well (specifically due to the uncertainty of the global state in relation to the COVID-19 pandemic and potential border closures). Though he remains in Russia, he claims to still identify as an American, holding American values with plans to raise his child as an American as well (albeit from Russia for the time being).

Pro-Snowden

One ethical lens from which the Snowden case study may be observed paints Snowden as a hero or a morally good individual. There are several reasons that may lead to this view. Given his service, several consider him to truly hold American values. It is undeniable that Snowden broke several regulations in the process of leaking all of the documents that he did, but this perspective would argue that the ends justify the means. By that, the perspective indicates that due to the government overreach in the form of mass surveillance, the government was doing wrong. While Snowden broke laws and contracts with the government to expose the wrongdoing of the NSA, it can be argued that his intentions and impact outweigh the legality of the situation. This perspective paints Snowden to be a watchdog for the American Citizens' privacy. While in Hong Kong, Snowden was interviewed, claiming "I'm willing to sacrifice my former life because I can't in good conscience allow the U.S. government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building." It would seem by that statement that he identified wrong in the systems that are currently in place, and exposed them in an effort to bring attention

to the issues and cause change. Upon examining the impacts, he certainly did cause reform, or at the very least change how surveillance was conducted.

Both Domestically and abroad, there was a large public outcry against the surveillance that the United States was conducting. This led to an inquiry by former President Barack Obama, as well as massive debate in the public sphere regarding what should and should not be acceptable. According to Snowden, mass surveillance creates an imbalance of power between the government and its citizens. He believes that in releasing this information, he returned some of that power to the people and opened an avenue to reform such that new policy could be enacted to prevent the surveillance that he saw occurring on a daily basis from continuing to occur. In terms of political change, Snowden's actions encouraged public debate on government surveillance, while also creating policy shifts, such as Presidential Policy Directive 28 (PPD-28), which directed the Intelligence Community to move away from bulk SIGINT surveillance and instead focus on SIGINT surveillance of specific foreign targets. The ACLU describes PPD-28 as taking unconstitutional acts and making the actions conducted less unconstitutional, though still perhaps outside the purview of what ought to be considered right. Another piece of policy that resulted from PPD-28 was the USA Freedom Act, which prevented the NSA from storing massive amounts of surveillance on their own servers and instead required them to get specific approval from a Foreign Intelligence Surveillance Court and then request the recorded information from the service providers. This changed the government from being able to store and potentially access large amounts of information to instead only being allowed to use information that has been specifically deemed necessary by the court, creating a system of Checks and Balances in government surveillance. While surveillance still occurs, it is significantly hindered relative to what it was before Snowden's whistle-blow.

Outside of the US, Snowden also had a major impact on privacy policy and caused a shift in global sentiment on government surveillance. Abraham Newman and Nikhil Kalyanpur of Georgetown University credit Snowden's actions as one of the primary drivers of the European Union's General Data Privacy Regulation. This policy sets stiff penalties for corporations who disclose information of EU citizens to governmental agencies. It has resulted in billions of dollars lost by major corporations such as Facebook and Google, as well as limited use of sites that collect mass data within the European Union. Additionally, several countries have begun requiring that corporations store data within the country from which it was obtained. For example, both Brazil and Russia require that companies such as Facebook store user information of their citizens within their respective countries as opposed to in the United States, where the US could request or demand access to the information in question. The damages caused by this were estimated to have been approximately 35 billion dollars to US cloud companies by 2016, and only increasing over time.

While Snowden certainly violated regulation in order to reveal this information to the public, those holding a pro-Snowden perspective would argue that his intention in the actions he took was in the interest of the greater good and would argue that the societal change that occurred due to his leaking of information far outweighs any ethical wrongdoings that he may have committed in order to accomplish his mission.

Anti-Snowden

While some take a perspective in favor of Snowden, there are also several arguments that could be made against what he did, both by those that are in favor of the NSA's actions prior to his leak, as well as those in favor of government transparency. One argument that could be made would be the question of Snowden's intentions and legitimacy. While he certainly did collect classified information and leak it to the public, there were questions that were raised to its validity. Since Snowden entered the public spotlight, some issues of his story have been raised dating all the way back to pre-agency Snowden. For example, Snowden has on numerous occasions claimed that he was discharged from the Army due to his breaking of both of his legs while going through training to join the Special Forces. Since coming to fame and making that claim, the government has since released that he was not in fact discharged for breaking his legs, but in fact merely developed some shin splints that prevented him from doing several aspects of training,

A Symbol For Hope by Eric Wilson Jr.

and overall he was simply not a very good soldier who washed out of his training and was discharged accordingly. Following his leak of classified documents, the House Intelligence Committee was charged with investigating the incident and two years later released a three-page unclassified summary of their findings. Rather than labeling him as the hero that some might claim him to be, the committee labeled him as a "serial exaggerator and fabricator" who became disgruntled with several managers, and was not performing as well as he should have been. He allegedly had frequent conflicts in the workplace and was described not as a whistle-blower, but someone who merely twisted the truth in order to paint a narrative that pleased him. This perspective would call into question the legitimacy of much of what Snowden released, indicating perhaps the surveillance was not as he described it, but rather a much more gray area. It would also call into question his motives. If his story was fabricated and he was not honestly releasing the documents but instead a disgruntled employee, then perhaps he was merely fed up with how work was going or looking for a way into the public spotlight. In 2015, Snowden's lawyer disclosed that Snowden made large amounts of income from public appearances and speaking, sometimes being paid more than $10,000 for a single engagement. It would certainly not be impossible that he chose to leak information to "fabricate and exaggerate" as described by the House Intelligence Committee in order to become something of a public figure and cash in for some easy money. As stated by his lawyer, Ben Wizner, "Any moment that he decides that he wants to be a wealthy person, that route is available to him."

Outside of seeing Snowden as fabricator or exaggerator, it is also important to look at the damage he caused. He released between nine and ten thousand documents. The military alone said that the information that he leaked caused billions of dollars worth of damage to its security structures. While some could argue that transparency of government is a good thing, there is, just like in any industry, a need for some secrets to be kept in order to preserve parts of an institution. That is not to say that all information should be hidden behind a shroud of "national security", but the classification system exists for a

reason. Top Secret information is labeled as such because, if released, there is the potential for severe harm to American interests to include the livelihood of its citizens as well as the safety of those who protect it. For example, troop movements are kept classified in order to ensure that enemy combatants are not able to track down and kill American soldiers. If the fact that a ship is supposed to pull into a port is leaked, oftentimes that ship will be delayed or the port visit will be canceled in an effort to protect those on-board from potential attack. While there is plenty of information that can be released to the public without causing danger or harm, there are also aspects of the government that, due to their nature, are unable to be released. While there may be a need for whistle-blowers to release information of egregious acts by the government, it is also important to consider both the actions and the cost of release and weigh the two against one another. It is not as simple as some may make it out to be, and several have questioned whether the information released by Snowden was truly worth the billions of dollars of damage that he caused in doing so, or the potential danger he may have exposed American citizens to in order to become the whistle-blower that he is today.

A third perspective against Snowden is actually for greater governmental transparency, which may seem to be counter intuitive. When analyzing the fallout of Snowden's actions it is easy to see the things he may have directly impacted, such as the PPD-28 or the USA Freedom Act, but there are several other impacts he had as well in the opposite direction. Glenn Greenwald, a journalist and legal expert on First Amendment issues, pointed out two interesting points to this effect. First and foremost, due to Snowden leaking documents in the manner which he did, several agencies of the Intelligence Community, as well as several other public and private sector institutions have implemented much more stringent policies in

Lunar Winter by Matthew Smith

order to prevent future leaks from occurring. One mentioned was the fact that now, places containing secure information and documents are much more strictly isolated from the outside world. If you are working on a computer with classified information, it is very likely that you would be unable to use plug-in devices such as disks or flash drives, degrading the quality of life of those working within that environment, as well as more importantly putting a much tighter lock on the flow of information. While some might appreciate the information that came to light from Snowden, he made it much harder for the next big whistle-blower to expose government secrets. Another interesting point that Greenwald made was the actual impact that Snowden had. On the one hand, policies came about that would in theory restrict governmental surveillance, especially with relation to US citizens, but on the other hand, who is it that is meant to police this? If you are already mistrustful of the government, it would be hard to trust them when they say they will no longer do something such as spy on US citizens when there is no means to check whether they are or are not doing so. While Snowden certainly brought the debate and discussion much more into the public sphere than it was before, what good does that discussion really do if there is no way to verify that the government has changed apart from trust of the government when they say they have changed.

While these are just a few of the arguments against Snowden, they seem to make up the majority in terms of volume. To summarize, Snowden was not necessarily a trusted source, so how can his claims be verified to be completely true, especially when there is a financial incentive present to him. Additionally, if what he said was true, was it worth the damage that he caused in releasing the secrets, and from a less government-trusting perspective, do his actions make it harder for bigger secrets to be exposed, and did he even have an actual tangible impact on the operations of agencies such as the NSA or CIA?

Whistle Blowing Standards

From analysis of the Snowden case, there are a few standards that could be viewed as an ethical framework to analyze "whistle-blowing". There are certainly times when the actions of governments need to be exposed. For example, consider Iran who was violating nuclear agreements. That information could be valuable and could save lives through exposure by directly causing actions of other nations against Iran to prevent them from becoming nuclear capable. Or consider Muammar Gaddafi, who was using chemical weapons against his own people to keep them under his rule. These horrendous acts need to be exposed in order to prevent them from continuing to occur. While this may be a hard matter to judge before the fact, a reasonable standard for whistle-blowers would seem to be whether releasing the information in question will net a greater good for the people of a given country. The government exists to serve and to protect the people, so if they are withholding information that would in fact better serve or protect their citizens if released, then ethically it seems reasonable to state that it ought to be released. Additionally, motivation is always an important thing to analyze. A whistle-blower's motivation for leaking information ought to be for the benefit of his or her fellow man, not for personal gain. While these two standards may be difficult to judge, especially before a leak occurs (to measure the impact) and because motive is a hard thing to quantify, they seem to be the two logical and necessary requirements in order to consider whistle-blowing activities to be ethical. Anything short of this would not be in the best interest of those that a government is meant to serve, and would thereby be considered to be unethical.

References

Edward Jay Epstein and Edward Jay Epstein. 2017. How America lost its secrets: Edward Snowden, the man and the theft. Alfred A. Knopf. Kieran Fitzgerald and Oliver Stone. 2017. Snowden. RAI cinema.

Glenn Greenwald. 2014. . Metropolitan Books/Henry Holt.

Nikhil Kalyanpur and Abraham L. Newman. 2019. The mnc-coalition paradox: Issue salience, foreign firms and the General Data Protection Regulation. JCMS: Journal of Common Market Studies 57, 3 (2019), 448–467. https://doi.org/10.1111/jcms.12810

William E. Scheuerman. 2014. Whistleblowing as civil disobedience. Philosophy Social Criticism 40, 7 (2014), 609–628. https:/doi.org/10.1177/0191453714537263

Carbon Nanotube Types and Application

Charles Geiger

Charles Geiger, a sophomore from Virginia Beach, VA, is a corporal in Charlie company. Charles is majoring in Mechanical Engineering. He has earned Gold Stars and Dean's List twice in his cadet career. He is a member of the Charleston Wesley Foundation, Cordell Airborne Rangers, and Special Operation Auxiliary. Charles plans to commission in the Army as an officer upon graduating the Citadel.

