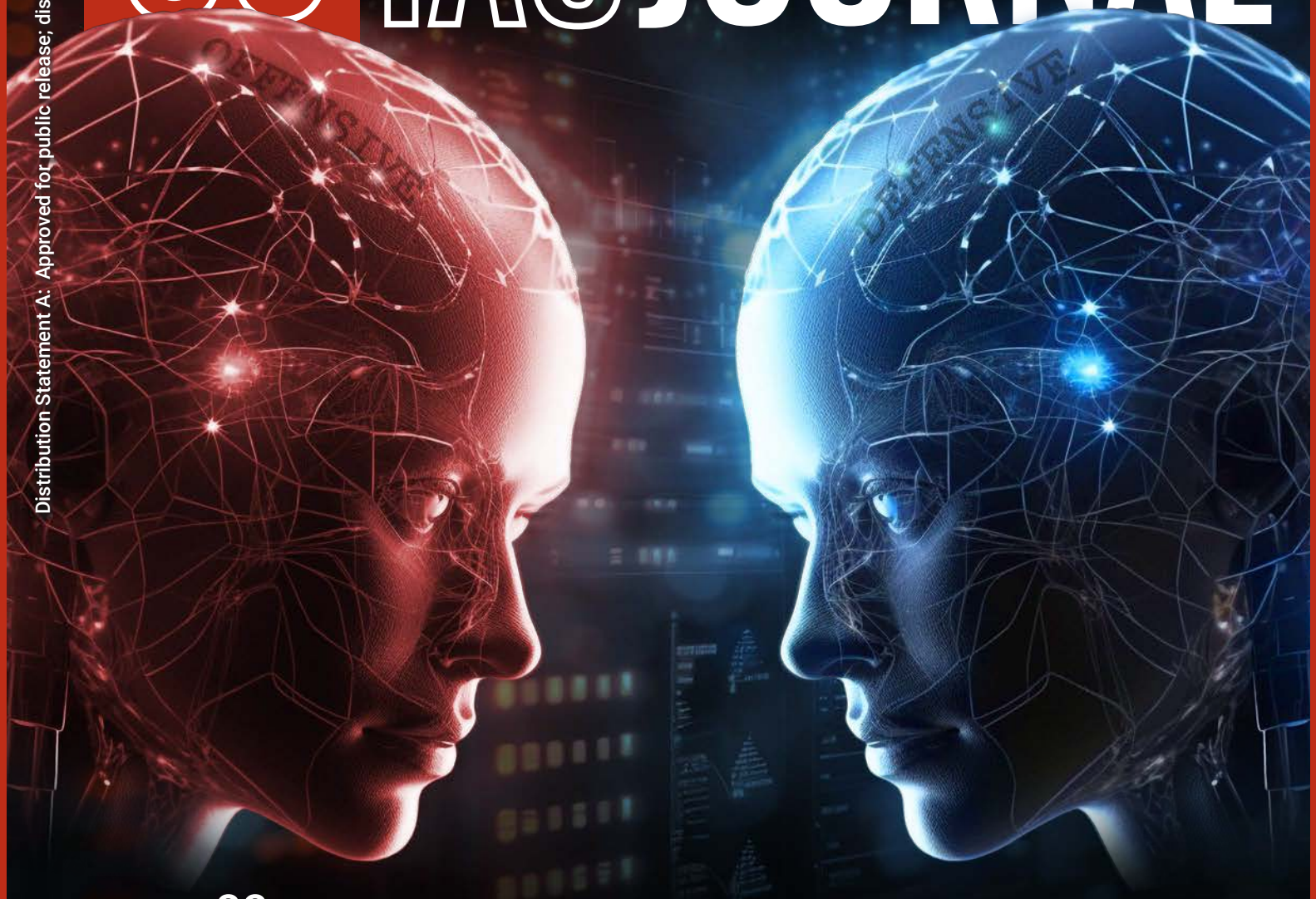
2024

CS IAC JOURNAL



PAGE 22

ARTIFICIAL INTELLIGENCE

AS A FORCE MULTIPLIER IN U.S. MILITARY INFORMATION CAMPAIGNS

SPECIAL AI/ML EDITION

CSIAC JOURNAL

Special Edition // AI/ML // 2024

Editor-in-Chief:
Aaron Hodges

Sr. Technical Editor:
Maria Brady

Graphic Designers:
Melissa Gestido, Katie Ogorzalek

The CSIAC Journal is a publication of the Cybersecurity & Information Systems Information Analysis Center (CSIAC). CSIAC is a DoD Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) with policy oversight provided by the Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E). CSIAC is operated by the SURVICE Engineering Company.

ISSN 2836-7383 (Print) // ISSN 2836-7391 (Online)

Distribution Statement A:
Approved for public release; distribution is unlimited.

On the Cover:
Digital Art Rendering *(Source: tongpatong32 and zinetron [123rf.com]).*

CSIAC Cybersecurity & Information Systems Information Analysis Center

ABOUT CSIAC

Who We Are

A DoD Information Analysis Center comprised of scientists, engineers, researchers, analysts, and information specialists.

What We Do

Generate, collect, research, analyze, synthesize, and disseminate scientific and technical information (STI) to DoD and federal government users and industry contractors.

Why Our Services

To eliminate redundancy, foster collaboration, and stimulate innovation.

CSIAC SERVICES

Subject Matter Expert (SME) Connections

Access to a network of experts with expertise across our technical focus areas.

Technical Inquiries (TIs)

Up to 4 hours of FREE research using vast DoD information resources and our extensive network of SMEs.

Specialized Task Orders

Research and analysis services to solve our customer's toughest scientific and technical problems.

Webinars & Events

Our webinars feature a technical presentation from a SME in one of our focus areas. We also offer key technical conferences and forums for the science and technology community.

STI Collection

Our knowledge management team collects and uploads all pertinent STI into DTIC's Research & Engineering Gateway.

Information Research Products

The Cybersecurity & Information Systems Digest, state-of-the-art reports, journals, TI response reports, and more available on our website.

CONTACT CSIAC

IAC Program Management Office

8725 John J. Kingman Road
Fort Belvoir, VA 22060
Office: 571.448.9753

CSIAC Headquarters

4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600
Fax: 410.272.6763
Email: contact@csiac.org

CSIAC Technical Project Lead

Phil Payne
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600

FEATURED ARTICLE

ARTIFICIAL INTELLIGENCE AS A FORCE MULTIPLIER IN U.S. MILITARY INFORMATION CAMPAIGNS

Aaron Sweeney, Danyl Miller, Joseph Vossler, Edward Olbrych, Jacob Strahan, Gerald Mazur, and Andre Slonopas

Military commanders have used information throughout warfare to influence, mislead, disrupt, or otherwise affect the enemy's decision-making and capabilities. This article discusses the history of information operations (IOs) and enduring importance of incorporating actions in the information environment in military strategy.

IN THIS ISSUE

SPECIAL AI/ML EDITION

NOTE FROM THE EDITOR-IN-CHIEF

BY AARON HODGES

Artificial intelligence (AI) and machine learning (ML) represent an increasingly exciting field of computer science. A term originally coined by John McCarthy in 1956,[1] AI is becoming increasingly pervasive in today's world. From internet search engines to applicant tracking software, humanity's interaction with AI/ML intersects in complex and oftentimes unforeseen ways. For the men and women of the U.S. Department of Defense (DoD), this complex relationship is increasingly magnified by the problem sets we face, the solutions we seek, and the missions we perform.

