Cybersecurity & Information Systems
Information Analysis Center

CSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Counter-AI Offensive Tools and Techniques

Report Number:

CSIAC-BCO-2023-441

Completed June 2023

CSIAC is a U.S. Department of Defense
Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
Philip Payne, Matthew Friar, Curtis Smedley
Office: CSIAC

Information contained in this report does not constitute endorsement by the U.S. Department of Defense of any nonfederal entity or technology sponsored by a nonfederal entity.

CSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. CSIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 30 June 2023	**2. REPORT TYPE** Technical Research Report	**3. DATES COVERED** *(From – To)*

4. TITLE AND SUBTITLE Counter-AI Offensive Tools and Techniques	**5a. CONTRACT NUMBER** FA8075-21-D-0001 **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Philip Payne, Matthew Friar, and Curtis Smedley	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Cybersecurity & Information Systems Information Analysis Center (CSIAC) SURVICE Engineering Company 4695 Millennium Drive Belcamp, MD 21017-1505	**8. PERFORMING ORGANIZATION REPORT NUMBER** CSAIC-BCO-2023-441
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center (DTIC) 8725 John J. Kingman Road Fort Belvoir, VA 22060-6218	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Cybersecurity & Information Systems Information Analysis Center performed open-source research and obtained white papers and reports from numerous sources to include the Defense Technical Information Center Research and Engineering Gateway and Elsevier's ScienceDirect. Overall, the research shows that the best way to counter artificial intelligence (AI) offensive tools is with AI defensive tools. The resulting research is described in detail. This TI response report is organized into three distinct sections: (1) completed cyber-AI research, (2) current market studies, and (3) cyber-AI centers. The first section discusses completed cyber-AI research, with reports and perspectives detailing the importance of AI in cybersecurity. Next, this report details current market research and studies. The top defensive and offensive tools and capabilities are mentioned, along with forecasts and statistics on current and future cyber-AI investments. Finally, two institutions specifically created for the study of cyber-AI are identified. The respective missions, along with current work of these institutions, are also highlighted.

15. SUBJECT TERMS

artificial intelligence (AI), machine learning (ML), AI/ML, offensive cyberoperations, counter-AI

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Ted Welsh, CSIAC Director
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	16	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

About DTIC and CSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense's (DoD's) annual multibillion-dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision-makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (IACs), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a DoD IAC sponsored by DTIC to provide expertise in four technical focus areas: cybersecurity; knowledge management & information sharing; modeling & simulation; and software data & analysis. CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

A chief service of the DoD IACs is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry jointly conducted by CSIAC.

Abstract

The Cybersecurity & Information Systems Information Analysis Center performed open-source research and obtained white papers and reports from numerous sources to include the Defense Technical Information Center Research and Engineering Gateway and Elsevier's ScienceDirect. Overall, the research shows that the best way to counter artificial intelligence (AI) offensive tools is with AI defensive tools. The resulting research is described in detail. This TI response report is organized into three distinct sections: (1) completed cyber-AI research, (2) current market studies, and (3) cyber-AI centers. The first section discusses completed cyber-AI research, with reports and perspectives detailing the importance of AI in cybersecurity. Next, this report details current market research and studies. The top defensive and offensive tools and capabilities are mentioned, along with forecasts and statistics on current and future cyber-AI investments. Finally, two institutions specifically created for the study of cyber-AI are identified. The respective missions, along with current work of these institutions, are also highlighted.

Contents

1.0 TI Request

1.1 Inquiry

What is the state of industry investment in and development of products in support of counter-artificial intelligence (AI) offensive tools and techniques?

1.2 Description

The objective for the information is to help the inquiring organization determine what types of tools and techniques are currently available, as well as what counter-AI investments are being made and in what areas. Current U.S. efforts and products are of primary interest.