Abstract

This paper presents an analysis of data collected on Carbon nanotubes' types based on geometry and their potential uses. First found, coincidentally in 1991, nanotubes have presented a unique opportunity to revolutionize composites and construction. With tensile strengths that are at least of times stronger than steel in all configurations and unmatched conductivity, carbon nanotubes may become a large proponent in creating spacecraft and small circuits that must endure large amounts of stress. Due to their carcinogenic properties they should not be used on any system exposed to humans. Therefore, I would recommend nanotubes use to stay limited to space or in extremely isolated systems until further research can possibly negate their hazardous side effects.

I. Introduction

Carbon Nanotubes have remained a topic of study for many years after their discovery in the 1990s. With time progressing and more advanced ways to synthesize nanotubes the study and possible application has increased research in the field. Carbon nanotubes present an alternative way to synthesize supports and conductors on a scale unfeasible until only a few years ago. The plausible applications of carbon-nanotubes depend solely on the efficiency of our methods to produce them. This report identifies the 3 types of carbon-nanotubes zigzag, wheelchair, and chiral while noting their properties and possible applications. An in-depth study of their capabilities and possible applications exemplifies nanotubes' ability in miniaturizing tech in our world and pioneering new options for design. This report recommends further testing into the disposal methods of these nanotubes and the effect on humans as preliminary studies present side effects like asbestos. Organized in four parts, section 2 consists of history of development and the applications of nanotubes. Section 3 will consist of an in-depth description of the three different types of nanotubes and their application due to their respective attributes. Section 4 will address the ethical concerns of applications regarding human and environmental safety. The concluding section 5 will discuss the ethical concerns of application and interim application during ongoing studies that will ensure safe use and future viability.

II. History and Development of Carbon Nanotubes

The coincidental discovery of Carbon-nanotubes, unlike most pioneered technologies in the field of composite engineering, will revolutionize our ability to produce micro technology. In the most conventional case, an engineer synthesizes a material specifically to a set group of parameters while carbon nanotubes were discovered as a byproduct of other carbon production. In 1991 Sumio Iijima observed micro tubes of graphitic carbon in the soot of an arc-discharge experiment to produce carbon fibers and fullerene. The first carbon nanotubes byproduct synthesized contained multiple walls of concentric carbon only one atom wide were labeled Multi-Walled Nanotubes (MWNTs).[1] These MWNT's

spurred research by Iijima, Ichihashi, and Bethune et al who developed the next breakthrough in Carbon nanotubes two years later after augmenting the arc-discharge method by including a metal catalyst to the process causing the production of single-walled Nanotubes (SWNTs). Though the intended product reached all parameters, the design process could not synthesize enough SWNTs to make them viable for study and application. In 1996 Smally and coworkers supplemented arc-discharge with laser-ablation (evaporation) synthesis to aligned SWNT with a smaller diameter from graphite rods with small amounts of Ni and Co at 1200 °C. While laser ablation was effective at creating SWNT, it still couldn't produce sustainable amounts at a cheap cost. The last method developed to produce SWNTs was to utilize catalysts during thermal decomposition (CVD). CVD technology stems from the generation of carbon filaments in the 60s by thermally decomposing hydrocarbons. Yacaman et al utilized this method in 1993 to generate hydrocarbon in large quantities. The current CVD process typically utilizes decomposition of hydrocarbons (a known toxin) ethylene, or acetylene, at temperatures of 550-750 C.[2] Since the inception of these new technologies methods of refining the product and easier production has pioneered most recent advancements with large scale production of nanotubes accomplished by the development of CVD with an iron catalyst by Li et al. Despite recent advancements in the production of carbon nanotubes a cost of 50 USD per gram is the limiting factor slowing testing and application. [3] With the demand constantly growing in tech industries the cost and time requirement will decrease with further study and soon it may end up in everyday devices.

III. Carbon Nanotube Types and Geometry

When studying Carbon nanotubes, the two categories consist of, SWNTs and MWNTs, based upon the number of concentric layers. The main point of study for carbon-nanotubes are the three subcategories differentiated by geometric shape due to different attributes each possess. These groups named for the form the nanotubes possess are armchair, zig-zag, and chiral. The way to distinguishing factor of the subcategory is the pattern generated in the nanotube structure, which is dependent on the angled cut and fold of the atom-wide sheet of graphene. A classification of zigzag indicates incisions in the graphene that remain straight in line with a value of (m=0) at a 0-degree angle. When the graphene sheet angle matches (m= n) at 30-degree angle it is classified as armchair. If the carbon nanotube's fold equals at any angle between 0 and 30 it is chiral, but these vary in design because the angle varies slightly between each nanotube.[4] (Figures 1 and 2 show the difference among the three patterns).

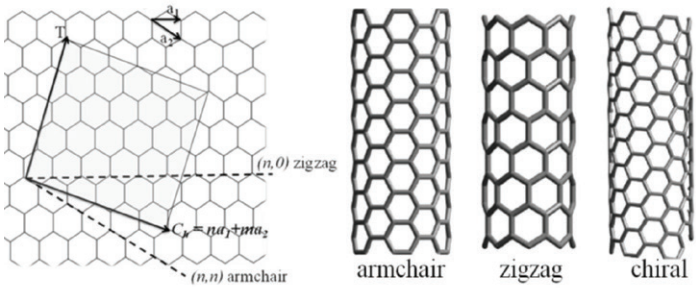


Fig. 1. Diagram showing how the cut angle of tubes affects the geometry and their corresponding labels [4].

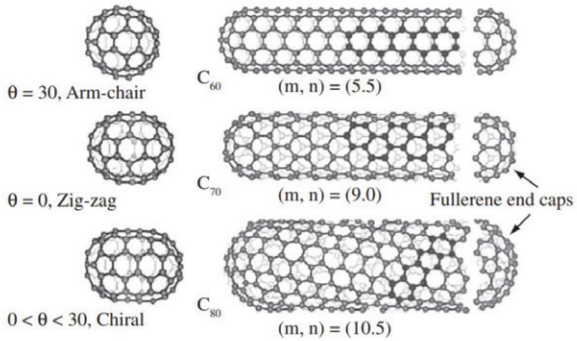


Fig. 2. 3D rendering of carbon nanotubes exemplifying the radial symmetry or lack thereof due to the cut angle [5].

The difference in these geometric patterns causes differences in their properties. Nanotubes all share identical composition which causes nearly identical thermally conductivity, electrical conductivity, and stability up to 2800 degrees Celsius (in a vacuum).[5] Despite their similar attributes in conductivity and thermal tolerance their difference is in pressure tolerance. When diameter is one-nanometer or larger, zig zag possesses the highest stress tolerance, while when under one-nanometer, armchair nanotubes possess the highest stress tolerance due to the curvature effect. In each scenario

chiral experiences the lowest pressure rating at a relatively unchanging

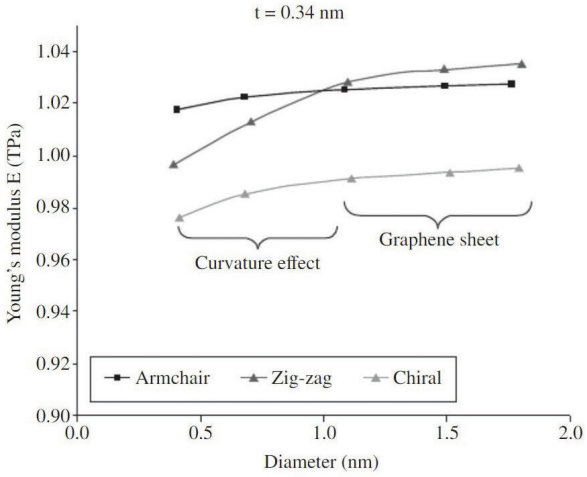


Fig. 3. Graphical representation of nanotube strength based on type and diameter [5].

level due to a very small curvature effect. (Figure 3 shows the curvature effects on stress tolerance for the three types of nanotubes). The three sub-types' overall strength affected the tensile strength differently in SWNTs and MWNTs with SWNT ranging from 0.32 to 1.42 TPa and MWNTs ranging from 0.27 – 0.96 TPa.[5] While impressive, the three ways discussed to produce carbon-nanotubes does not escape design flaws and this inconsistency in diameter, chirality, and length cause the strength ranges to vary. Carbon Nanotubes present unparalleled tensile and flexible strength capacities despite minor variation due to the angled cut ranging from 0-30 degrees. With the difference in cost to produce nanotubes being negligible an argument for any type could be presented, but I recommend using the zig-zag geometry due to most room for error at high stress at a similar cost.

IV. Recommendation for Application

My recommendation for the future of nanotubes is complicated. While the attributes of nanotubes are virtually unparalleled preliminary studies unfortunately show effects close to those of asbestos. Further research in mice concluded that Carbon nanotubes do cause cancer and because of the diameter of only nanometers the way they interact with the human body is nearly identical to asbestos. Inhaling nanotubes is the primary way nanotubes effect the human body as once inside the lungs nanotubes' small sizes causes severe cell damage directly linked to cancer and left untreated can cause death.[6] Due to the hazardous effects, as a future engineer, I cannot in good faith recommend their use on any construction or design plan that could one day expose living creatures or the environment to nanotube particles when in use or in disposal. Therefore, until further studies determine how to synthesize nanotube's in a safe manner such as coating them, combining them in other composites, or coiling them in steel piping, I would recommend applying nanotubes strictly on satellites and in isolated computer systems to limit possible effects. While limiting their use on Earth is not preferable their applications in space and ability to conduct heat and electricity may revolutionize the speed at which our satellites can generate electricity, disperse heat, and transmit data.

V. Conclusion

Carbon Nanotubes present an unparalleled opportunity for humanity to push the boundary of what is physically pssible due to current limits on tensile strength and conductivity issues. With tensile strength at least five times stronger than steel in all configurations the plausible applications are endless to what money can design and will allow for new technologies to be pioneered. Unfortunately, while we are close to reaching this point further studies in the effects on humans and animals must be done as the carcinogenic properties present pose too large of a risk to utilize nanotubes in everyday products. Hopefully one day the technology will be present to nullify these effects, but until then, the uses in isolated systems and space will be one to look forward to.

References

[1] S. Iijima, "Carbon nanotubes: past, present, and future," Physica B: Condensed Matter, vol. 323, no. 1-4, pp. 1–5, 2002.
[2] V. N. Popov, "Carbon nanotubes: properties and application," Materials Science and Engineering: R: Reports, vol. 43, no. 3, pp. 61–102, 2004.
[3] A. M. Thayer, "Carbon nanotubes by the metric ton," Chem. Eng. News, vol. 85, no. 46, pp. 29–35, 2007.
[4] V. Choudhary and A. Gupta, "Polymer/carbon nanotube nanocomposites," Carbon nanotubes-polymer nanocomposites, vol. 2011, pp. 65–90, 2011.
[5] A. F. A´ vila and G. S. R. Lacerda, "Molecular mechanics applied to singlewalled carbon nanotubes," Materials Research, vol. 11, pp. 325–333, 2008.
[6] S. Toyokuni, "Genotoxicity and carcinogenicity risk of carbon nanotubes," Advanced Drug Delivery Reviews, vol. 65, no. 15, pp. 2098–2110, 2013.

An Examination and Analysis of Sensor Technology as it Relates to Autonomous Vehicle Design

Matthew Unden

Matthew Unden, a sophomore from Huntsville, AL, is a private in Charlie company. Matthew is majoring in Mechanical Engineering and has earned Gold Stars three times. He is a Peer Instructor for Calculus II, former Vice President of Public Relations for The Citadel's Toastmaster Chapter, and a Regimental Operations Clerk. He is a founding member of The Citadel's Rocket Club and a member of The Citadel Honors Program. Matthew plans to work as a civilian mechatronics engineer in the future, researching and developing new robotic technologies.