Four years ago, DoD leadership recognized the limitless potential of AI/ML while acknowledging the need to establish ethical guardrails to contain wanton development of weaponized AI/ML systems. Addressing existing ethical ambiguities and future risks associated with AI use in defense applications, former Secretary of Defense Dr. Mark T. Esper accepted the Defense Innovation Board's recommendations on ethical principles governing AI/ML development and application. Focusing on five core principles, the DoD requires that AI/ML capabilities developed for defense applications be responsible, equitable, traceable, reliable, and governable. Uniting new frontiers with the United States' unwavering values, these principles ensure AI/ML development remains responsive to the needs of the country and its allies while remaining aligned with the DoD's existing ethical framework and legal obligations.[2]

The articles in this special issue of the CSIAC Journal represent a small portion of the research and evaluation and real-world employment of AI/ML capabilities with defense applications. Our contributors focused on AI/ML's linkage to several defense-related needs, including cybersecurity, knowledge management and information sharing, and modeling and simulation (M&S). In our featured article "Artificial Intelligence (AI) as a Force Multiplier in U.S. Military Information Campaigns," Aaron Sweeney and his team of coauthors from the Virginia National Guard explore the use of AI to assist Warfighters in planning, executing, and evaluating military information operations. Tracing the history of

> ***The articles in this special issue of the CSIAC Journal represent a small portion of the research and evaluation and real-world employment of AI/ML capabilities with defense applications.***

[1] BBVA OpenMind. "The True Father of Artificial Intelligence." https://www.bbvaopenmind.com/en/technology/artificial-intelligence/the-true-father-of-artificial-intelligence/, accessed on 29 May 2024.

[2] U.S. DoD. "DoD Adopts Ethical Principles for Artificial Intelligence." https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/, accessed on 29 May 2024.

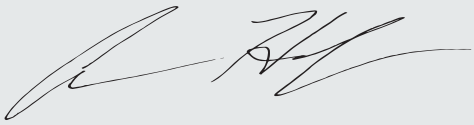
information operations from Sun Tzu onward to the modern wargaming environment of Cyber Fortress, they explore how AI systems can aggregate data sources to both generate content and disseminate false narratives and detect and counter an adversary's use of these techniques.

With a focus on M&S, U.S. Army Major David Niblick and Dr. David Bauer from the Army Evaluation Center present a case study and recommendations for developing small-scale AI solutions in "Development, Test, and Evaluation of Small-Scale Artificial Intelligence Models." Using a model that automates an acoustic trilateration system, they highlight how even a small number of neural-networked acoustic sensors can create data sets that require extensive knowledge to interpret and understand. Also related to M&S but with a cybersecurity focus, Dr. Corren McCoy and her team of researchers from Old Dominion University and the Virginia Modeling Analysis and Simulation Center outline a framework for vulnerability management. This framework provides a personalized, rank-structured approach to mitigating cyber vulnerabilities that offers significant improvement over the generalized Common Vulnerability Scoring System.

Finally, Dr. Anthony Rhem provides a pragmatic approach to using AI/ML in knowledge management and information-sharing operations. Advocating for quality data and the ethical use of AI/ML systems, he creates an ethically grounded, AI/ML-enabled framework leaders can use to assess the health of their organizations.

As our contributors have demonstrated, the future of AI and ML is now! Scientific curiosity and human intuition have brought us to the dawn of a promising future in which collecting, analyzing, and aggregating digitized data play an important role in defense operations. The applications for AI/ML are vast, and the contributions are limitless. As I close this letter, I look forward to witnessing how the DoD and its partners in industry and academia can harness the power of AI/ML while remaining true to the spirit of American ideals. ■

Sincerely,



Development, Test, and Evaluation of

SMALL-SCALE ARTIFICIAL INTELLIGENCE MODELS

BY DAVID K. NIBLICK AND DAVID A. BAUER (PHOTO SOURCE: BLUEXHAND [CANVA])

SUMMARY

As data becomes more commoditized across all echelons of the U.S. Department of Defense, developing artificial intelligence/machine-learning (AI/ML) solutions allows for advanced data analysis and processing. However, these solutions require intimate knowledge of the relevant data as well as robust test and evaluation (T&E) procedures to ensure performance and trustworthiness. This article presents a case study and recommendations for developing and evaluating small-scale AI solutions. The model automates an acoustic event location system.

First, the system identifies events across acoustic sensors using an algorithm trained via ML. It then corresponds the events through a heuristic matching process that uses the correspondences and difference of times to multilaterate a physical location. Even a relatively simple dataset requires extensive understanding at all phases of the process. The T&E metrics and pipeline require unique approaches to account for the AI solution, which lacks traceability and explainability. As leaders leverage the growing availability of AI tools to solve problems within their organizations, strong data analysis skills must remain at the core of the process.

INTRODUCTION

Like many organizations, the U.S. Army Test and Evaluation Command (ATEC) creates and archives massive amounts of data. Combined with modern advances in analytics, this data has potential to revolutionize business practices. However, the process of identifying useful datasets, developing a model, and then deploying the model safely and responsibly is complex. Though advances of ML and deep-learning models have made great strides in recent years, they are not feasible without a deep understanding of the data upon which they are built.

This article explores using data from an acoustic-based multilateration system to automate what is currently a tedious, labor-intensive process. In a multilateration system, a minimum of three sensors is used to locate an object in space and time by calculating the time differences between the sensors. For the case study, a single test consists of capturing explosive events across a set of 6 to 12 audio channels covering tens of seconds of time, along with metadata about sensor locations, weather station data, and, optionally, the results of preprocessing and manual processing of the data. Engineers manually identify and label the events in each channel. Each audio channel is from a different physical sensor. An example dataset from a single test is shown in Figure 1.

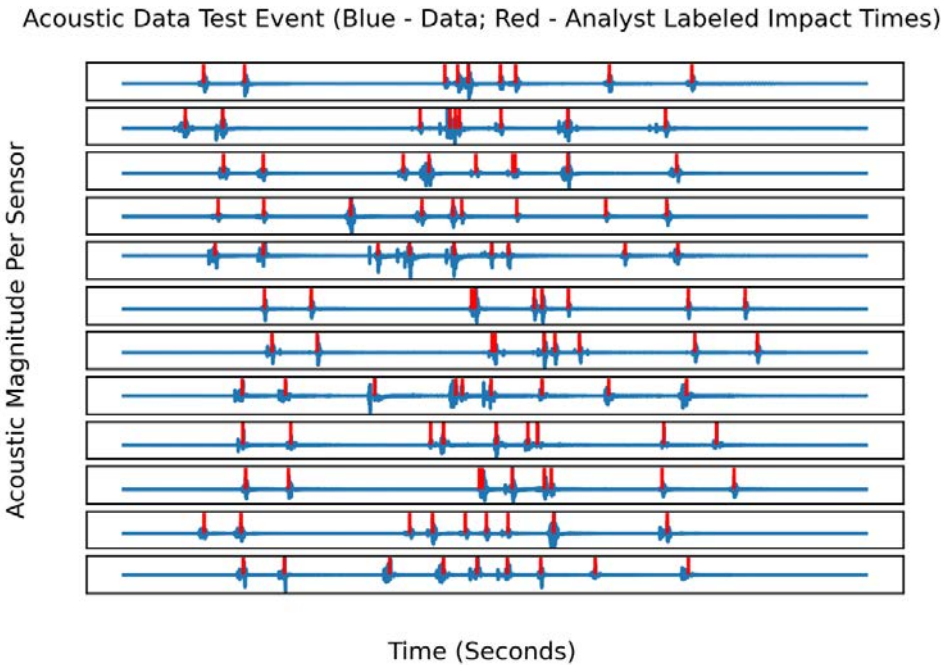


Figure 1. Multilateration Dataset Sample: Blue Lines Depict Acoustic Signals Across 12 Sensors, and Red Dashes Depict Manually Determined Event Labels *(Source: D. Niblick and D. Bauer)*.