2.0 TI Response

This report summarizes the research findings of the inquiry. Given the limited duration of the research effort, this report is primarily a curated summary of sources and information, analyzed by our researchers, pertaining to counter-AI cyberoffensive tools and techniques. Section 2.1 begins by highlighting research that has already been completed in cyber-AI research to date.

2.1 Completed Cyber-AI Research

Notable research has been completed in the field of cyber-AI regarding its weaponization, how to defend against it, and implications on how the United States can use AI offensively and defend itself moving forward. Research indicates that AI is being weaponized against U.S. military, government, and public citizens through surveillance, coercion, and the AI weapons factory. AI is also being used to tamper with technology in a dangerous manner through things such as autonomous vehicles, medical documents, and traffic signals. Defending against cyber-AI attacks and utilizing AI have underlying complexities that lead to different methods when trying to mitigate, disrupt, recover from, or utilize AI weaponization.

The evolution and advancements of AI have brought to light new threats for the U.S. military, government, and private citizens. AI allows for a larger and less manageable rise in scale for surveillance. Adversaries can use that increased state of surveillance to coerce individuals or industries. Weaponized AI is also less trackable than physical munitions, making it harder to stop its production and distribution. Moreover, the integration of AI into everyday life increases susceptibility toward weaponized AI by making it more accessible to U.S. adversaries, as well as increasing the number of ways in which AI can be weaponized. Actions required to defend against weaponized AI attacks involve further research from academia including tools to help the United States deal with future attacks; stricter policies from industries on the use and management of AI; work toward legislation that will regulate the use of AI and how it is operated; and cooperation from private citizens, trusting them to not share information with adversaries.

The United States may face future threats from the evolution of AI. Focused on weaponized AI—used as a weapon, intentionally or otherwise—a report from Arizona State University titled “The New Dogs of War: The Future of Weaponized Artificial Intelligence” examines how next-generation threat actors could use AI and advanced machine learning (ML) techniques against the U.S. military, government, industry, and private citizens [1]. That report identifies three key threats (surveillance and coercion, the AI weapons factory, and the careless destabilization of national security), as well as actions necessary by academia, nonprofits, industry, government, and individuals to mitigate, disrupt, or recover from possible threats.

Defensive AI has gained international attention. The definition of defensive AI is discussed from the perspective of the defender and the adversary in “Defensive AI: the Future Is Yesterday” [2]. Opportunities exist to apply defensive AI to the foremost problems plaguing cyberspace. Defensive AI, or AI that is used to protect against cyberattacks, has been commonplace in society for a long time, with a good example being the facial recognition on cell phones. An increased risk of cyberattacks has brought greater attention to the use of defensive AI on a larger scale. There are two main roles that defensive AI needs to perform. The first being the real-time management of infrastructure-operating information. This AI must be able to transfer critical information safely and without slowing operations. The second role defensive AI must fulfill is the ability to trace where the cyberattack is originating. These capabilities will require an intelligent AI that has potential to be developed. Once AI such as this has been fully integrated, it could also identify the potential severity of an incoming attack, identify weaknesses and compromises in weapons systems, and aid in decision-making for the government [2].

As the development of AI rises, it will begin to increasingly define how future conflict in the cyber-realm will be executed. Implications of new weaponized AI indicate that it will increase the effectiveness of offensive cyberoperations while decreasing the effectiveness of U.S. defense capabilities. Moreover, the advancements of AI make powerful attacks more accessible to adversaries. AI-driven malware can use incoming data to make informed decisions on potential future infections and if it will create value. AI-driven malware will also be able to successfully monitor the speed and scale of its infections, leading to a decrease in detectability. The increase in available data to adversaries will also lead to a decrease in security. In addition, malware will be able to use a wide range of tools to optimize further spread, adjust its strategy of infection in real time, and decide an optimal strategy completely autonomously for each individual. These new threats can be utilized through input attacks that involve misleading AI systems to alter their efforts and poisoning attacks that mess with the programming of AI used in enemy systems. So far, the United States has employed the idea of persistent engagement for cybersecurity, which states that cybersecurity must constantly be utilized everywhere to be properly prepared for an attack. However, AI compromises this idea by decreasing the common knowledge among practitioners, making it much harder to properly defend against these attacks. AI of this caliber is also much less predictable, and its intent is much harder to identify, making persistent engagement less viable as it is impossible to prepare for the unpredictable.