Abstract

The role of sensor technology in the advancement of vehicle autonomy will be discussed. Major problems regarding sensor technology as it relates to autonomous automotive enhancement will be identified, and recommended solutions to these problems will be presented.

1. Introduction

Since the invention of the first Automobile, vehicular technology has consistently evolved in a fashion leading to less and less human interaction, and with the latest advances in Artificial Intelligence (AI) and Robotics, fully automated motor vehicles are no longer a thing of the future. Currently, self-driving vehicles tend to be an experimental tool used by wealthy corporations, far too experimental and expensive for the average citizen to own; however, as this feature becomes more available and spreads to the general population, autonomous vehicles (AVs) have the capability to half the number of deaths and injuries caused by human errors such as DUIs, speeding, and road rage. However, autonomous machines are not infallible; there are several failure points to address when designing fully automated vehicles, and most relating to how the vehicle perceives the world around it. The purpose of this report is to outline and to evaluate three failure points of modern sensor technology as it relates to AV design and development. This stems from the idea that most vehicle autonomy errors stem from the fallibility of sensor technology, specifically its accuracy and reliability, vulnerability to hacking, and response to sensor input which will all be addressed later in the paper. **Section 2** will discuss the technological design of autonomous vehicle sensor technology. **Section 3** will evaluate the failure points of that technology by using real-life examples. **Section 4** will address the recommended course of action to be taken to maximize the efficiency and safety of autonomous vehicle development. Lastly, **Section 5** will discuss the overall nature of AV sensor technology and address the future trajectory of AVs.

2. Design of Autonomous Vehicles

Simply put, autonomous vehicles work just like a standard computer; they take in sensory information and then use that information to perform actions related to the vehicle's motion. Devices like this are commonly referred to as Input/Output (I/O) Devices, where the input is the sensory information going in, and the output is the actions performed according to the input information. Since vehicular technology has been constantly developing since the late 1800s, the output physical motions of a

vehicle have been fine-tuned to the point where it is not difficult for experienced designers to control. As such, the complexity of the system comes almost solely from the complexity of the input data. The vehicle must consider data from a multitude of range detection sensors, cameras, and internal data systems such as GPS to make instantaneous decisions about how to move the vehicle. Luckily, this is well within a modern computer's capabilities, though it may prove challenging for modern programmers and engineers.

2.1 Obtaining and Interpreting Input Data

AVs utilize several different types of input instruments, or sensors, to obtain accurate information about the world around them and react accordingly. Commonly used sensors on autonomous vehicles include Radio Detection and Ranging (Radar) sensors, Light Detection and Ranging (Lidar) sensors, and Cameras all of which will be explained in-depth in the following subsections [1].

I. **Radar Sensors**: Radar sensors function by sending out radio waves and counting the time it takes for the waves to bounce off something and return to the sensor [2]. Utilizing the return time and the known speed of radar waves, the sensor calculates the distance traveled by the wave and cuts that in half to determine the distance from the sensor to the object the wave bounced off [2]. Radar sensors have been in use for a very long time, and as such, they have been developed over time to determine distance much more reliably and for a further distance than any of the other sensors [2]. However, radar sensors respond significantly slower than the other light-based sensors and are more prone to interference [2].

II. **LiDAR Sensors**: LiDAR sensors function essentially the same way as radar sensors, only using laser light instead of radio waves [2]. LiDAR is much newer, so it has had less time to develop than radar; as a consequence, LiDAR has not been quite as fine-tuned as Radar making it slightly less reliable [2]. However, light travels much quicker than radio waves making LiDAR detection much faster than radar, but at a slightly shorter effective range [2].

III. **Cameras**: Essentially, cameras function as a way of capturing images by exposing a light-sensitive grid to the environment and making note of the changes to create digital images [3]. However, computers do not process these images the same way the brain does. The brain sees a collection of objects at different points in space, while the computer only sees an assortment of colors with no perception of depth or special awareness [1]. As such, in order for a camera to be used as a sensor in an AV, it needs to go through a lot of complex editing and processing so that the system can utilize color variations to recognize some important objects as we do [1]. While this type of sensing is highly difficult and largely inaccurate in many cases, it is necessary for detecting visual signals such as street signs or signal lights, as there is currently no other technology capable of detecting these objects.

2.2 Sensor Fusion

While these sensors are helpful on their own, none are consistently accurate enough to be relied on to solely protect the vehicle and its passengers. As such, many companies developing AVs have turned to sensor fusion. This involves combining the input data of multiple sensors covering the same area to get more descriptive results [1]. The most common combinations of sensors in sensor fusion in AVs are **camera-radar (CR), camera-LiDAR (CL), and camera-LiDAR-radar (CLR)** [1]. The fusion of the sensors in this manner aids the vehicle best in determining accurately where objects are (camera-based object detection) and at what distance (radar and LiDAR sensing) [1]. Furthermore, there are three methods of combining sensors in sensor fusion: **high-level fusion (HLF), low-level fusion (LLF), and mid-level fusion (MLF)** [1]. In HLF, sensory data is processed individually and then combined to reduce uncertainty [1]. This method is more accurate than one sensor alone and is easier to program, but less accurate than the other two methods of fusion [1]. LLF combines the raw data from both or all sensors and processes them together [1]. This leads to much more accurate information than the other two methods but is incredibly complex and difficult to program [1]. Finally, MLF is a sort of middle ground between the two, offering more accuracy than HLF without the full complexity of LLF [1]. MLF takes certain important aspects of each sensors raw data, such as depth or color and processes them together [1].

3. Analysis of Autonomous Vehicles

Because the process of interpreting sensory data is so complex, there are many ways it can fail, all of which need to be accounted for in AV design. The following subsections utilize case studies of in-use Autonomous Vehicles and Semi-Autonomous Vehicles (SAVs) to identify major failure points in AV design.

3.1 What if My Car Sensors Fail?

As discussed previously, processes like object identification, depth, and position mapping are not infallible, even when using LLF sensor fusion. Under abnormal conditions, identifying important objects such as road markers, stop signs, or other vehicles can be next to impossible due to interferences and abnormalities on the road or with the sensors themselves. What if heavy rain or fog interferes with the sensors or blocks the camera? What if the sun leaves a glare on the camera lenses making identification more difficult? What if you're on a road with unclear or no lane markers? All these things could lead to inaccuracies in input data regardless of how it is processed, and thus could lead to a catastrophic response from the vehicle. One such study conducted by AAA Automotive in August of 2020 on SAVs with Driving Assistance demonstrates this principle. AAA Automotive researchers found that over the course of 4,000 miles, SAVs with driving assistance tended to show a problem potentially caused by sensor abnormalities every 8 miles [4]. These problems relating to sensor misinterpretation or uncertainty ranged from getting too close to other vehicles, guard rails, or lane markers to disengaging acceleration or speed control with little to no warning and handing control back to the user [4]. While on their own these mistakes aren't much; however, in unusual driving situations these minor failures could lead to a catastrophe, putting the vehicle's passengers and surrounding vehicles/ pedestrians in major danger.

3.2 What if My Vehicle is Hacked?

One problem that must be considered in the design of any autonomous device or technology is cyber security. If hackers were allowed to remote access the AVs central computer and replace or edit the input sensory data, there's no limit to the havoc it could cause. Hackers could reroute the GPS sending people to unsafe destinations and leaving the passengers vulnerable to attacks such as kidnapping, theft, or rape; they could make the vehicle veer off course into a brick wall at high speeds; or they could tell the vehicle to brake suddenly as seen in this ethical hacking study on a 2014 Jeep Cherokee [5]. In this study, two ethical hackers successfully accessed the Jeep of a consenting journalist, telling it to brake immediately [5]. This exploit was found to be functional at high speeds, which could prove fatal if the vehicle was accessed going 70 mph on a busy freeway [5].

3.3 What if My Vehicle Detects Something It Can't React to?

A common issue people tend to associate with AVs revolves around a famous ethical discussion called "The Trolley Problem." The problem suggests a scenario in which there really is no right answer and the person in control must know how to act [6]. The original trolly problem depicts a case in which an out-of-control trolley speeds down a track towards 5 people with no time to remove them from the track; however, you are in front of a switch that can change the trolley's heading to only one person [6]. In both cases, someone dies, but the person gets to choose who lives and who dies. This problem has led to a long debate over how to best handle the situation knowing that there is no clear answer, but computers rely on clear answers. They make black and white decisions by sensing the surroundings, identifying the possible outcomes, and determining the best course of action to take, but if there is no clear answer, the computer will stall not knowing how to react. For example, what if an AV's sensors detect a crowd of pedestrians 5 feet in front of it when going 40 mph on a single lane road? Does the vehicle veer off the road potentially harming its passengers or just attempt to stop as safely as possible? This unclear situation would cause the AV computer to get trapped in an infinite loop of trying to determine a correct course of action eventually causing it to crash if reactions to the scenario are not built into the vehicle. Thus, this eventuality must be accounted for when designing AVs, but if a programmer is to account for such situations, are they partially at fault for the horrendous results? The ambiguity of this situation must be resolved for AVs to have a future.

The Price of Warmth by Matthew Smith

4. Recommendations

While there are plenty of concerns and difficulties with AV sensor technology, if implemented correctly, the technology has the potential to save millions of lives each year. Thus, it is imperative that we continue to design, to test, and to develop this technology in SAVs so that it may create a safer standard of transportation in the future when full autonomy is reached. Though throughout the future development of AV sensors, all the problems in Section 3 must be addressed. While there is no clear-cut solution to fix all these problems, there are some steps we can take to minimize the risk factor of each issue. To minimize the issue regarding sensor accuracy under debilitating conditions, the vehicle should be tested in each condition to ensure safe driving capability within a certain safety threshold and contain backup sensors to fall back on should the other sensors fail. Furthermore, additional research should be conducted into sensor fusion and object detection so that the margin for standard sensor error lessens. To fix the cyber security issue, it should be made standard that all AVs be tested thoroughly by cybersecurity professionals and ethical hackers to ensure maximum passenger safety. Finally, in the "Trolley Problem" failure mode, AVs should be programmed to make the decision causing the least amount of impact at the slowest speeds. This decision should be agreed upon publicly and defined legally so that there is no room for liability suits so long as the vehicle follows the agreed upon standards.

5. Discussion

To ensure maximum public safety, passenger vehicle engineers should stick to designing only semi autonomous vehicles (SAVs) until sensor fusion technology and object recognition programming reach a 99.9% accuracy rate. While the technology itself could be instrumental in decreasing the number of roadway casualty and injuries, if improperly designed, the AVs could instead double the number of vehicular incidents. At the current junction, AV sensor technology is not at a point where vehicles can remain reliably autonomous. Though by continuing to advance this technology in SAVs, the car industry will slowly but surely move into higher levels of autonomy until full autonomy is reliably reached, finally achieving the century-long goal of fully automated roadways.

References

[1] D. J. Yeong, G. Velasco-Hernandez, J. Barry, and J. Walsh, "Sensor and Sensor Fusion Technology in Autonomous Vehicles: A Review," Sensors, vol. 21, no. 6, 2021, doi: 10.3390/s21062140.

[2] E. Brandt, "Lidar vs Radar: Pros and Cons of Different Autonomous Driving Technologies," The Drive, Dec. 12, 2017. https://www.thedrive.com/article/16916/lidar-vs-radar-pros-and-cons-of-different-autonomous-driving-technologies (accessed Nov. 08, 2021).

[3] J. Lodriguss, "How Digital Cameras Work," AstroPix, 2021. https://www.astropix.com/html/astrophotography/how.html (accessed Nov. 16, 2021).

[4] E. Edmonds, "AAA Finds Active Driving Assistance Systems Do Less to Assist Drivers and More to Interfere," AAA Newsroom, Orlando, FL, Aug. 06, 2020.