Using the multilateration problem as a case study, an architecture is proposed for small teams to develop AI/ML tools to benefit their organizations. Critical steps are illustrated to maximize the chance of success or identify when success is not yet feasible. Teams must become deeply knowledgeable on the data, focus on a useful solution as opposed to fixating on a particular tool, and integrate a requirements-based approached for T&E early in the process. These threads are chronologically separated into a preparation phase, a development phase, and the T&E phase. The phases are broken into subsections based on recommendations and how they apply to this case study.

PREPARATION

Prior to beginning solution development, teams should assess return on investment (ROI), develop solution requirements with customers, and execute minimal viable experiments (MVEs).

Recommendations

Before committing resources to solve a problem, teams need to deliberately assess the feasibility of a solution and ROI. First steps include assessing the difficulty of the problem, identifying if similar problems have already been solved, analyzing the quality and quantity of the data available, and ensuring relevant expertise exists within the team. There are many ways to quantitatively assess an ROI. However, when making a predictive or automation-based tool, the team must seriously consider the overall process that this tool supports by asking the following questions:

Will users trust it and want to use it?

What speed and accuracy are necessary to increase capacity or efficiency?

Are there safety and ethical considerations that increase the threshold for success?

Many of these nontechnical factors will significantly impact the process and, therefore, the investment required to create a valuable tool.

As soon as possible, the team must interface heavily with the end user to develop a set of preliminary requirements. Requirement development is an iterative process—at the very least, the team and end user must determine some key performance parameters that, if met, will improve the end user's overall process. These requirements should include prime metrics like accuracy and speed, as well as inputs and outputs between the tool and other software, user interface needs, environments the tool must operate in, cybersecurity, etc., and using quantitative and qualitative metrics.

Before committing resources to full development, the team should execute one or more MVEs. The goal is to isolate the problem into simple terms and see if a solution that achieves a low threshold of success can be quickly built. Although the threshold can change depending on the problem, often even proving a preliminary model does better than "random" is enough to show that the model can learn from the data. The purpose is to determine whether a solution is feasible, identify any aspects not previously considered, refine the requirements, and develop a T&E methodology. Data preparation is critical here, but teams should emphasize speed on a subset of data. During the MVEs, it is helpful to try multiple off-the-shelf models/approaches. The knowledge gained here will benefit development. Additionally, to ensure that the MVEs are successful and justify committing resources to development, a T&E methodology must be established. While this does not need to be perfect,

> ***To ensure that the MVEs are successful and justify committing resources to development, a T&E methodology must be established.***

it should integrate T&E into the overall development cycle.

Application to the Multilateration Problem

In the case of the acoustic multilateration tool, there was a significant ROI after interfacing with the end user. The current process included manually identifying the exact timing of bursts in the acoustic channels. The system vendor's proprietary software automatically scanned the audio data for events but produced numerous false positives. Analysts then went through a lengthy process of moving, deleting, and adding labels to the audio channels. They frequently switched between visual/auditory analysis of individual channels and adjustments to get the best overall solution fit. The tedious label-editing process implements an optimization operation but without the benefits of an optimization algorithm and modern computational capability. Given the frequency of tests that use this system, hundreds of analyst hours were spent on this "cleaning" process every month, so any time savings would have significant impact.

At first glance, the problem appeared relatively easy. The team had access to sufficient quality of labeled data, and multilateration is generally considered a solved problem. The requirement described by the end user was a localization accuracy of 10 m. Speed of application was trivial, as test results already take weeks to finalize. The acoustic multilateration tool operated in a semicontrolled environment. The location was consistent and isolated, and there was flexibility to avoid significant weather events. Identifying the "events" involved separating loud explosions vs. background noise. The difficulty of the multilateration problem existed in not just identifying the explosion but consistently selecting the same moment of time across all explosion detections. Because the explosions are close together in time relative to their separation in space, their shockwaves arrive at the sensors in different orders. This is a major driver of the problem's complexity.

An MVE was executed to accurately identify and localize the events within the audio. The goal was to find at least 50 percent of the events with a 75 percent recall accuracy. The average time needed to be within 30 ms. During the MVE, a minimal amount of data preparation was conducted, including some manual relabelling on acoustic streams. Accepting risk on the event correlation was decided, as that was expected to be the "easier" phase. In retrospect, this assumption was false. Ultimately, the MVE was a success, and many eccentricities in the data were discovered that affected future algorithm development.

As an example of these eccentricities, the labels were found to be much more inaccurate than initially assumed. Events were generally labeled across all audio channels when each sensor would have been expected to hear the event. However, in many cases, an audio channel did not actually capture the event or the audio was distorted. This caused labels that appeared obviously wrong for their specific audio channel. In addition to lowering the accuracy of ML algorithms that depend on accurate labels, the seemingly bad labels caused trust issues, which hampered development. The team manually labeled or relabeled some of the sample data as part of working around the concerns with the existing labels.

A learning point for the team was to be more careful when accepting risk on portions of the problem. The event correlation task proved much more difficult than anticipated. Additionally, the 30-ms time accuracy target corresponded with a 10-m average error only under otherwise perfect conditions, which was not the case here. Had a second MVE been conducted that focused on proving

out potential solutions for event correlation, the issues would have been discovered much earlier in the process and saved much effort during the development phase. Thus, it is important to identify the significant components of the tool during MVE and experiment on each component.

SOLUTION DEVELOPMENT

The development process for the multilateration problem iterated through multiple approaches, both for the event-detection and event-matching problems.

Recommendations

The development stage will depend greatly on the problem, the team, and the tools available. In cases like this case study where there was no obvious single approach, the team will need to decide how to allocate time between breadth and depth in exploring options and try to look at the problem from different viewpoints throughout the development process. They may need to incorporate an aspect of a different method or even change the solution approach entirely midway through the project. Similarly, the teams are encouraged to spend more time exploring and verifying data before beginning but be prepared to adapt to surprises at any point in development.

Application to the Multilateration Problem

In parallel to cleaning the data, the team began developing the technical solution through sessions of exploratory analysis and brainstorming. The acoustic multilateration problem was initially addressed as two independent tasks. The first task was to detect signals from events in the audio data. The second was to match up the detections to find the location and time of the events. The multilateration calculation itself was a basic least-squares fit. Alternatives like orthogonal regression [1] were investigated, but efficiency of the least-squares routine used prevailed.

The team began with the assumption that a deep neural network (DNN) would be the best algorithm to detect audio signals. A variety of networks was trained using real data with basic data augmentation. A substantial amount of effort was put into testing DNN architectures and training options in what turned out to be a case of premature optimization. The best DNN models were the ones that had been fine-tuned on the subset of data relabeled by the development team. A parallel effort tested a simpler method of signal detection using a combination of filtering and thresholding. Both methods worked well for clear, unambiguous signals, but both had trouble with noisy audio tracks and overlapping signals.

The best DNN models were the ones that had been fine-tuned on the subset of data relabeled by the development team.

The final solution to the audio detection discarded the DNN in favor of a simpler, hybrid AI/ML approach. A set of building blocks (e.g., filters, time-domain peak detection, and thresholding) was provided to a genetic algorithm, which produced better-performing detection algorithms than both prior manual efforts and the DNNs. The training data was insufficient in both quality and quantity to train a superior DNN. By providing building blocks—which were determined based on a series of hand-crafted algorithms—the team effectively reverted to an older style of feature engineering. By having far fewer parameters, overfitting the limited training data was avoided.