The report “Problems of Poison: New Paradigms and ‘Agreed’ Competition in the Era of AI-Enabled Cyber Operations” takes on two primary tasks [3]. First, it considers and categorizes the primary ways in which AI technologies are likely to augment offensive cyberoperations, including the shape of cyberactivities designed to target AI systems. Then, it frames a discussion of implications for deterrence in cyberspace by referring to the policy of persistent engagement, agreed competition, and forward defense promulgated in 2018 by the United States. “Here, it is argued that the centrality of cyberspace to the deployment and operation of soon-to-be-ubiquitous AI systems implies new motivations for operation within the domain,” complicating numerous assumptions that underlie current approaches [3]. AI cyberoperations pose unique measurement issues for the policy regime.

The United States is currently in an arms race with other countries such as China and Russia to develop the best and most efficient AI for offense against adversaries and national security. Ideally, this desired AI would change the way military operations and national security protocols are run through management and efficient decision-making. On the offensive side, AI can be used for nuclear materials, toxins, chemical materials, and space. AI can also be integrated into the military to help with offensive procedures. However, the United States must use caution when proceeding with this AI integration as it can be easily manipulated and the effects would be catastrophic. Offensively, AI can also be used for data misclassification, synthetic data generation, and data analysis. These attacks can be audio based, visually based, or textually based, each presenting its own unique challenges. AI is also being developed for the autonomous use of combat vehicles in military operations. Defensively, these cyberattacks can be mitigated through regularization, gaining information on AI-model security threats, and antiphishing. Through these defense tactics, the effects of cyberattacks will be lessened.

A report titled "Weaponized AI for Cyber Attacks," concludes that [4]:

> AI-based technologies are actively used for the purposes of cyberdefense. With the passage of time and decreasing complexity in implementing AI-based solutions, the usage of AI-based technologies for offensive purposes has begun to appear worldwide. These attacks vary from tampering with medical images using adversarial ML for false identification of cancer to the generation of adversarial traffic signals for influencing the safety of autonomous vehicles.

The report also investigated "recent cyberattacks that utilize AI-based techniques" and identifies "various mitigation strategies that are helpful in handling such attacks." It further identifies "existing methods and techniques that are used in executing AI-based cyberattacks," along with "probable future scenarios that might be plausible to control such attacks" [4].

2.2 Current Market Studies

With this increase in AI usage and a larger attack surface due to the digitization of processes comes a new and advanced wave of cyberattacks that uses ML to bypass normal security protocols. Organizations and experts alike agree that human-led services for cybersecurity are no longer a viable option. However, the implementation of defensive AI for organizations comes with its own risks such as exploitations of compromises made within systems. Defensive AI will learn what is normal and detect and fight back against any abnormalities spotted. With an increase of adversaries has come an increase in tools used for defensive AI.

Top-priority targets for cyberattacks include power plants, hospitals, and financial service companies. The rise in AI creates new opportunities to help defend these entities from unwanted breaches in their security. Cybersecurity has five branches: (1) critical infrastructure security, (2) cloud security, (3) internet of things security, (4) application security, and (5) network security [5]. AI will soon be able to run these five branches and help mitigate compromises in security from attackers. Techniques used by attackers include malware infections, ransomware attacks, phishing attacks, and social engineering. AI software is already being used for cybersecurity. This includes Cybersecurity (CS) Tool Kit, Sophos Intercept X Tool, Vectra's Cognito, Tessian, International Business Machines Corporation (better known as IBM) QRadar Advisor, Targeted Attack Analytics by Symantec, bio-inspired hybrid artificial intelligence framework for cyber security (known as BioHAIFCS), StringSifter, Defplore X, and Vectra's Cognito Platform [5]. This software can be used for early spam and malware detection, as well as for connecting signals from disparate systems.