[5] T. Brewster, "How Jeep Hackers Took Over Steering And Forced Emergency Stop At High Speed," Forbes Magazine, Aug. 02, 2016. Accessed: Nov. 08, 2021. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/08/02/charlie-miller-chris-valasek-jeep-hackers-steering-brake/?sh=60bc51263f48

[6] H. Roff, "The Folly of Trolleys: Ethical Challenges and Autonomous Vehicles," Washington, DC., Dec. 2018.

Dangerous Technology: Modern Threats Posed by China and Russia

Cooper Morse

Cooper Morse is a freshman with an Intelligence and Securities Studies major and History minor. He is pursuing a career in the United States Air Force with the hope of becoming a pilot. Cooper's father is a Citadel alumni, Class of '89, and is his source of motivation to succeed and to achieve academic excellence.

Abstract

The emerging technology from China and Russia pose potential serious threats for the US. In this intelligence report, key technologies in China and Russia are analyzed for their threat potential, weaknesses, and overall stake in the race to come out as the most technologically advanced military. These technologies include AI, Space Capable Assets and UGVs, all of which present concerns for national defense and international peace.

Key Judgement

1. We believe that emerging technology in foreign countries will pose a threat to the US.

2. We believe that China is the world leader in the field of technological advancements.

3. We believe that China is making advancements in AI technology.

4. We believe that China is developing space technologies for military operations.

5. We believe that Russia is also a threat in technological advancement.

6. We believe that Russia is developing AI technology for military application.

Analysis

Throughout history, it was often true that whichever side of a military conflict had the most advanced technology, was the side likely to emerge from the conflict victorious. World powers are constantly racing to be the most technologically advanced nation so that, in the event of an armed conflict, they might have an edge and emerge victorious, or at the very least, be secure. The United States is concerned with monitoring the emerging technology of foreign countries for this very reason. The US is primarily focused on China, as they are widely regarded as the leaders of technological advancement in the world. Though China's technological advancements branch into a wide range of application fields, this paper focuses on the military applications specifically, or those which pose the most profound threat to US. Artificial Intelligence (AI) prospects. Space assets are another potentially threatening technology coming out of China due to China's future operation plans for the military application of space technology. Russia also presents a prevalent concern for the US as they have, for the last half-century, established themselves as a global power in research and development. However, it is important to note that Russia is not as advanced as China, or even the US, but still their focus on developing AI technology for military application; UGVs (Unmanned Ground Vehicles) present merit for concerns.

Assessment

Emerging technology has always been a key concern for the US. Being "ahead of the game" in the field of technology is crucial to promote peaceful advancements among the world powers. But to remain objective and never naive, we note that the two most threatening countries in this regard are China and Russia. Although there are other countries such as India with a growing mission of technological development, here we are discussing the two countries that the US views as the most historic and, thus, probable threat.

Throughout the 20th century, technological innovation is what made the US one of the most powerful nations in the world. Recently, however, the scale has seemingly tipped to the side of China, enabled by the largest command-driven market, centralized government, and coordination between private sector and state technology research. These factors have given the Chinese the resources necessary to make unprecedented leaps in technological development in the fields of artificial intelligence and space capable assets. This has led to the US taking a particular interest in the emerging technology and technological advancements of China.

One of the main technological threats that the US is monitoring is artificial intelligence. AI is seen by many as the next breakthrough in military technology due to the numerous applications it could have if developed to a certain level of proficiency. One of the advantages of military applied AI is the notion that it could reduce the endangerment of human life in warfare. However, this could also be the downfall of AI application, as many believe that if it were less costly on human life to go to war, countries would choose to go to war more readily. Because of this, the US monitors its rival's developing AI technologies. China is the largest concern, as they have been shown to have incredibly advanced AI technology, as well as their New Generation Artificial Intelligence Development Plan of China, which describes China's plan to develop advanced AI to use in various capacities through 2030. China has a specific focus on the military application of AI, which is why the US views this technology as such a threat in the hands of the Chinese. China plans on increasing the precision, speed, and effectiveness of future military operations using advanced AI-assisted systems.

Another technological threat emerging from China is the possibility of space warfare technology. Although the idea of space warfare sounds like science fiction, it is becoming increasingly more possible as the boundaries between physics and computing are being tested. As revealed in the China Space and Counterspace Report, China is researching space capable asset technology, and they are likely to become the dominant force in this emerging field. The basic concept of space capable assets is through satellites or spacecraft that are directed towards

The Perspective by Joshua Babcock

armed intervention rather than merely surveillance. If joint firepower strike operations become operable, which would specifically target Taiwanese and US persons of interest for elimination, the game field of war and the threat of atomic contingencies approach apocalyptic levels. Additionally, China is researching joint blockade operations of space assets in a prelude to an invasion of Taiwan. Although this technology seems far off, China appears quite confident in their capabilities as a diversified nation invests much of its time, intellectual and financial resources.

Although not nearly as advanced in the field as China, Russia has a long history of tension with the US, now exacerbated with AI as the current pinnacle of technological capabilities and the

expansion outward from the limitations of the past. Russia's belief is that whichever county is the leader of AI technology, will be the leading world power. Despite this mantra, Russia is noticeably behind both China and the US in AI advancements. Russia's AI development programs are unique, however, given that jurisdiction of research and development are directed solely by state-owned firms, rather than any private sector or political interest groups. Ultimately, this seems due to deep-founded distrust between the Russian government and private-sector tech companies looking towards the intrinsic value of innovation rather than geopolitical "tech races." The state-owned firm Sberbank is Russia's primary researcher and developer of AI technology.

Though being far less organized and capable in AI development than the US or China, Russia is still pushing AI research in hopes of finding sufficient military application. One of these military applications that Russia has found for AI is unmanned ground vehicles (UGVs). Russia has been found testing UGVs in Syria, and has seemingly made significant development in the application of this technology for military operations. The benefits of such technology would be the reduction of human lives risked in warfare, and the coordination of a centrally controlled fleet of UGVs, adding to the effectiveness of coordinated strikes.

The implications of China and Russia possessing these technologies is concerning beyond the mere implications of what public life will look like in the East. AI is such a new field of technology that the US does not have extensive knowledge on how to combat technology, primarily regarding AI operated hacking programs. Thus, creating a "national insecurity" in the field. A program with AI could potentially rewrite its code to hack through firewalls while remaining largely untraceable. AI operated UGVs are a less severe threat however, as EMP weapons would likely be highly effective at disabling these vehicles. Space capable assets from China could be devastating if they possessed the ability to perform orbital strikes against US targets. The best defense against this that the US prossesses is anti-satellite weapons which could eliminate these space capable assets in a preemptive strike.

China is responsible for numerous covert actions against the US in the form of cyber and drone attacks and possibly preparing for an invasion of Taiwan, one of the allies of the US. Similarly, Russia is massing troops on the Ukrainian border and making demands for the nation to relinquish its territory, pointing towards Russia's interest in reclaiming the territory they lost post WWII. So in order for the US to remain strong in its defense of freedom, not only domestically, but also for its allies abroad, it is imperative that the US maintains a close watch of the emerging technologies coming out of these two countries, in order that the US might be able to better counteract whatever conflicts arise involving these technologies.

We conclude that a close watch on the development of emerging technology in China and Russia is prudent for the safety of the US. The potentially catastrophic consequences of an unforeseen attack utilizing one or more of these technologies is reason for the US intelligence community to conduct counterintelligence operations but also perpetuates further dilemmas concerning global power competition, privacy and liberty for Americans and our allies, and the future landscape of AI relations among nations and the citizens they wish to protect.

References

[1] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, (April 9, 2021): pp 20
[2] Can Huang, Naubahar Sharif, "Global Technology Leadership: The Case of China," Science and Public Policy 43, no. 1 (February 2016): pp 62–73
[3] Fei Wu, Cewu Lu, Mingjie Zhu, Hao Chen, Jun Zhu, Kai Yu, Lei Li, Ming Li, Qianfeng Chen, Xi Li, Xudong Xoa, Zhongyuan Wang, Zhengjun Zha, Yueting Zhuang, Yunhe Pan, "Towards a New Generation of Artificial Intelligence in China," Nature Machine Intelligence 2 (June 16, 2020): pp 312-316
[4] Elsa Kania, "'AI Weapons' in Chinese Military Innovations," Global China (April 2020)
[5] Mark Stokes, Gabriel Alvarado, Emily Weinstein, Ian Easton, "China's Space and Counterspace Capabilities and Activities," (March 30, 2020)
[6] Stephanie Petrella, Chris Miller, Benjamin Cooper, "Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms," Orbis 65, no. 1 (2021): pp 75-100
[7] Ash Rossiter, "Bots on the Ground: an Impending UGV Revolution in Military Affairs?," Small Wars and Insurgencies 31 no. 4 (June 5, 2020): pp 851-873
[8] Oriana Mastro, "The Taiwan Temptation: Why Beijing Might Resort to Force," Foreign Affairs 100, no. 4 (July/August 2021): pp 58-67
[9] Eray Alim, "'Decentralize or Else': Russia's Use of Offensive Coercive Diplomacy against Ukraine." World Affairs 183, no. 2 (June 2020): pp 155–82

The Opioid Crisis and its Connection to Dentistry

Harry Charles

Harry Charles is a junior from Rock Hill, South Carolina. He is the Drum Major for Band company, and is majoring in Biology with the intent to become a dentist after graduating. In his free time, Harry enjoys playing piano and juggling.

Abstract

The correlation between dental prescriptions and the opioid crisis has long been established, but poorly understood. This paper will discuss the history, techniques, and trends that explain how the modern dental industry has inadvertently contributed to the opioid crisis, and what measures should be or have already been taken in order to address this problem.

I. Introduction

The opioid crisis has been on the rise since the 1990s and has only become more prominent as opioids have become more readily available as a medication. Dentistry is a common contributor of opioids to the public as dentists are capable of and often expected to prescribe opioids to patients. Opioids are frequently a go-to medication for common dental pains/aches. Dentists have a responsibility to prescribe opioids to patients who need this medication; the only problem is that there are many who seek out dentists for the sole purpose of acquiring opioids with the intent to abuse them. While it may seem like the opioid crisis does not affect everyone, this could not be further from the truth; "In 2017, 11.4 million US citizens misused prescription opioids, resulting in 46 overdose deaths daily and a $78.5 billion burden on the economy" [8].

For these reasons, the opioid crisis has become an issue relevant not only to dentists but the general public as well. This report will identify the different classes of opioids relevant to dentistry and what can be done in response to the crisis by the dental community. The most common opioids are codeine, oxycodone, and tramadol. To combat the opioid crisis, dental education should require knowledge of the opioid crisis, as well as how to recognize those patients who are potentially addicted to opioids. In addition to this, dentists should seek to prescribe other effective but less addictive medications before resorting to prescribing opioids. Only through this increased awareness and alternative routes can dentists do their part to combat the opioid crisis.

II. History

To know how to end the opioid crisis, it is important to know how it began. The opioid crisis is generally said to have begun in the 1990s, when doctors began prescribing opioids to patients complaining of aches and pains. It was not long after this that people began dying due to overdoses on opioids. In fact, during the time between 1999 and 2010, over 630,000 people in the United States died due to drug overdoses, most of which were due to use of opioids prescribed for pain [1]. The government has taken many measures to try and lessen the effects of opioids on our society, most of which have been increased control of these sorts of substances [1]. Some of these measures have been

somewhat successful, but the opioid crisis is still an issue as many gain opioids through legal means. The writer asserts that this problem must be handled at the source, that being one of America's primary sources of opioids: dentists.