For the task of matching up detections to determine events, this problem was initially approached as a literal matching problem to solve with integer programming methods. Most of the algorithm work on this task was done using synthetic data, which avoided data quality issues. Early on, it was found that common methods like simulated annealing [2] could consistently solve the matching

problem if the set of detections was nearly complete and with very few false positives or false negatives.

Later, the second task was reframed as a continuous optimization problem, which allowed for a much wider variety of algorithms to be used. A variety of algorithms was tested from the SciPy [3], pymoo [4], and pySOT [5] libraries. The best results came from the SciPy package's DIRECT algorithm [6]. However, none of the optimization algorithms tested could directly solve the entire matching problem under noisy conditions. Instead, the optimizer was used to solve a smaller problem—the set of audio detections which corresponded to a single explosion event. The optimizer became a building block of a larger, heuristic algorithm that determined the sets of audio detections for all events.

Throughout the development process, focus iterated back and forth between the two tasks. It was clear early on that a better solution for the first task made the second task much more accurate. However, what level is possible is still unknown. During development, finding false solution sets with lower residual error than the real solution was possible. The existing manual process is also subject to false solution fits but was not tested. Fear of overfitting also prevented the team from pursuing an algorithm that adjusted labels based on feedback from the event-matching task, as done in the manual process.

T&E

A general framework to conduct T&E for AI/ML solutions should emphasize the role of data, consider conditions and environments, and evaluate risk.

Recommendations

Conducting T&E for AI/ML solutions, even for small-scale solutions, is notoriously difficult and often intractable. AI/ML solutions often exhibit black-box qualities and lack traceability and explainability [7]. It is recommended a portion of the team focus on developing T&E tools and methodologies in parallel to and integrated with the development team. The T&E team should focus not only on quantitative aspects like accuracy but also on how the tool will interface into the overall pipeline, how to ensure end-user trust, etc.

Just as data was central to preparation and development, it is once again central to T&E. The T&E team must be just as knowledgeable on the data as the development team. The team must understand the nuances to the following questions: Does your data represent future operational conditions? Is your data not only balanced in class but in environment and conditions?

When working with problems in the realm of AI, taking a requirements-based approach [8] through the lens of the relevant environment/conditions and communicated through capabilities, limitations, and risk is recommended. Simple metrics such as accuracy and recall are not sufficient for tools that operate under real-world conditions as part of a larger, complex process. Metrics and test design need to deeply consider environment, operational conditions, class balance, etc. The goal of T&E is to go beyond a "pass/fail" assessment and quantify and communicate in terms of environmental risks and end-user conditions. Users should understand in what circumstances their solutions are successful and what circumstances correlate to a higher level of risk. Communicating to the user about model performance risk broken out by conditions helps instill confidence and avoid model misuse.

Once the right metrics are selected, the T&E loop of plan, execute, evaluate, and refine must be as automated and

The goal of T&E is to go beyond a "pass/fail" assessment and quantify and communicate in terms of environmental risks and end user conditions.

fast as possible. Ideally, following a DevOps model, these tools are integrated to the extent that as soon as the development team updates the solution, they get real-time feedback on the results. Even if tools can be automated, overall T&E is not. The T&E team must understand where risk is involved through the overall pipeline. Does our tool introduce new risk and can that be mitigated somehow? The team must consider how the tool will eventually be used and evaluate against that. This can only be achieved through a "user IN the loop" mentality. To ensure that requirements development follows the customers' needs, it is recommended to collaborate with them early and often.

Application to the Multilateration Problem

For the multilateration tool, the team collaborated with the users to determine not only the requirements just discussed (such as average location error) but the environment and conditions in which this tool will be used. Metric selection was refined and experiments designed to closely track how the tool performs under different test conditions. When executing the plan, execute, evaluate, refine loop (shown in Figure 2) midway through the development process, it was discovered that the overall average model error was unacceptable. However, the median error was close to the requirement. Due to the refined experiments, the conditions which increased risk for error were elicited. Figures 3–5 show some of the results.

Based on these outcomes, the model failed requirements at air burst events but succeeded at ground burst events. Atmospheric conditions on days normally selected for tests have minimal impact to accuracy.

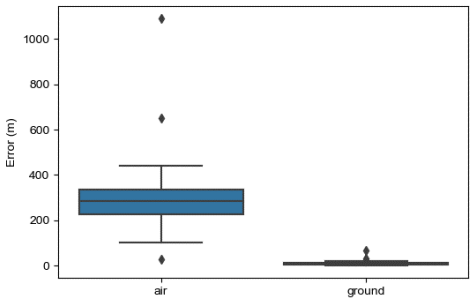


Figure 3. Box Plots Comparing Location Error of Air Burst to Ground Burst Events. A T-Test P-Value of 1.15e-16 Indicates a Strong Correlation of Error to Burst Elevation *(Source: D. Niblick and D. Bauer)*.

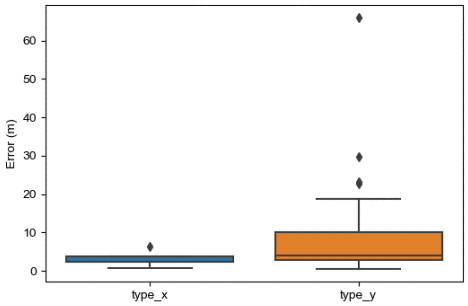


Figure 4. Box Plots Comparing Location Error of Different Munition Types (Ground Burst Only). A T-Test P-Value of 0.28 Indicates Possible Increased Risk of Error With Type Y Munitions *(Source: D. Niblick and D. Bauer)*.

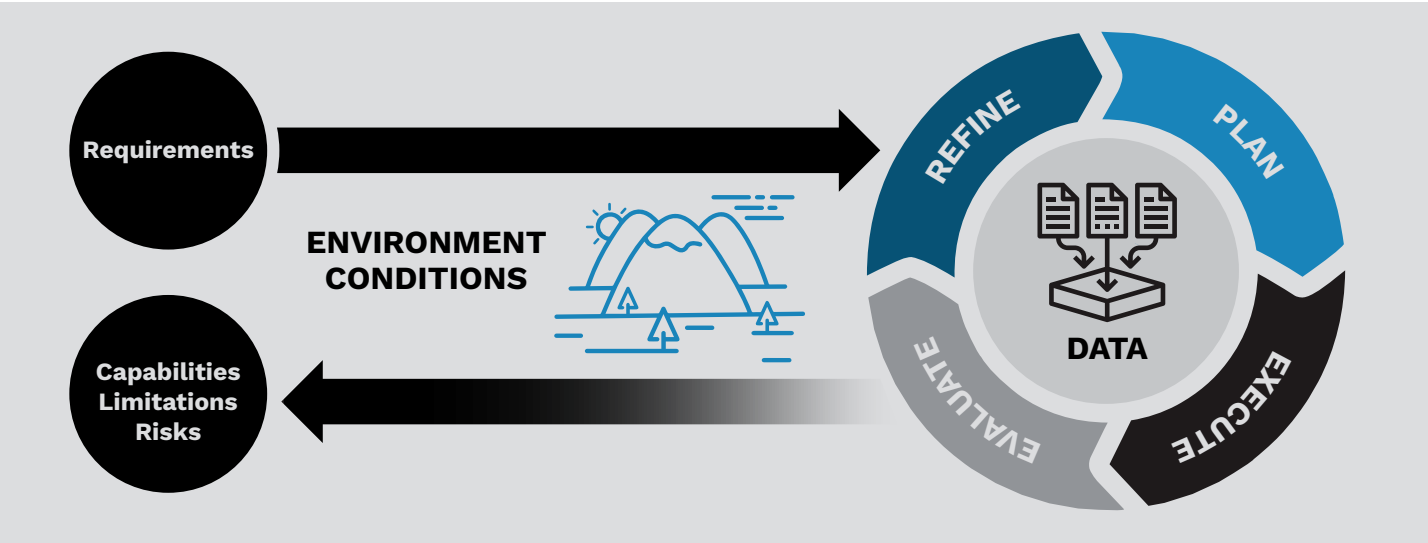


Figure 2. The Plan, Executive, Evaluate, and Refine Loop *(Source: D. Niblick and D. Bauer)*.