An article by Baraik notes [5]:

> AI can help...protect against spoof[ing] and sophisticated attacks done by cybercriminals. According to a global survey released by Pillsbury, an international law firm, 49% of its executives think AI is the best tool to counter nation-state cyberattacks. It also predicts that cybersecurity-related AI spending will increase at a [compound annual growth rate] CAGR of 24% through 2027 and reach a market value of $46 billion. Its applications include classification algorithms for early malware and spam detection, abnormality in malicious traffic or user behaviors, and correlation algorithms that connect signals from disparate systems.

Offensive AI poses a unique threat to organizations and gives an advantage to threat agents looking to harm organizations. These threat agents include cyberterrorists, cybercriminals, employees, hacktivists, nation-states, online social hackers, script kiddies, and other organizations looking for an advantage. These cyberattacks are often aimed to give an advantage such as money, information, or fame. These threats also prevent a significant concern to the organizations. AI-enabled cyberattacks can range from impersonation of high-ranking officials and spear phishing (using a higher-ranking official's face and voice) to activity tracking and cache mining, with the most prominent threats being reverse engineering, impersonation, and AI model theft. To defend against these cyberattacks, organizations must develop AI/ML, as well as begin to research and develop ML security operations. Organizations must also incorporate security testing, protection, and monitoring of their AI/ML models. This will enable them to safely and securely integrate AI into their everyday practices.

In "The Threat of Offensive AI to Organizations," the threat of offensive AI to organizations is explored [6]. The report first presents the background and then discusses "how AI changes the adversary's methods, strategies, goals, and overall attack model." It next identifies "through a literature review...33 offensive AI capabilities which adversaries can use to enhance their attacks." The report concludes, "through a user study spanning industry and academia...[by ranking] the AI threats and...[providing] insights on the adversaries" [6].

Cyberattacks have become commonplace in offices and organizations. With the uprising of AI-based attacks, human-led resources are no longer enough to counter these attacks. Over half of business executives around the globe have stated in a survey that human-led resources are failing and more sophisticated technologies are critical. Ninety-six percent of chief-level executives state that they have some sort of defensive AI in place to defend against the new and advanced waves of AI-enabled cyberattacks [7]. Static defense systems are unable to accommodate the rapidly changing nature of these new attacks. AI defense systems are dynamic in the sense that they can adapt to cyberattacks in real time and stop ransomware and malware in seconds. Defensive AI will learn what is “normal” for an organization and will detect any abnormalities and quickly stop them. Defensive AI will also work around the clock detecting threats to ensure organizations are always protected. Organizations have begun allocating more of their budget to information technology (IT) security, as well as IT, audits to quickly and effectively integrate AI into their security systems.

Based on a combination of survey-based market research and in-depth executive interviews, a report titled “Preparing for AI-enabled cyberattacks” explores organizations’ biggest cybersecurity concerns and how they are adopting AI in preparation to find and repel AI-enabled cyberattacks [7]. The report is sponsored by Darktrace, and the views expressed within are those of MIT Technology Review Insights, which is editorially independent.

As organizations become more digitized, the “attack surface” for AI-driven cyberattacks will also increase. Seventy-nine percent of firms say that there has been an increase in cyberattacks in the past 5 years. Eighty-six percent of those say that the volume of advanced security threats has increased drastically in the same amount of time. On average, it takes a human-led service over 3 hours to respond to a high-level security threat, and even longer to return to business as normal. With this increase in digitization, organizations must employ defensive AI to identify and eradicate advanced security threats in minutes. Defensive AI adds a layer of security for organizations that would be impossible for a human to provide. Offensive AI is on the rise, and organizations need to put appropriate defenses in place if they are to fend off attacks [8].