Hovel by Cort Hanellin

III. The Crisis' connection to Dentistry

1. *Are Dentists really contributing to the Opioid Crisis?*

The origin of scandalous activity is often ambiguous, as those who participate intend it to be that way. Thus, the above question must be asked; attacking a falsely perceived cause will do nothing to hinder the effect. Unfortunately, the evidence overwhelmingly points to dentists as an inadvertent but prominent source for opioid abuse in America. According to the Journal of the American Dental Association, "an estimated 23 percent of prescribed doses are used nonmedically" [2]. 1 out of every 5 people leaving a dentist's office with opioids are inappropriately using that medication to get "high," which as the history of the opioid crisis demonstrates, can have less-than-desirable effects on society. Furthermore, the Australian Prescriber writes that "In the United States a pre-filled opioid prescription, given for the extraction of wisdom teeth, has been found to be an independent risk factor for persistent opioid use" [7]. It seems unmistakably obvious, but it must be acknowledged by all medical professionals: giving patients opioids increases their risk of opioid addiction. All of this is not to say that dentists are acting irresponsibly with their prescribing of opioids. They are an efficient medication at their intended purpose (pain alleviation), and often do a huge service to those patients with strong pain after intense procedures. But the Australian Prescriber goes on to say that "Dentists may…be targets of 'doctor shopping', in which drug-dependent people seek drugs for misuse from multiple prescribers" [7]. Dentists cannot read minds, so when a patient says they are experiencing dental pain, there is no choice but to try and treat it. For a long time, this has meant giving patients codeine, oxycodone, and tramadol (which constitute the 3 most misused pharmaceutical products) [7]. Dentists must be aware that not all patients truly need the prescribed medicine, and that many negative effects can arise from erroneous prescription of opioids. Dentists must then respond to this burden of responsibility by doing what they can to mitigate the opioid crisis.

2. *Do Dentists have an obligation to fight the opioid crisis?*

The goal of a dentist is simple: treat medical issues of the mouth. With the opioid crisis in mind, however, the question must be asked: What should a dentist do when their treatment of a single person is potentially decreasing the health of the overall population? If there is any sort of substance which they deem an adequate medication for use on their patients, one would generally agree that they should use it. After all, the Hippocratic Oath (a covenant taken by all medical professionals upon graduating

from medical school) states "I will apply, for the benefit of the sick, all measures [that] are required" [4]. But the Hippocratic Oath also says, "I will prevent disease whenever I can, for prevention is preferable to cure" [4]. The responsibility of a dentist is not solely to uphold the health of one person, but to uphold the health of all. By continuing to prescribe opioids despite the evidence that it is worsening the opioid crisis, dentists are ironically undermining populational health. For these reasons, dentists have a clear and undeniable obligation to do what they can to combat the opioid crisis. The writer's answer to the previously asked question: Dentists should consider methods of providing pain alleviation to their patients without overprescribing opioids if it is possible. This paper will elaborate on those possibilities.

3. Is lessening the prescription of opioids feasible?

It is easy to slander opioids and call for them being taken off the market when one looks at any data concerning the opioid crisis. But anyone who has ever undergone an intense medical procedure will surely testify to the importance of pain medication. So, is increased risk of addiction as opposed to suffering patients really just the lesser of two evils? The data suggests otherwise. "In 2016, the proportion of prescriptions written by US dentists that were for opioids was 37 times greater than the proportion written by English dentists" (Table 1) [6]. America is very advanced in many ways, but it seems to be lagging when it comes to the opioid crisis. Dentists in England typically try to prescribe nonsteroidal anti-inflammatory drugs (NSAIDs) and acetaminophen rather than opioids, which is obviously a preventative measure for opioid addiction. The effectiveness of these alternatives to opioids will be discussed later in this paper. Furthermore, this same study found that while "the codeine derivative dihydrocodeine was the sole opioid prescribed by English dentists, US dentists prescribed a range of opioids containing hydrocodone (62.3%), codeine (23.2%), oxycodone (9.1%), and tramadol (4.8%)" [6]. This is very worrisome because as previously stated, codeine, oxycodone, and tramadol constitute the 3 most misused pharmaceutical products [7]. These opioids with high potential for abuse are far less likely to be prescribed in England [6]. The evidence shows that it is completely feasible to decrease the number of opioids prescribed for dental pain, but that American Dentists simply are not making the effort to do so.

IV. Recommendations

1. *Dentists must be more skeptical of patients*

Patients lie to dentists sometimes. This is nothing new, seeing as many dentists must frequently interrogate as to just how often their patients are really flossing. As previously cited, "Dentists may…be targets of 'doctor shopping', in which drug-dependent people seek drugs for misuse from multiple prescribers' [7]. When it comes to opioids, being aware of human nature and being somewhat mistrustful of patients could be the difference between life and death. If dentists are to ever be capable of doing their part to end this opioid crisis, they must be willing to question returning patients constantly complaining of mouth pain and wanting opioids. Of course, there would be far less worry for addicted patients if dentists could simply prescribe only non-addictive drugs. Luckily, this is an entirely possible solution, and should be put into practice.

Table 1. Dental Prescribing Rates and Frequencies in the United States and England in 2016 [6]

Prescribing Outcomes	United States	England
Number of Dental Opioid Prescriptions	11,440,198	28,082
Population-based Opioid Prescribing Rate, Number of Prescriptions per 1,000 Population (95% CI)	35.4 (25.2-48.7)	0.5 (0.03-3.7)
Clinician-based Opioid Prescribing Rate, Number of Prescriptions per Dentist (95% CI)	58.2 (44.9-75.0)	1.2 (0.2-5.6)

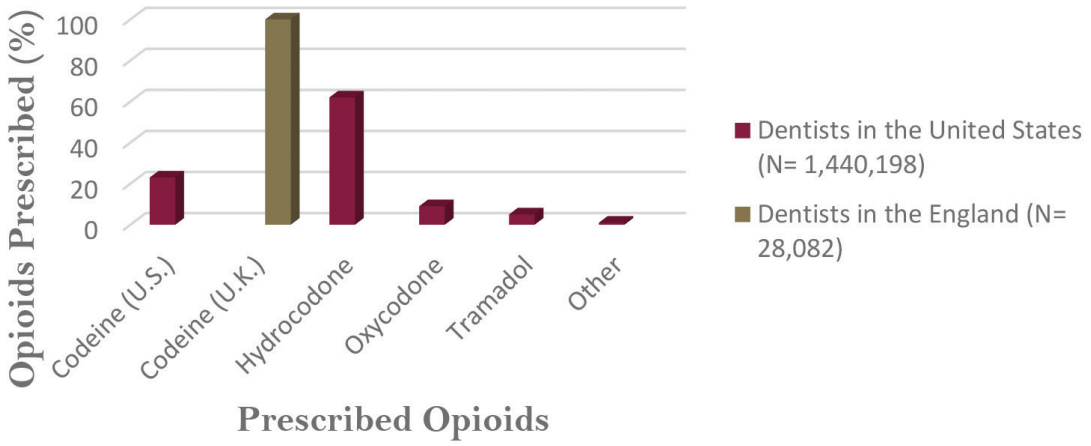


Fig 1. A bar graph showing the variety in opioid prescriptions made in the United States and England [6].

2. Alternative Medications

The easiest way to prevent opioid abuse is to stop giving people opioids. It seems so obvious as to not even be worth mentioning, but as the previously mentioned data shows, American dentists have not yet made a coordinated effort to avoid opioid prescription where possible. Dentists must consider alternative methods for pain alleviation, of which there are many: "results from reviews published respectively in 2018 and 2016 help confirm that NSAIDs and NSAID-acetaminophen combinations are as effective as or more effective than opioids for controlling dental pain and cause significantly fewer adverse effects" [8]. NSAIDs are nonsteroidal anti-inflammatory drugs, and they account for most analgesic prescriptions in Europe, where opioids only account for 0.6% of dental prescriptions [8]. This contrasts greatly with America, where "22.3% of US dental prescriptions were for opioids" [8]. Multiple studies have found that NSAID and acetaminophen are just as effective for dental pain alleviation if not more so than opioids, yet so many American dentists still prescribe opioids. Why? One could argue that many dentists are simply sticking with what they know/are comfortable with and are unenthusiastic about having to increase their knowledge set. But medicine is a constantly growing field, and doctors must be made aware of new developments that improve the field.

3. Increased Education about opioids

There must be a large-scale campaign by the American Dental Association to ensure all dentists are aware of the potential determinants associated with prescribing opioids, as well as being made aware of the alternative medicinal options available. Luckily, some areas of the country have already begun efforts to make this idea reality. For instance, in 2017, "Governor [of Massachusetts] Charles D. Baker… challenged the state's four medical schools and three dental schools to improve their curricula to prepare the next generation of clinicians to deal with this crisis in an evidence-based, effective, and sympathetic way" [3]. Awareness is the most important thing when dealing with a large-scale issue like this one, and Charles Baker's initiative is a great start. Thankfully, the data in the past couple of years, shows that most dental students are being made aware of their role in the opioid crisis in dental school.

Mitigation plans like this one are effective, too. According to the scientific journal entitled Substance Abuse, "Dentists reporting prior training in drug diversion were significantly more likely to have accessed their [Patient's] PDMP [prescription drug monitoring program], $P < .01$" [5] The prescription drug monitoring program is a running file on all patients which shows what medication they have been prescribed and when, which assists in avoiding over-prescription (especially of opioids). Dentists have been known to rarely bother in accessing these files, but as the evidence demonstrates, increased education about opioids can change this. Dentists must be advised to be wary of patients who might deceive them to obtain opioids.

V. Discussion

The opioid crisis has had devastating effects on our society, and it is clearly in everyone's best interest that it be taken care of. But dentists, one of the biggest providers of opioids in America, have yet to do that which is in their power to mitigate the abuse of opioids by Americans. Dentists must acknowledge that patients may lie to them to obtain opioids, as awareness of this phenomenon will allow them to avoid being manipulated. They must be aware of the alternative but equally effective medications which patients are less likely to become addicted to, such as NSAIDs. Most importantly, as awareness is key, every state should do as Massachusetts has done, and ensure that no dentist can become certified without being made fully aware of the opioid crisis and the power that they must use to fight it. If dentists continue to practice and prescribe as they have done in the past (which is more comfortable for them), opioids will continue to run rampant, and continue to spread its negative effects on society. But with these new implementations, dentists can become smarter and thereby safer with their prescriptions and help to create a better economy built by better people to make our nation a better place to live.

VI. Acknowledgments

The author would like to thank his parents for supporting his education, as well as Dr. Eggleston for all she has taught.

VII. References

Bernard, S. A., Chelminski, P. R., Ives, T. J., & Ranapurwala, S. I. (2018). Management of Pain in the United States—A Brief History and Implications for the Opioid Epidemic. Health Services Insights, 11. https://doi.org/10.1177/1178632918819440

Denisco, R. C., Kenna, G. A., O'Neil, M. G., Kulich, R. J., Moore, P. A., Kane, W. T., Mehta, N. R., Hersh, E. v., & Katz, N. P. (2011). Prevention of prescription opioid abuse: The role of the dentist. Journal of the American Dental Association, 142(7), 800–810. https://doi.org/10.14219/jada.archive.2011.0268

Keith, D. A., Kulich, R. J., Bharel, M., Boose, R. E., Brownstein, J., da Silva, J. D., D'Innocenzo, R., Donoff, R. B., Factor, E., Hutter, J. W., Shaefer, J. R., Karimbux, N. Y., Jack, H., & Thomas, H. F. (2017). Massachusetts Dental Schools Respond to the Prescription Opioid Crisis: A Statewide Collaboration. Journal of Dental Education, 81(12), 1388–1394. https://doi.org/10.21815/JDE.017.098

Edelstein, L. (1943). The Hippocratic oath: Text, translation, and interpretation. Baltimore: The Johns Hopkins Press.