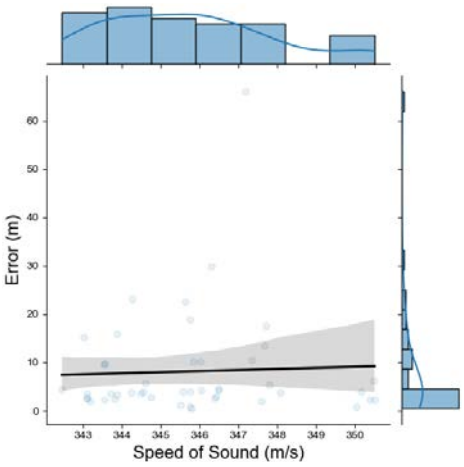


Figure 5. Analysis on Impact of Weather Conditions (Measured as Impact on Speed of Sound) to Model Location Error. The Result Is a Pearson P-Value of 0.78, Which Indicates Insignificant Impact *(Source: D. Niblick and D. Bauer)*.

Though both munition types met the requirement, there was increased risk when using the tool for Type Y munitions. After communicating these results and nuances to the end user, the team discovered a tool successfully multilaterating ground bursts provided significant ROI to their process, and they acknowledged the ongoing work on air-burst multilateration.

CONCLUSIONS

There is incredible potential to leverage analytic and AI/ML tools developed by small, in-house teams to solve business problems. However, teams must take a data-centric approach that heavily considers end-user requirements. They must become deeply knowledgeable on the data, focus on a useful solution as opposed to fixating on a particular tool, and integrate a requirements-based approached for T&E early in the process. Although this does not assure the successful deployment of a tool, it minimizes risk in wasted resources by identifying obstacles early and often. ■

REFERENCES

[1] Boggs, P. T., and J. E. Rogers. "Orthogonal Distance Regression" in "Statistical Analysis of Measurement Error Models and Applications: Proceedings of the AMS-IMS-SIAM Joint Summer Research Conference held 10–16 June 1989." *Contemporary Mathematics*, vol. 112, 1990.

[2] Tsallis, C., and D. A. Stariolo. "Generalized Simulated Annealing." *Physica A: Statistical Mechanics and Its Applications*, vol. 233, issues 1–2, 1996.

[3] Virtanen, P., et. al. "SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python." *Nature Methods*, vol. 17, no. 3, pp. 261-272, 2020.

[4] Blank, J., and K. Deb. "Pymoo: Multi-Objective Optimization in Python." *IEEE Access*, vol. 8, pp. 89497–89509, 2020.

[5] Eriksson, D., D. Bindel, and C. Shoemaker. "Surrogate Optimization Toolbox (pySOT)." github.com/dme65/pySOT, 2015.

[6] Jones, D. R., C. D. Perttunen, and B. E. Stuckman. "Lipschitzian Optimization Without the Lipschitz Constant." *J. Optim. Theory Appl.*, vol. 79, pp. 157–181, 1993.

[7] Rudin, C., and J. Radin. "Why Are We Using Black Box Models in AI When We Don't Need To?" Harvard Data Science Review, https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8, accessed on 28 February 2024.

[8] Whalen, M. W., et al. "Coverage Metrics for Requirements-Based Testing." Proceedings of the 2006 International Symposium on Software Testing and Analysis, 2006.

BIOGRAPHIES

DAVID NIBLICK is an artificial intelligence evaluator with ATEC at Aberdeen Proving Ground (APG), MD. He served in the Engineer Branch as a lieutenant and captain at Fort Campbell, KY, with the 101st Airborne Division (Air Assault) and at Schofield Barracks, HI, with the 130th Engineer Brigade. He deployed twice to Afghanistan and the Republic of Korea. He instructed in the Department of Electrical Engineering and Computer Science at the United States Military Academy (USMA) and transferred to Functional Area 49 (Operations Research and Systems Analysis). MAJ Niblick holds a B.S. in electrical engineering from USMA at West Point and an M.S. in electrical and computer engineering from Purdue University, with a thesis in computer vision and deep learning.

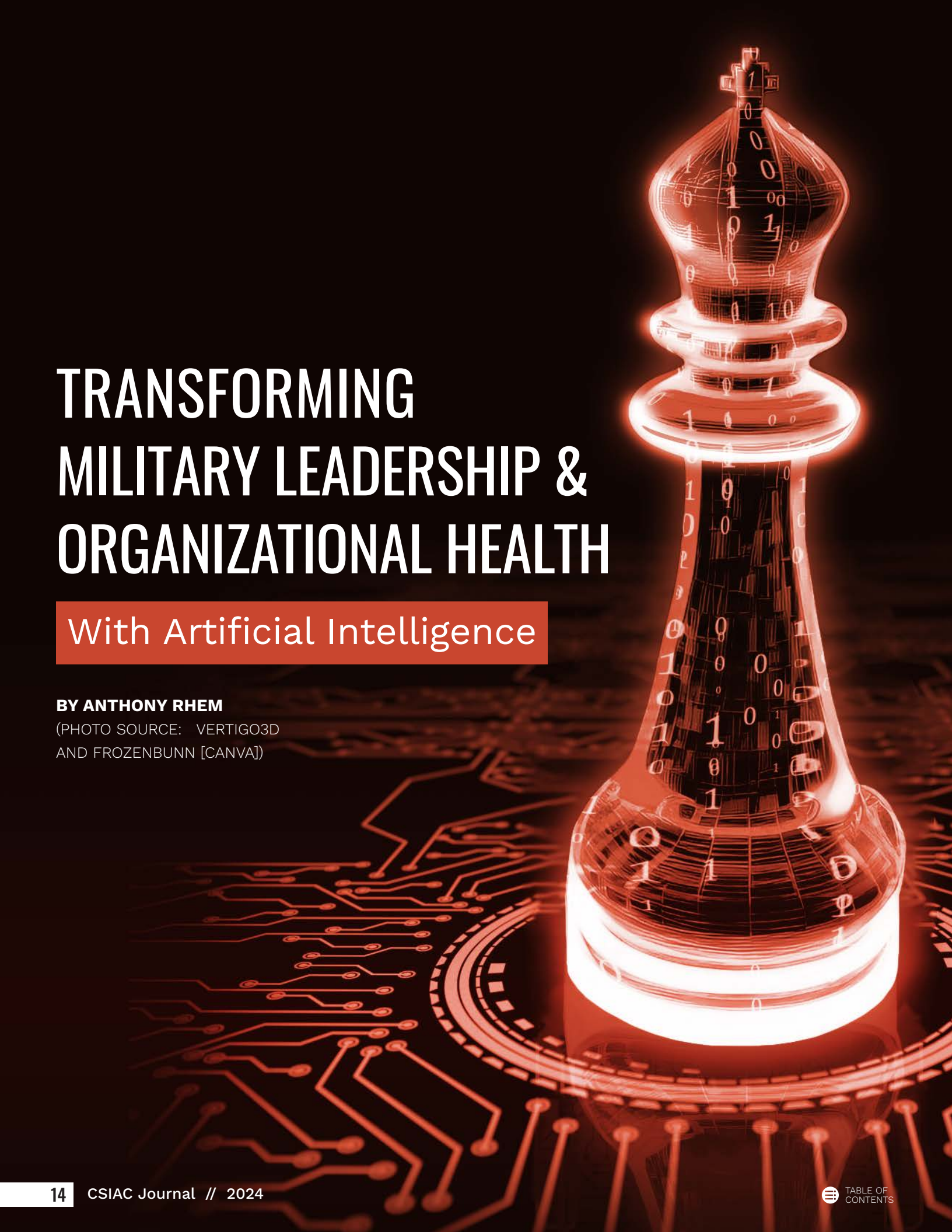
DAVID BAUER is an artificial intelligence evaluator with the U.S. Army Evaluation Center at APG, MD, under ATEC. After working as an evaluator of reliability, availability, and maintainability for over a decade, he transitioned to artificial intelligence and machine learning. Dr. Bauer holds a Ph.D. in computer engineering from the Georgia Institute of Technology.