The current best response to advanced cyberattacks is the implementation of defensive AI/ML. However, defensive AI/ML brings a plethora of new and unique challenges. It works by learning what is normal for a company or organization and identifying and eliminating any abnormalities. If an adversary were to learn what is normal for a company, it would easily be able to bypass the defensive AI/ML and successfully attack the organization. Organizations can account for this by teaching the AI/ML to look for more specific and advanced threats with the trade-off of losing accuracy. Organizations must be able to balance this trade-off to avoid cyberattacks. Many organizations have multiple AI/ML in place to account for inaccuracies that may occur, as adversaries will often exploit compromises that organizations make. To be successful against adversaries, there are policies and strategies that an organization must follow as detailed in “Making AI Work for Cyber Defense” by Wyatt Hoffman [9]:

- Build security into the process of ML design and development
- Promote resilience through system diversity and redundancy
- Manage the risk that cuts across the ML and cybersecurity ecosystem
- Counter strategic rivals' attempts to compromise and sabotage ML development

According to Hoffman [9]:

> Cyberthreats are multiplying and escalating. AI could exacerbate the problem or be part of the solution. Innovations in ML methodologies have already proven their usefulness for cybersecurity. But can ML-enabled defenses deployed at scale contend with adaptive attackers? To level the playing field for defenders, ML must be able to perform reliably under sustained pressure from offensive campaigns—without constant human supervision.

2.3 Cyber-AI Centers

Some cyber-AI research centers are dedicated to researching defense against the rise in AI-based cyberattacks. While these research centers are relatively new, they have a grasp on the danger that AI presents and the unpreparedness of the United States to defend against such attacks. Their main goal is to help provide research to officials and the public on how to best defend against these attacks so the United States can maintain national security.

The Darktrace Cyber AI Research Centre is dedicated to the application of AI to solve real-world problems. With 130 patents and 200 research and development employees holding 100 master's degree and 20 doctorates, the Darktrace Cyber AI Research Centre has been able to make numerous award-winning breakthroughs in AI capabilities [10]. It has also published many academic research papers such as "Innovating Cyber Recovery—Key to Cyber Resilience: The Dynamic, Real-Time Approach to Recovering From Cyber Disruption" [11] and "Darktrace Attack Path Modeling: Utilizing Graph Theory to Derive Multi-Domain, Risk-Prioritized Attack Paths Within Computer Networks" [12], as well as research on defensive AI capabilities.

The Offensive AI Research Lab was founded in 2020 for the purpose of working on ways to give the advantage to the defender of a cyber-AI attack. It provides research that will help prepare for the rapid emergence of offensive AI in the coming years. The Offensive AI Research Lab is against the idea of AI causing physical, financial, or psychological harm, which is why its mission is to identify, counter, and mitigate the rising threat of offensive AI [13].

References

[1] Johnson, B. D., N Vanatta, A. Draudt, and J. R. West. "The New Dogs of War: The Future of Weaponized Artificial Intelligence." Arizona State University—Tempe, Tempe, AZ, September 2017.

[2] Michael, J. B., and T. C. Wingfield. "Defensive AI: the Future Is Yesterday." *Computer,* vol. 54, issue 9, 27 August 2021.

[3] Whyte, C. "Problems of Poison: New Paradigms and 'Agreed' Competition in the Era of AI-Enabled Cyber Operations." 2020 12th International Conference on Cyber Conflict (CyCon), Estonia, pp. 215–232, May 2020.

[4] Yamin, M. M., M. Ullah, H. Ullah, and B. Katt. "Weaponized AI for Cyber Attacks." *Journal of Information Security and Applications,* vol. 57, March 2021.

[5] Baraik, P. "Top Artificial Intelligence-Based Tools for Cyber Security" *Marktechpost,* https://www.marktechpost.com/2022/08/11/top-artificial-intelligence-based-tools-for-cyber-security/, 11 August 2022.