McCauley, J. L., Leite, R. S., Melvin, C. L., Fillingim, R. B., & Brady, K. T. (2016). Dental opioid prescrib ing practices and risk mitigation strategy imple mentation: Identification of potential targets for provider-level intervention. Substance Abuse, 37(1), 9–14. https://doi.org/10.1080/08897077.2015.1127870

Suda, K. J., Durkin, M. J., Calip, G. S., Gellad, W. F., Kim, H., Lockhart, P. B., Rowan, S. A., & Thornhill, M. H. (2019). Comparison of Opioid Prescribing by Dentists in the United States and England. JAMA Network Open, 2(5), e194303. https://doi.org/10.1001/ jamanetworkopen.2019.4303

Teoh, L. (2020). Editorial: Opioid prescribing in dentistry – is there a problem? Australian Prescriber, 43(5), 144–145. https://doi.org/10.18773/austprescr.2020.056

Thornhill, M. H., Suda, K. J., Durkin, M. J., & Lockhart, P. B. (2019). Is it time US dentistry ended its opioid dependence? The Journal of the American Dental Association, 150(10), 883–889. https://doi.org/10.1016/j.adaj.2019.07.003

Tompach, P. C., Vincent, S., Peterson, A., Tu, H. K., & Born, D. O. (n.d.). *Corresponding author. https://doi.org/10.47363/JDSR/2020(2)111

Upon the Perch by Eric Wilson Jr.

Understanding the Impact of Quantum Technology on Modern Cryptography

Shiloh Smiles

Shiloh Smiles is a senior from Oscar company currently serving as the Regimental Recruiting Officer. She is a double major in Computer Science and Cyber Operations, as well as a minor in Computer Engineering. She serves as both the captain of the Competitive Cyber Team as well as the newly-founded Citadel Rock Climbing Team. After graduation, she will work for the Navy as a red team operator.

Abstract

Modern cryptographical standards are intrinsically threatened by the advent of quantum technology. Standard modern-day cryptography permeates all aspects of life, from individual's daily correspondence to the most secure business's inner working. When quantum computing becomes an available technology, all information being encrypted and sent today will become visible to adversaries who care to look for it. Due to the heavily technical nature of quantum computing and its relatively non-immediate nature, most average citizens are not informed as to what quantum computing entails for their security. Understanding the technical and social mechanics of this threat will cause individuals, businesses, and teams alike to be more informed about this threat. In response to the security threat quantum computing poses, several groups, including governmental cybersecurity standard creators, are developing solutions to this future threat. The information in this report was compiled from a variety of reports on the subject of quantum cryptography as well as current government documents.

Keywords- Quantum, qubits, superpositions, Grover's Algorithm, Shor's Algorithm, cryptography, period-finding, post-quantum cryptography, cryptosystem, information-theoretic cryptography

I. Introduction

Quantum technology is not only a buzzword in the tech industry, but a rapidly developing field that will completely change the computing landscape. This futuristic technology will have countless applications on processing power, computer speed, and computational complexity.

Notably, quantum technology will have a negative impact on the security of modern cryptography. This paper will explain the mechanics of cryptography, why and how quantum cryptography is a threat to modern cryptography, what this means for businesses and consumers, and will explore potential solutions.

II. Background

The term quantum, as space-age as it may sound, simply refers to the smallest amount of physical entity needed in any given interaction. When referring to computers, this refers to using the smallest logical units possible to facilitate decision-making. These quantum bits, smaller even than typical binary 1's and 0's are referred to as qubits. In addition to being physically smaller, qubits can have superpositions, which allows them to have more states than just a binary system. The combination of these two traits allows quantum computers to be almost inconceivably quicker—in fact, even simple systems of about a dozen particles would take thousands of years of energy to model on existing architecture [13]. To put this into perspective, quantum computing would require millions if not billions of particles—a far cry from twelve.

It was first theorized nearly two decades ago that the advent of quantum computing would lead to the downfall of modern-day cryptographic standards, such as public-key or symmetric ciphers. These cryptographic standards, along with the mechanics of the quantum computers which threaten them, will be broken down in the following pages [10].

Thankfully for modern data security, quantum computing is not yet a reality. Forbes estimates quantum computers coming to market as early as 2030, but it would be such a leap in technology that it is difficult to truly ascertain [7]. The National Institute of Standards and Technology's (NIST) Computer Science Resource Center, one of the reigning authorities on computer security standards, estimates total obscurity of modern cryptography standards in twenty years due to quantum technology [3]. Regardless of the exact timeline, quantum technology is an inevitable threat. Due to this threat, it is becoming increasingly important for society to understand what is to come in the realm of cryptography.

III. Classical Cryptography

Cryptography is the security technique of encrypting communications to make their contents unreadable. A very simple form of cryptography may call for a person to simply make each letter one further in the alphabet, while more complex ciphers involve mathematics that a human brain alone couldn't begin to solve. The most used cryptographic or "encryption" algorithms today have names such as RSA, AES, and DES. This report will refer to the wide array of cryptographic techniques which make up the modern standard as "classical cryptography".

There are three pivotal steps to any successful classical algorithm. Each must have a random method of encoding (encryption), a way to ensure the randomness of numbers, and a method of transmission of the code and its key [1]. Compromising any one of these factors leads to a breakdown in the security of encryption. Currently, several different encryption algorithms exist which rely on different methods of transmission or levels of encryption. Some notable algorithms include the unbreakable one-time pad and the wide-spread symmetric and public-key encryptions.

The one-time pad is well known as the most secure form of encryption. Every single character is rotated by a completely random number independent of any other part of the message and random digits are interjected into the message. Since the message is so well encoded, it is not all too critical that the actual message is kept secret; however, the key being intercepted in transmission would be disastrous.

The most common form of encoding is symmetric-key encryption. In this form, a common algorithm with a custom key is used to encrypt the information. See Figure 1 below. This is different than the one-time pad because it is not a completely random scramble; it still follows rules. However, the sheer length and mathematical complexity of the algorithm leads to it being nearly impossible to crack—in one instance, it took a group of 300,000 people four-and-a-half years to crack one 64-bit symmetric key [5].

Figure 1. Symmetric Key Encryption [16]

Another common form of cryptography, and the method facing the largest threat from quantum computing, is public-key encryption. This form of encryption uses a publicly available "public key" to encrypt the information, and a separate "private key" to decrypt it. See Figure 2 below for a diagram. RSA is one of the most famous forms of public-key encryption and bases its security off the difficulty of factoring incredibly long prime numbers. To explain further, imagine someone wants to use the numbers p = 5 and q = 20 as their keys. Multiply these two numbers together and the answer is 100. However, if all someone knows is that p * q = 100, then there is no way to know if p = 10 and q = 10, if p= 25 and q = 4, or several other possible factors. Now imagine this concept but with a value thousands of digits long; it is nearly impossible to determine the exact two numbers that were the original keys. These secret numbers are then used in an algorithm to transform the original message into something unreadable, making the message just as irretrievable as the original "p" and "q".

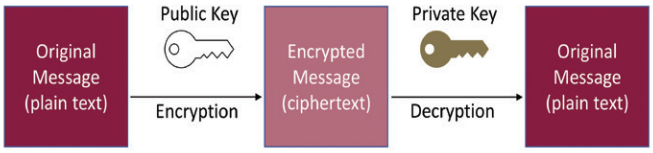


Figure 2. Public Key Encryption [12]

IV. Threat of Quantum Computing

As explained earlier, quantum technology is exponentially faster than classical computing, meaning that the timelines needed to crack modern cryptography become expedited. This threatens the integrity of modern cryptography as its security is due to the fact that cracking it would take thousands of years to brute-force. Cracking symmetric key encryption could take half the time due to Grover's algorithm and cracking public-key encryption could take a matter of hours due to Shor's algorithm [5].

Grover's Algorithm

Grover's algorithm, at its core, is a quantum algorithm which brings a linear search into quadratic time. To explain this in less technical terms, imagine a team is tasked with finding a specific person's business card out of a jar containing thirty cards. At most, they will check all thirty, at least, they will check just one, but on average, they will check fifteen cards before they find it. If n = 30, then the average would be n/2. In Grover's algorithm, the average case is $\sqrt{N}$. In the business card case, this would bring the average closer to 5.5—a significant improvement on 15. It is difficult to visualize how this works as it does not follow the rules of traditional physics, but the following section from my paper titled "Implications of Quantum Computing on Computational Complexity Theory" includes a simple analysis of the main components of Grover's algorithm:

"Grover's algorithm beings with a quantum "coin flip". It applies the equation:

$$m = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

which essentially transforms a bit into a superposition of two states, appearing as a coordinate pair with both values having a value = $\left(\frac{1}{\sqrt{2}}, \pm\frac{1}{\sqrt{2}}\right)$. The second value is either negative or positive and represents a phase.

The Walsh-Hadamard Transformation (WHT) is one of the crucial steps of Grover's algorithm and is applied by comparing these superposition values. This transformation is vital to the efficiency of quantum algorithms, as it allows multiple states, distinguished by their amplitudes, to exist at one time. This cannot be replicated in classical computing." [2]

The pivotal and most applicable piece of Grover's Algorithm, bolded above, is its ability to analyze multiple states at once. Referring to the earlier example of the business cards, Grover's Algorithm can set the states in such a way that more than one business card can be analyzed at the same exact time. This is impossible in both the human brain and by classical computing.

This has very dangerous implications for symmetric key encryption as it is primarily protected by the sheer quantity of time it would take to try every possible key. With Grover's Algorithm, this time would be divided down by several factors [9]. This quantum speedup is what causes quantum computing to be able to break modern cryptographic standards so quickly in comparison to modern technology.

Shor's Algorithm

Shor's algorithm has dangerous implications for public-key encryption. Using a quantum mechanics known as period-finding, Shor's Algorithm can bring the process of factoring a number to a speed of 3(logN), as opposed to classical cryptography, which is unable to bring it to (logN) for any number. The "log" in this equation is short for logarithm, which is the inverse of an exponent. An example of a process which can run in logarithmic time would be searching for a name in a telephone book. If someone is searching for "Sally Smith" and opens to last names beginning with F's, they can skip a large chunk of the pages to get closer to the S's. In the end, they will likely only need to check 10-12 pages instead of the hundreds of pages in the phonebook. This would be logarithmic time and is a significant improvement over checking every page, or value, individually.

Shor's Algorithm can attain this quantum speedup by the utilization of superpositions (see Background for further information). Since each qubit can hold more than just a singular one or zero, the algorithm is able to evaluate more than a single possibility at any given time, which is the key difference between classical and quantum architecture. This is the difference between trying each key on a key ring one at a time versus being able to try them all at once.

As expected, the latter experiences a very significant speedup.

The algorithm is split into two parts: a classical reduction section and the quantum period-finding section. The classical section involves the following steps:

As discussed previously in Section III, the key to security in public-key encryption is the difficulty of reverse engineering the factors of a given number. The above algorithm makes use of the "gcd" factor several times, which is "greatest common denominator"

1. "Pick a pseudo-random number a < N
2. Compute gcd(a, N). This may be done using the Euclidean algorithm.
3. If gcd(a, N) ≠ 1, then there is a nontrivial factor of N, so we are done.
4. Otherwise, use the period-finding subroutine (below) to find r, the period of the following function:

   f(x) = ax mod N, i.e. the smallest integer r for which f(x + r) = f(x).
5. If r is odd, go back to step 1.
6. If a r/2 ≡ -1 (mod N), go back to step 1.
7. The factors of N are gcd(ar/2 ± 1, N). We are done." [14]

(GCD). Using GCD is key to determining factors. The use of this, along with quantum computing's ability to test several states or possibilities at once, is the heart of why this algorithm can break factors so much more effectively. Section III explains the importance of factors to public key encryption and this section of Shor's algorithm works to find these pivotal factors, therefore destroying the framework of public key encryption's strength.