TRANSFORMING MILITARY LEADERSHIP & ORGANIZATIONAL HEALTH

With Artificial Intelligence

BY ANTHONY RHEM

(PHOTO SOURCE: VERTIGO3D AND FROZENBUNN [CANVA])



INTRODUCTION

Artificial intelligence (AI) fuels not only the technological advancements in our businesses and homes but also redefines the operational frameworks of governments, military, and the broader societal constructs. The essence of this transformative power, however, finds its most compelling narrative in leadership and organizational health, where machine learning (ML), a subset of AI, plays a pivotal role. AI/ML can be used to support leaders in their efforts to manage and monitor initiatives and drive decisions. ML algorithms using continuous data collection activities can assist and support organization's leaders through understanding if implemented initiatives are impacting operations by improving staff cross-collaboration and productivity while improving product and service innovation. Using predictive analytics to analyze trending data to predict future outcomes, leaders can determine if staying the course or pivoting in a certain direction is needed.

THE ROLE OF ML IN LEADERSHIP

At the heart of leadership is the ability to foresee, adapt, and strategically steer organizations toward success. Powered by continuous data collection, ML algorithms offer leaders a mechanism for insight into their organizations. This provides data-driven insights that inform decision-making processes. Whether it is monitoring the efficacy of newly implemented initiatives or enhancing cross-collaboration among teams, ML stands as an ally for leaders. Its capacity to sift through vast amounts of data and identify patterns not only aids in improving operational efficiencies but also fosters product innovation by revealing untapped opportunities.

The predictive capabilities of ML, fueled by analytics, allow leaders to navigate their organizations with foresight. Analyzing trends and predicting future outcomes become instrumental in deciding whether to maintain the current trajectory or pivot in a new direction. This not only ensures agility and resilience in an ever-changing environment but also aligns organizational efforts with the most promising pathways to success.

ETHICAL CONSIDERATIONS IN THE USE OF AI

As AI becomes increasingly integral to organizational strategy and decision-making, the importance of ethical considerations grows exponentially. Infusing AI solutions with ethical data practices is nonnegotiable. Leaders are tasked with the responsibility to ensure that AI is employed in a manner that respects privacy, promotes fairness, and prevents biases. The ethical deployment of AI underscores the commitment of an organization to responsible innovation and builds trust among stakeholders.

> ***As AI becomes increasingly integral to organizational strategy and decision-making, the importance of ethical considerations grows exponentially.***

Ensuring that AI systems are developed and used in a way that promotes equality and fairness for the users and those effected by the AI system should be at the forefront of any AI system's implementation as well as its ethical use and the ethical use of data. To ensure AI systems are developed with an ethical core, it is essential to start with establishing a diverse AI product development team that is active in designing, developing, and implementing the AI application [1]. A diverse team will bring a "diversity of thought" to the initiative and during the selection and cleansing of data to assist in removing bias from being a part of the algorithms used and ensure the models are trained with ethical data that adheres to privacy and security. Through collaboration, knowledge sharing, and knowledge reuse, a diverse team will bring different points of view, experiences,

and cultural backgrounds to stimulate innovation and eliminate (or limit) bias. This action leads to innovation, which will enable organizations to deliver unique and/or improved AI products.

Leaders also need to be aware of the ethicality of AI applications being developed and deployed at their organizations. They must examine and understand whether the outcomes from applying AI violate U.S. federal, European Union General Data Protection Regulation, and/or other ethical, security, and privacy standards. Leadership will need to adopt a standard for AI that identifies general tenants for AI implementation focused on ethical adherence. Leaders must enable support for implementation, acceptance, and adoption of AI. Considerations for cultivating a system-thinking mindset and incorporating systems thinking, personal mastery, creation of mental models and a shared vision, and cultivation of team learning are essential for effective leadership of AI implementation.

QUALITY DATA: A CRITICAL INGREDIENT TO EFFECTIVE AI SOLUTIONS

For AI and ML to unlock their full potential, the foundation must be laid with quality data. The adage "garbage in, garbage out" holds particularly true in the context of AI. High-quality data not only enhances the accuracy of ML algorithms but also ensures that the insights generated are actionable and relevant. Leaders must prioritize establishing robust data collection and management systems that guarantee integrity and reliability of the data fed into AI systems [2].

The ethical use of data in AI applications is a critical issue, as AI systems and algorithms rely on data to learn and make decisions. The way data is collected, stored, used, and shared can have significant impacts on individuals, organizations, and society. Ethical use of data in AI systems builds trust and ensures that they are adopted and used in a responsible manner. Data ethics principles emphasize the importance of privacy, transparency, and responsibility in practices and provide guidelines for ensuring that data is collected, stored, and used in an ethical manner.

The following are key areas representing data ethic principles [2]:

- Transparency: Data ethics principles should be clear, open, and transparent to all stakeholders. This includes clearly stating the purpose and use of collected data, as well as providing information on how data is collected, stored, and protected.
- Fairness: Data should be collected and used in a way that is fair and nondiscriminatory. This includes ensuring that data collection does not perpetuate or exacerbate existing inequalities or biases.
- Privacy: Data privacy should be respected, and data should be collected and used in a way that protects individuals' personal information and autonomy. This includes ensuring that data collection is done with informed consent and that it is not shared or used in ways that violate individuals' privacy rights.
- Responsibility: Data collectors and users are responsible for ensuring that data is collected and used ethically. This includes being accountable for any harm that may result from collecting or using data and taking steps to mitigate that harm.
- Security: Data should be stored and transmitted securely to protect it from unauthorized access, use, or disclosure.
- Inclusivity: Data collection and use should be inclusive and considerate of diverse perspectives and experiences. This includes being aware of and addressing

High-quality data not only enhances the accuracy of ML algorithms but also ensures that the insights generated are actionable and relevant.

any potential biases in the data and actively seeking out underrepresented perspectives.

- Transparency in Decision-Making: Decisions that are made using data should be explainable and interpretable so that individuals can understand how and why decisions are being made and if any bias is present in the model.
- Continual Assessment: Organizations should regularly assess the ethical implications of their data collection and use practices and make any necessary changes to ensure they align with these principles.