[6] Mirsky, Y., A. Demontis, J. Kotak, R. Shankar, D. Gelei, L. Yang, X. Zhang, W. Lee, Y. Elovici, and B. Biggio. "The Threat of Offensive AI to Organizations." *ACM Computing Surveys*, vol. 1, no. 1, July 2021.

[7] MIT Technology Review Insights, Darktrace. "Preparing for AI-Enabled Cyberattacks." *The MIT Technology Review,* 8 April 2021.

[8] Vogel, S. "What Is Offensive AI and How Do You Protect Against It?" *IT Pro,* https://www.itpro.com/security/cyber-security/359302/what-is-offensive-ai-and-how-do-you-protect-against-it, 22 April 2021.

[9] Hoffman, W. "Making AI Work for Cyber Defense." Center for Security and Emerging Technology, Georgetown University, Washington, DC, December 2021.

[10] Darktrace Holdings Limited. "Darktrace Cyber AI Research Centre." *Darktrace,* https://darktrace.com/research, accessed 22 June 2023.

[11] Allen, J. “Innovating Cyber Recovery—Key to Cyber Resilience: The Dynamic, Real-Time Approach to Recovering From Cyber Distribution.” *Darktrace,* https://darktrace.com/research/innovating-cyber-recovery-key-to-cyber-resilience, 16 December 2022.

[12] Darktrace Holdings Limited. “Darktrace Attack Path Modeling: Utilizing Graph Theory to Derive Multi-Domain, Risk-Prioritized Attack Paths Within Computer Networks.” *Darktrace,* https://darktrace.com/research/attack-path-modeling-research, 23 February 2022.

[13] Offensive AI Research Lab. “What Is Offensive AI?” *Offensive AI Lab,* https://offensive-ai-lab.github.io/about/, accessed 22 June 2023.

Biographies

Philip Payne is the Cybersecurity & Information Systems Information Analysis Center (CSIAC) technical lead. Mr. Payne (certified information systems security professional and Security+ certified) comes from a rich background in cybersecurity with the Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance Center (C5ISR) (formerly the Communications-Electronics Research, Development, and Engineering Center) and possesses a Bachelor of Science and Master of Science in computer engineering from Johns Hopkins University and Polytechnic University, respectively. At the C5ISR Center, he led a world-class cross domain solution (CDS) laboratory. Within the lab, he performed CDS lab-based security assessments on U.S. Army CDSs going through secret and below interoperability CDS certification and accreditation approval process. He was a key member of the Information Security Branch, which has made a myriad of contributions in cyberspace for the U.S. Department of Defense at large. At SURVICE Engineering, he served as a vital member of the Cyber Research and Development Team as senior cybersecurity engineer, supporting the Data Analysis Center (formerly the U.S. Army Materiel Systems Analysis Activity) on early acquisition cybersecurity assessments for Army systems.

Matthew Friar works with the CSIAC team as a research inquiry analyst. He recently graduated from Stevenson University, acquiring a Bachelor of Science in computer information systems, with a specialization in software design. At Stevenson, he was a member of the Leadership Scholars Program and was an active participant in technology-related events on campus. At SURVICE Engineering, Matthew performs in-depth research relating to technology fields such as cybersecurity and information systems. He also works with government clients to provide them with information-oriented solutions and answer their technical inquiries.

Curtis Smedley is an Intern at SURVICE Engineering tasked with supporting Homeland Defense & Security Information Analysis Center, CSIAC, and Defense Systems Information Analysis Center analysts with research, formatting, and summarization. Curtis is also working with the CSIAC department to edit and organize databases. He is currently a mechanical engineering student at the University of Maryland, College Park, and is planning to graduate in 2025. At his college, Curtis helps aid new students through his teacher’s assistant position for entry-level physics courses including general physics, mechanics, and particle dynamics.