The quantum section is also known as a period-finding subroutine or order-finding subroutine and utilizes a quantum algorithm known as "the Fourier transformation" [14]. The mathematical proof contains several quantum equations such as this probability-determining transformation:

$$N^{-1}\left|\sum_{x\,:\,f(x)=f(x_0)} e^{2\pi i x y/N}\right|^2 = N^{-1}\left|\sum_{b} e^{2\pi i (x_0 + rb) y/N}\right|^2$$

Similarly to Grover's algorithm, this quantum equation serves to shorten the amount of time it takes to test possible solutions. The Fourier transformation can process many states at once and return the state with the highest probability. The quantum mathematics behind this transformation, while fascinating, are not especially important to understanding its impact on public key encryption. By combining with the GCD equation in the previous paragraph, Shor's algorithm can quickly determine potential factors and test them in record time, rendering public key encryption ineffective.

V. Impact of Quantum Computing

It is a matter of when, not if, quantum computing will be able to break all current cryptographic standards. This means that all data that is being sent right now will one day be able to be decrypted. Currently, threat groups are actively compiling encrypted data in massive dumps to be broken when quantum technology becomes available. These dumps come from intercepting network traffic, data exfiltration from hacks, and even just encrypted data available on the Internet. Some things will no longer matter, like a credit card number that will expire in a few years. Other things, such as a social security number, will still be a hazard if they are broken a decade later. This will have life-changing impacts on businesses and individuals.

Impact on Businesses

Businesses of all kinds, from banks to grocery stores, have private data that they are obligated to protect. Although businesses tend to have better cybersecurity than any given individual, there are still countless ways for a hacker or threat actor to gather encrypted data to store for future cracking. This raises pressing ethical and financial concerns.

Most credible businesses use very secure forms of encryption. It is rare that encrypted data is brute-force decoded using modern computer hardware. However, when these quantum methods become prevalent, a question could be raised about to what extent a business is responsible for the privacy of its consumer's data in such a rapidly changing environment. Even businesses using the most up-to-date, state-of-the-art encryption protocols will have their current encryption standard broken as if it

were stored in plaintext. This means that all current encrypted data will be easily visible to even the most amateur hackers. Businesses will soon need to decide, or be legislated on, to what extent they are responsible for protecting modern data from future hackers.

Impact on Individuals

Individuals take on some of the greatest risk from the advent of quantum computing. Since most individuals do not hold any sort of legal obligation for their own data, keeping perfectly updated cyber security standards is not too important. Threat groups are far more likely to have individual's encrypted passwords than they are to have a business's internal data. Although individuals may not hold the responsibility for millions of clients in their hands, losing the security of their encrypted data could still be disastrous. Social Security numbers, banking information for long-term investments, or logins for sensitive items such as a life insurance policy could be disastrous to be uncovered fifteen years from now.

VI. Post-quantum cryptography

As the threat of quantum computing technology draws ever closer, the age of classical cryptography will come to an end. The future of cryptography lies in the aptly named field of post-quantum cryptography. Post-quantum cryptography will need to create enhanced security that is resistant to the increased speed and complexity of quantum systems. This comes in several forms, such as longer keys, algorithms inundated with quantum mathematics, and use of quantum random number generation. Fortunately, there are several existing research bodies and techniques within this field.

Current Approaches

There are several existing approaches to post-quantum cryptography, all of which are in their infancy. Some of the most famous are "lattice-based cryptography", "extended hash-based cryptography", "code-based cryptography" and even "super singular elliptic curve isogeny cryptography" [11]. These very jargon-filled terms are not just to confuse the average citizen but are instead indicative of the complexity of these techniques.

All the current post-quantum cryptographic techniques have strengths and weaknesses. For example, code-based cryptography is vulnerable to a form of modified brute-force-style attack known as "information-set decoding" [6]. There are solutions to this attack, but it causes messages with code-based cryptography to have keys up to a megabyte in size, which is too large for a reliable system. Code-based cryptography will not be an effective solution until its space requirements are solved.

Lattice-based cryptography, conversely, does not have a current known weakness. However, similar algorithms have been broken with Shor's Algorithm, and more time dedicated to breaking lattice-based cryptography will likely yield a similar disastrous result. This potential vulnerability prevents lattice-based cryptography from being an ideal standard.

Hash-based cryptography has a heavy need for reliable logging and note-taking, as reusing a key can destroy the entire cryptosystem—the set of algorithms used to implement a given security standard. Although hash-based cryptography is one of the most well-researched methods [4], this vulnerability makes it imperfect as a global standard.

As evidenced by current approaches' flaws, there is no one post-quantum cryptographic technique that is equitable in security level or ease of use to classical cryptography. Due to a lack of funding, available architecture, and qualified researchers, research in the field of post-quantum has not raised to the same relative level to quantum technology as classical cryptography to modern architecture. As the time of quantum computing draws ever nearer however, more companies, organizations, and even parts of the government have begun their searches in the field of developing a cryptographic standard.

Current Standardization Efforts

NIST has formally "initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms" [3]. This means that there will soon exist a standardized, governmental method to resisting the threat of quantum computing in the future. Once a quantum-resistant cryptography standard is formally implemented, businesses, individuals, and especially

the government and military will be able to have a uniform method of encrypting information that will not need to be wary of an encroaching threat. The sooner a quantum-resistant standards can be implemented, the better, as that means less present-day encrypted information will need to be hidden or expunged when the technology comes into existence.

The search for a quantum standard launched in November of 2017 and is ongoing at the time of this paper's creation. NIST made a public call for submission with several rules, such as strict evaluation

Grateful by Cort Hanellin

requirements for any algorithm wanting to be considered. Since the initiation of this search in 2017, NIST has narrowed the pool down to four groups. The four teams making it to Round 3, the current round, presented their findings less than a year ago at the time of this paper's creation [4]. Most of the submissions are based off the techniques discussed in the prior section.

NIST, although the most relevant in this paper's country of origin, America, is not the only body funding research into a standard for post-quantum cryptography. Other bodies include The Internet Engineering Task Force, who has almost finalized a complete standard for a hash-based signature system. This effort is well-known as the most developed current effort globally. In Europe, the EU Horizon 2020 PCRYPTO project leads. They have already released several suggestions, such as AES-256 and a version of code-based cryptography. The drawback to these suggestions is their immense cost. Other groups include ETSI and OASIS [6]. These efforts show that the global scientific community is moving towards a standard which addresses the threat of quantum computing and hopefully eliminating the looming threat.

Information-Theoretic Cryptography

An alternative approach to the advent of quantum computing is the implementation of information-theoretic cryptography. This form of cryptography encrypts messages under the precedent that a given adversary has unlimited computing potential and can apply to both classical and quantum scenarios. The cryptosystem was developed using principles from the mathematical field of information theory focused on the rules guiding how messages are transmitted through a communication system or network [8].

Although often theoretical and "probabilistic" in nature [8], information-theoretic cryptography is important to consider in post-quantum cryptography. It approaches encryption algorithms with the assumption that any adversary has unlimited computing potential. This assumption is known as "information-theoretic" or "unconditional" security. This differs from traditional algorithms like RSA or AES, as they rely on the power limits of classical computing as a safety mechanism, leading to the moniker of "computational security" [15]. As technology heads towards more computationally powerful quantum architectures, cryptosystems using computational security will become insecure or even useless, while information-theoretic systems will remain secure. This permanent promise of security makes information-theoretic systems a promising avenue to protect against the computationally powerful quantum computing threat.

Information-theoretic systems are very resource-intensive to implement, and therefore do not have many modern implementations. One famous example, and one mentioned earlier in Section II, is the one-time pad. The one-time pad is information-theoretic because the amount of computational power present has no bearing on the ability to decrypt the message—it will stay impossible. Unfortunately, the

one-time pad is far too resource-intensive and secure channel-dependent to be applicable as a post-quantum standard. However, there are several potential implementations being researched in the field of information-theoretic systems, such as "generalized random oracles" or a quantum key agreement [15]. Like the standards discussed in subsections A and B of this section, information-theoretic cryptography is a potential route to secure information in a world with quantum technology. It is worth noting that an information-theoretic standard would come with the added benefit of secure classical encryption in the modern era.

Summary and Conclusion

As the threat of quantum computing technology draws ever closer, the age of classical cryptography will come to an end. The future of cryptography lies in the aptly named field of post-quantum cryptography. Post-quantum cryptography will need to create enhanced security that is resistant to the increased speed and complexity of quantum systems. This comes in several forms, such as longer keys, algorithms inundated with quantum mathematics, and use of quantum random number generation.

The impact that quantum computing will bring to the security playing field cannot be understood. Its sheer power, relatively low energy requirements, and effective speed will render many modern security and cryptography standards moot. In response to this looming threat, several research groups and agencies have begun to take the steps necessary to implement security protocols which can tackle this new technology.

As with any new technology, worry and fear are bound to spread throughout the public due to a lack of information. However, through the information learned in this report, you will be able to leave more informed about not only the threat, but the actions being taken to protect data for lifetimes to come.

References

C. Abellan and V. Pruneri, "The future of cybersecurity is Quantum," IEEE Spectrum, vol. 55, no. 7, pp. 30–35, 2018.

S. O. Smiles, " Implications of Quantum Computing on Computational Complexity Theory," Gold Star Journal, 2021.

I. T. L. Computer Security Division, "Post-quantum cryptography: CSRC," CSRC. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. [Accessed: 12-Nov-2021].

I. T. L. Computer Security Division, "Round 3 submissions - post-quantum cryptography: CSRC," CSRC. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions. [Accessed: 19-Nov-2021].

D. Denning, "Is quantum computing a cybersecurity threat?," American Scientist, vol. 107, no. 2, p. 83, 2019.

D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature News, 14-Sep-2017. [Online]. Available: https://www.nature.com/articles/nature23461. [Accessed: 30-Nov-2021].

G. Fowler, "Council post: When will quantum computers impact our day-to-day?," Forbes, 28-Apr-2021. [Online]. Available: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/04/28/when-will-quantum-computers-impact-our-day-to-day/?sh=55cfd2ba43d9. [Accessed: 15-Nov-2021].

L. Martignon, "Information theory," International Encyclopedia of the Social & Behavioral Sciences, pp. 7476–7480, 2001.

Lov K. Grover. 1996. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC '96). Association for Computing Machinery, New York, NY, USA, 212–219. DOI:https://doi.org/10.1145/237814.237866

M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.

M. Nahed and S. Alawneh, "Cybersecurity in a Post-Quantum World: How quantum computing will forever change the world of Cybersecurity," American Journal of Electrical and Computer Engineering, vol. 4, no. 2, p. 81, 2020.