EXAMINING THE ETHICAL USE OF AI APPLICATIONS

When examining the ethical use of AI, there are several key factors to consider. These factors align with the key areas representing data ethics principles. Having ethical data to train the algorithms contributes greatly to ensuring the AI solution delivers ethical results. The key factors in examining AI applications include the following [3].

Data Bias: The training data used to develop an AI model may contain biases that are then reflected in the model's decisions and predictions. It is important to examine the data used to train the model and identify any potential sources of bias that may be present.

Algorithmic Bias: The algorithms and mathematical models used in AI can also be biased and may lead to biased decisions or predictions. It is important to examine the algorithms used in the AI system and identify any potential sources of bias that may be present.

Fairness: AI systems should be fair and nondiscriminatory and not perpetuate or exacerbate existing inequalities or biases. It is important to examine the AI system to ensure that it is not treating different groups of people unfairly.

Explainability: AI systems should be explainable so that individuals can understand how and why decisions are being made. It is important to examine the AI system to ensure that it is transparent and interpretable.

Privacy: The use of AI should respect privacy and personal autonomy and not violate individuals' rights. It is important to examine the AI system to ensure that it is collecting and using data in a way that is consistent with privacy laws and regulations.

Transparency: The purpose and use of the AI system should be clear and open to all stakeholders. It is important to examine the AI system to ensure that it is transparent and that stakeholders are aware of how the data is being used.

Security: The AI system should be designed to protect data from unauthorized access, use, or disclosure. It is important to examine the AI system to ensure that it is secure and that data is being stored and transmitted securely.

Continual Assessment: Organizations should regularly assess the ethical implications of their AI use and make any necessary changes to ensure they align with these principles.

Having an AI ethics framework is essential for enabling the implementation and execution of ethics in an AI application (see Figure 1). This framework plays a significant role in ensuring that AI systems are developed and used in a way that is ethical, fair, transparent, and accountable. While the benefits of an AI ethics framework are clear, its implementation can be challenging. This requires a commitment to ongoing evaluation, the flexibility to adapt to new insights and circumstances, and the incorporation of diverse perspectives to address complex ethical dilemmas. Organizations must invest in education, training, and interdisciplinary collaboration to effectively implement an AI ethics framework and ensure that AI technologies serve the interest of the organization while respecting ethical norms and values.

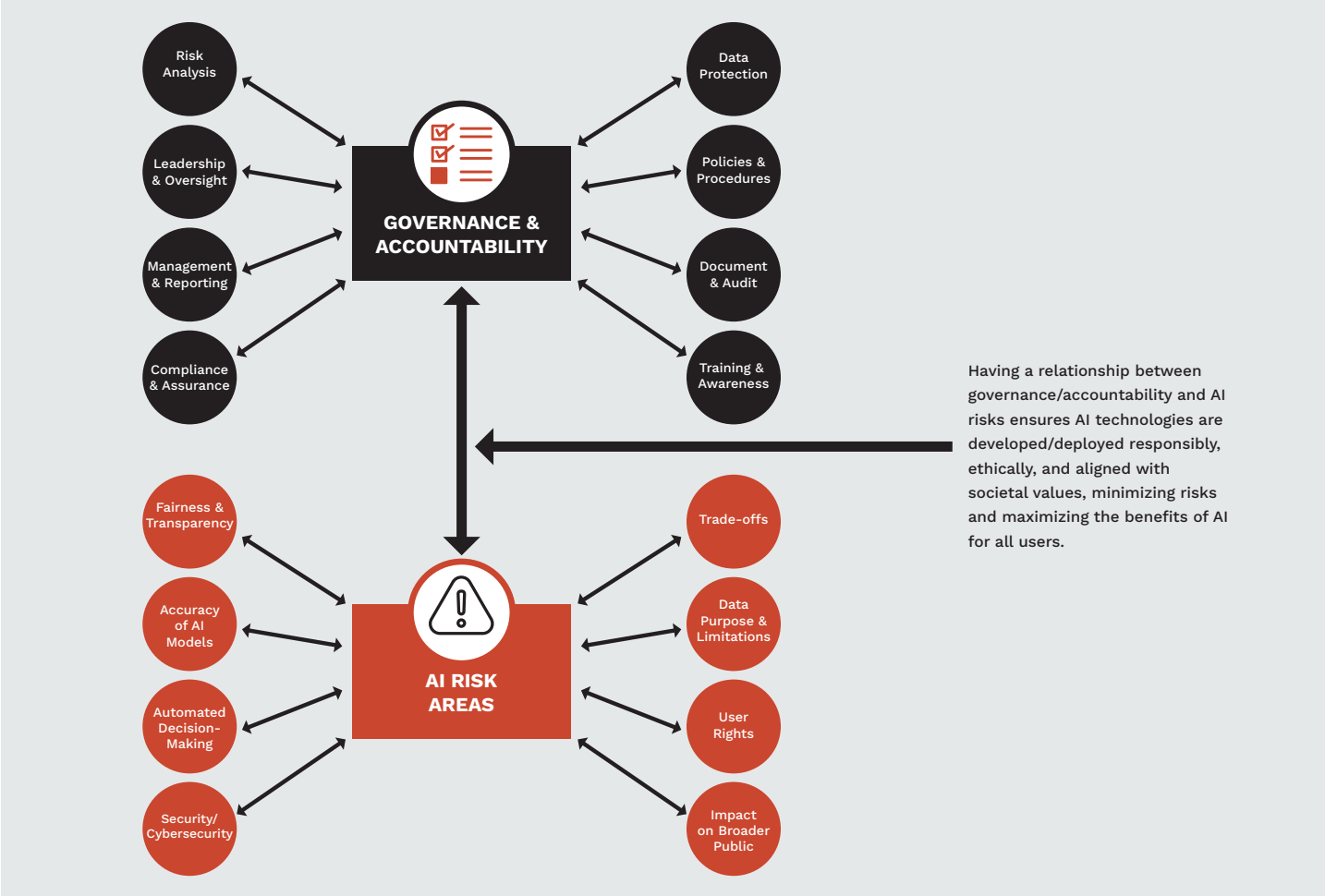


Figure 1. AI Ethics Framework Example *(Source: A. Rhem)*.

EMPOWERING DEFENSE LEADERSHIP THROUGH ML

AI has the potential to fundamentally transform the operational, strategic, and leadership paradigms within the U.S. Department of Defense (DoD) and broader defense community. This transformation is rooted in the capabilities of ML, a subset of AI, which acts as a catalyst in enhancing decision-making, operational efficiency, and innovation in defense mechanisms [4].

Leadership within the defense sector is characterized by the necessity for rapid, informed, and strategic decision-making often under high-stake conditions. Through their ability to process and analyze vast datasets continuously, ML algorithms provide an unparalleled asset. For defense leaders, this translates into actionable intelligence—offering insights into operational readiness, threat detection, and resource allocation. ML's predictive analytics capabilities enable the anticipation of potential threats and assessment of various strategic outcomes, thereby informing critical decisions that could shape the future security landscape.

Applying ML extends beyond strategic oversight and includes facilitating enhancements in cross-collaboration among different arms of the defense community. It supports integrating operations and optimizing logistics, ensuring that the defense apparatus functions as a cohesive and agile unit. Furthermore, by leveraging ML for product innovation, defense organizations can stay ahead of the technological curve, developing advanced defense solutions that ensure

> ***AI has the potential to fundamentally transform the operational, strategic, and leadership paradigms within the U.S. Department of Defense and broader defense community.***

a competitive edge in national and global security arenas.