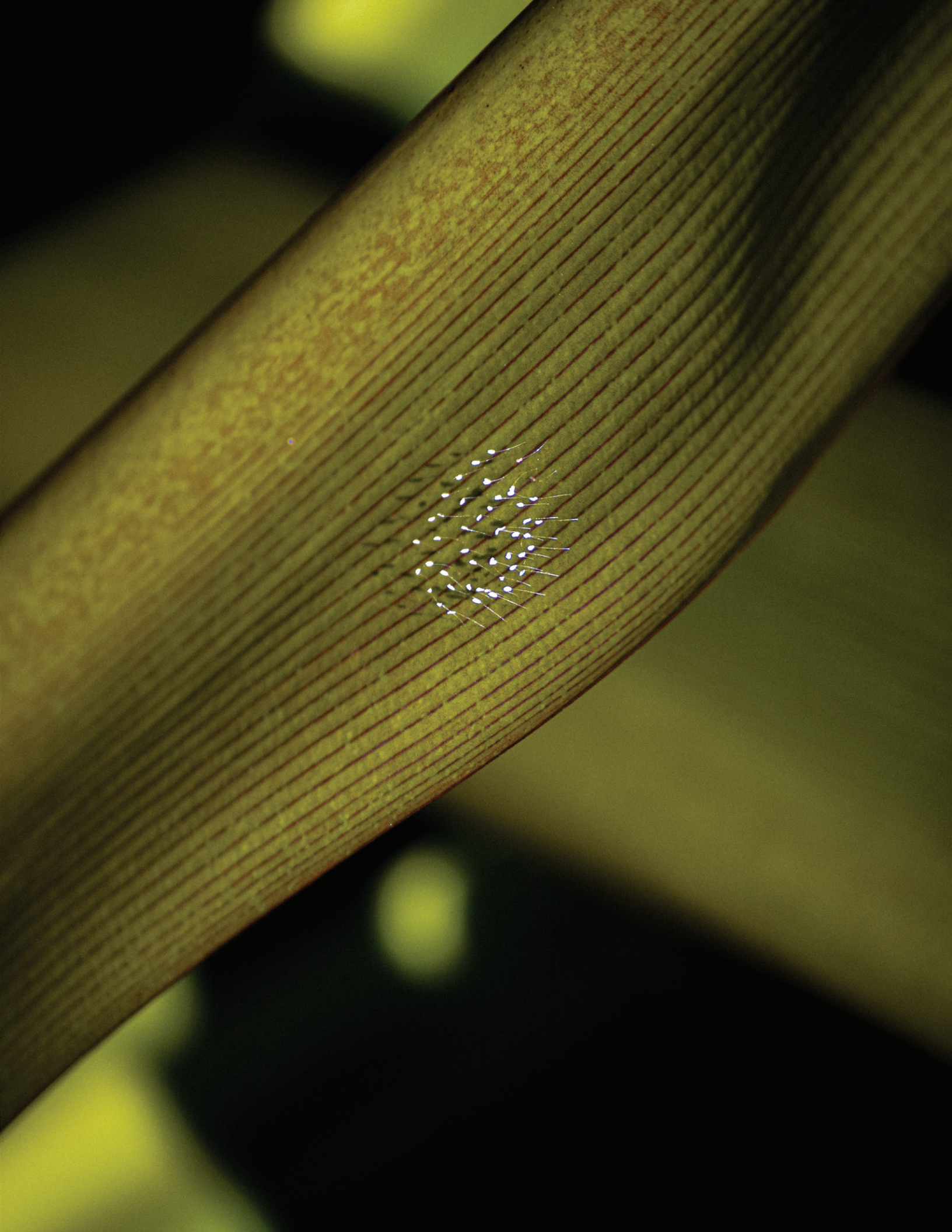
"Public key encryption: What is public cryptography?," Okta Australia. [Online]. Available: https://www.okta.com/au/identity-101/public-key-encryption/. [Accessed: 01-Dec-2021].

QuantumWriter, "Quantum computing history and background - azure quantum," Azure Quantum | Microsoft Docs. [Online]. Available: https://docs.microsoft.com/en-us/azure/quantum/concepts-overview. [Accessed: 15-Nov-2021].

"Shor's factoring algorithm," Quantiki. [Online]. Available: https://www.quantiki.org/wiki/shors- factoring-algorithm. [Accessed: 12-Nov-2021].

U. Maurer, "Information-theoretic cryptography," Advances in Cryptology — CRYPTO' 99, pp. 47–65, 1999.

"What is symmetric key cryptography encryption?: Security wiki," Secret double octopus, 15-Aug-2021. [Online]. Available: https://doubleoctopus.com/security-wiki/encryption-and-cryptography/symmetric-key-cryptography/. [Accessed: 01-Dec-2021].



Featured Photographers

Eric Wilson Jr.

Eric Wilson Jr. is a junior from East Granby, CT, and current squad sergeant in Romeo company. He is a Mechanical Engineering major with a Fine Arts minor and will be commissioning into the United States Air Force upon graduation. He is a photographer for The Brigadier Newspaper, Sphinx Yearbook, and Citadel Republican Society and assists many clubs on campus. Outside of photography, he enjoys hiking, fishing, and nearly any outdoor activity.

Matthew Smith

Matthew Smith, a senior from Leavenworth KS, is a senior private of Alpha company. He is a Physical Education major with aspirations of becoming a personal trainer. He states, "I desire to improve the awareness of the importance of physical fitness." Matthew is a member of The Cadet Chorale and as such, enjoys the performing arts. As a hobby, he enjoys taking pictures of nature and desires to continue to improve his skills in photography.

Joshua Babcock

Joshua Babcock, a senior from Johnson City, NY, originally from Band company, is the Regimental Provost Marshal on Regimental Staff. He is an Intelligence and Securities Studies major with a concentration in Military Intelligence and a minor in Fine Arts. Joshua has been on the Dean's List and has received Gold Stars. He is also the President of The Citadel Flying Club. His aspirations are to work in the intelligence community after graduation. Joshua has a passion for art and photography, and enjoys doing photoshoots during his free time. Joshua states that, "Photography has been an escape from the routine; it has opened a door to new perspectives and viewpoints with a deeper meaning."

Thank you to Cort Hanellin for taking the head shot photographs of the authors and photographers and Brett Stevens for taking the head shot photographs of the Editors.

Featured Photographers

Cort Hanellin

Cort Hanellin is a senior Business major focusing in management. He is in Sierra company, and he is from Long Island, New York. His hobbies include photography, hiking, and riding motorcycles. After graduation, he hopes to live in Charlotte with his dogs and work in a management position for a development company.

Jacob Williams

Jacob Williams is senior from Aiken, SC. He is a Chemistry major and a Fine Arts minor with a love for photography. In addition to photography, Jacob enjoys to travel and is an avid reader. He won the award for best photograph in the 2021 edition of The Gold Star Journal. On campus he is part of the American Chemical Society as well as the Eagle Scout Association.

Kaytlynne McCord

Kaytlynne McCord, a senior from Aynor, SC, is in Delta company. She is a Chemistry major and a Fine Arts minor. She has earned Gold Stars and Dean's List three consecutive times and had a photograph published in *The Gold Star Journal* in 2019. She is a member of the American Chemical Society and is the forward's captain for The Citadel women's rugby team.

The Editors of *The Gold Star Journal* highlight Eric Wilson Jr.'s photohgraphs, The Flag Bearer on page i, Cause For Celebration on pages 50 and 51, and On the Line on page 52, Jacob William's photograph, Blue Ridge Bridge on page 25, and Cort Hanellin's photographs, Steeple Chaser on page vii, Sun Rays on pages 14-15, Basic Sunset on pages 30-31, and Egg Drop on page 47.

The Gold Star Journal 2022 Award Winners

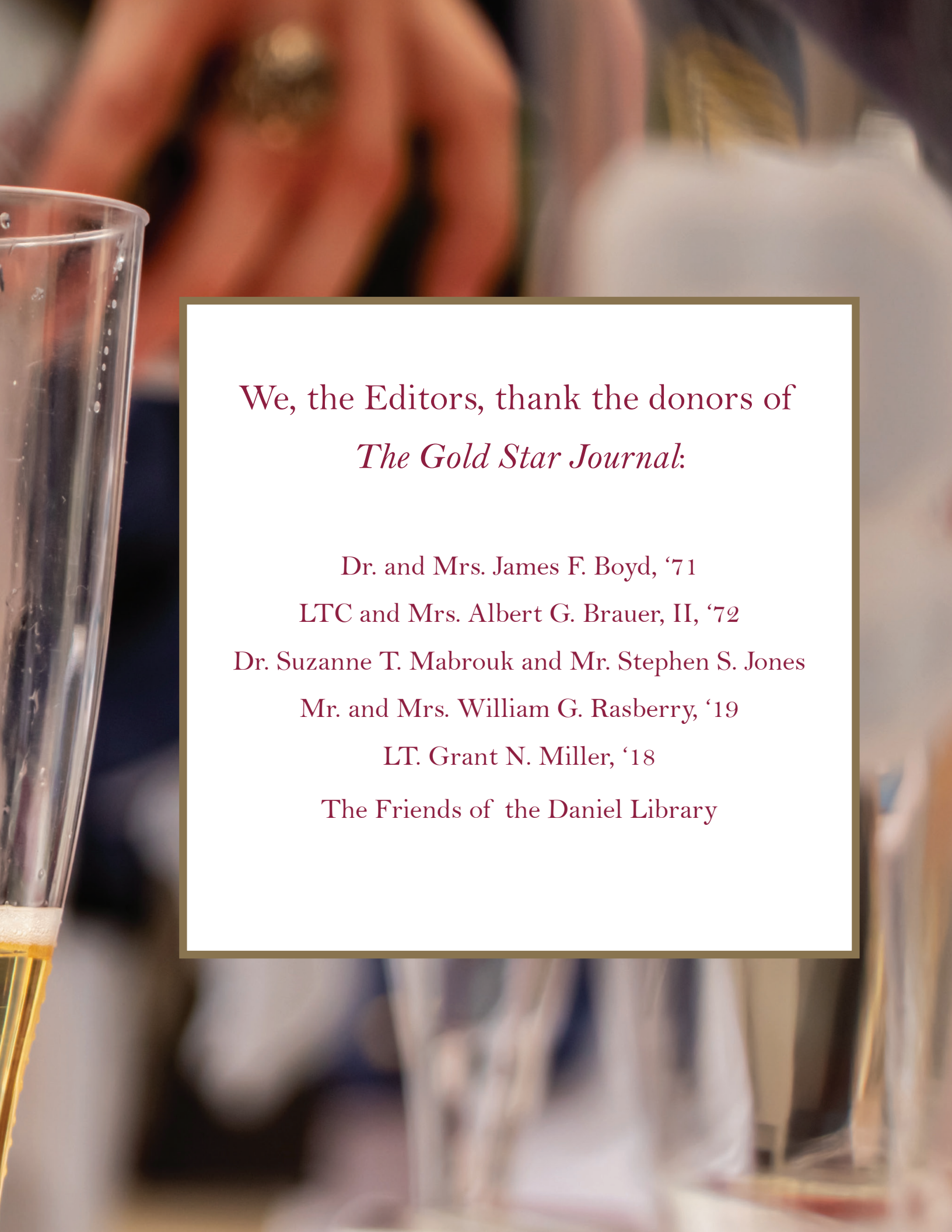
The Best Undergraduate Submission Award
Harry Charles
The Opioid Crisis and its
Connection to Dentistry

The Boyd Family Distinction Award
Charles Geiger
Carbon Nanotube Types and Application

The GSJ Distinction in Photography Award
Matthew Smith
Lunar Winter

The Best Photograph Award
Eric Wilson Jr.
The Flag Bearer

The Best Oral Presentation Award will be given on Tuesday, March 29, 2022 at The Gold Star Journal Academic Conference.



We, the Editors, thank the donors of

The Gold Star Journal:

Dr. and Mrs. James F. Boyd, ‘71

LTC and Mrs. Albert G. Brauer, II, ‘72

Dr. Suzanne T. Mabrouk and Mr. Stephen S. Jones

Mr. and Mrs. William G. Rasberry, ‘19

LT. Grant N. Miller, ‘18

The Friends of the Daniel Library