ENSURING MISSION SUCCESS WITH QUALITY DATA

The effectiveness of AI and ML within the defense community hinges on the availability of high-quality data. Accurate, timely, and relevant data is the lifeblood of AI systems, enabling them to deliver insights critical for mission success. From intelligence analysis to autonomous systems, cyber defense, and logistical support, high-quality data ensures AI-driven decisions are accurate and timely, which is vital in high-stakes scenarios where inaccuracies can lead to significant consequences. It enables real-time intelligence gathering, allowing military personnel to make informed strategic decisions and effectively plan operations. The DoD and defense organizations must prioritize establishing data curation processes and frameworks to ensure data integrity and security while applying ethical principles (see Figure 2) given the sensitive nature of defense operations.

Additionally, quality data drives the automation of routine tasks, such as surveillance and data analysis, freeing up personnel to focus on strategic duties and ensuring resources are utilized efficiently through optimized logistics and supply chains. Enhanced situational awareness and operational efficiency are direct benefits of quality data in military AI applications. It facilitates comprehensive analysis across various intelligence types, offering a holistic, operational view and improving planning and responsiveness. Powered by quality data, predictive analysis enables the anticipation of potential threats and changes, fostering a proactive stance in military operations. Moreover, the importance of quality data in the cyber realm extends to securing sensitive information and infrastructure, with AI systems relying on it to detect, identify, and effectively neutralize cyber threats.

The ethical use of AI in military operations, particularly in reducing collateral damage and ensuring compliance with international laws, underscores the necessity for quality

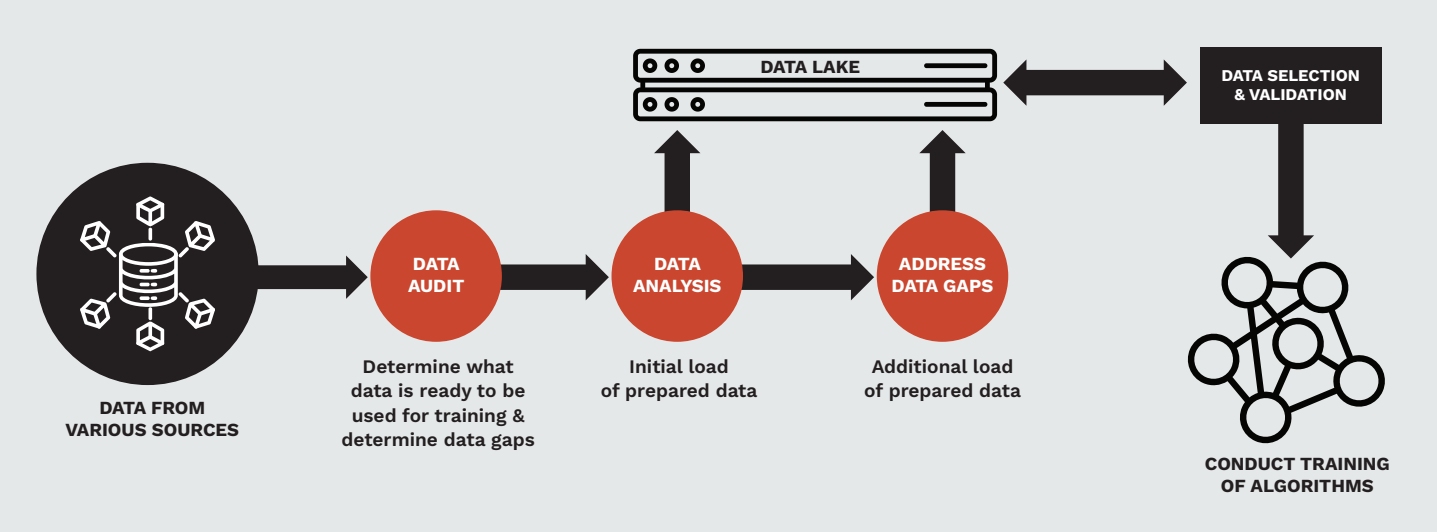


Figure 2. Ethical Data Curation Process *(Source: Rhem [2])*.

> ***Powered by quality data, predictive analysis enables the anticipation of potential threats and changes, fostering a proactive stance in military operations.***

data [5]. High-quality data is crucial for accurately identifying targets and minimizing unintended harm, thus supporting ethical considerations and bias mitigation in AI applications. This adherence to ethical standards and international norms is paramount in maintaining the legitimacy and effectiveness of military actions in the global arena.

The role of quality data extends to training and simulation, enhancing the realism of training programs and preparing military forces for various scenarios. It is also pivotal in developing, testing, and refining AI systems themselves, ensuring these technologies perform reliably under diverse conditions. Facing challenges like data security and integration, military organizations must prioritize advanced data management practices and foster collaborations to maintain a technological edge in the complex security landscape, highlighting the indispensable role of quality data in the effectiveness and ethical deployment of military AI solutions.

IMPLEMENTING AI SOLUTIONS

Implementing AI solutions within military organizations involves a systematic and strategic approach to integrate advanced technologies with existing military operations, capabilities, and infrastructure [4]. The process requires careful planning, adherence to ethical standards, and consideration of operational, technological, and human factors.

Human factors are an important aspect of implementing AI solutions in the military and cover the physical and task conditions [6]. These factors refer to the study and application of psychological, physiological, and ergonomic principles to design systems, equipment, processes, and strategies that effectively integrate human capabilities and limitations [7]. Such factors will help safety personnel and members implement safety protocols. The aim is to enhance operational effectiveness, safety, and well-being in the challenging and often high-risk military environment. This interdisciplinary approach encompasses various aspects from the design of user-friendly technology and equipment to the optimization of training, team dynamics, and decision-making processes [7].

The development or acquisition of AI technology is a critical step, with military organizations needing to decide between in-house development, leveraging partnerships with industry and academia, or procuring off-the-shelf solutions [4]. This decision-making process should weigh the benefits of rapid access to cutting-edge technologies against the need for secure management of intellectual property and operational security. Rigorous testing and validation are essential to confirm that AI solutions meet stringent military requirements and can integrate smoothly with existing operational standards.

Integrating AI solutions into the military ecosystem requires careful attention to interoperability and operational integration. Ensuring that new AI technologies work seamlessly with legacy systems and complement existing tactics and procedures is crucial for their successful adoption. This stage involves significant adjustments, including upgrading outdated systems, training personnel to operate new AI tools effectively, and integrating AI technologies into live operations gradually. Training and change management are indispensable in this phase, equipping personnel with the necessary skills and addressing cultural and organizational resistance to change, thus facilitating a smooth transition to AI-enhanced operations.

Additionally, ongoing evaluation, adaptation, and cybersecurity are paramount for maintaining the effectiveness and security of AI applications in military contexts.

Establishing mechanisms for real-time performance monitoring and creating feedback loops from operational use enable continuous improvement and rapid adaptation to emerging challenges. Robust cybersecurity measures protect sensitive AI systems from threats, while resilience planning ensures that military operations can persist in the face of AI system failures or adversarial threats. Through these comprehensive steps, military organizations can successfully implement AI solutions, leveraging them to achieve strategic advantages and operational excellence in modern warfare scenarios.

Robust cybersecurity measures protect sensitive AI systems from threats, while resilience planning ensures that military operations can persist in the face of AI system failures or adversarial threats.

CONCLUSIONS

As the complexities of the 21st century are explored, the role of AI in enhancing organizational health, performance, and leadership cannot be overstated. It offers a path forward that is informed by data-driven insights, characterized by innovation, and guided by ethical considerations. Incorporating AI and ML into the strategic fabric of the defense community signifies a transformative shift. It presents an opportunity to redefine leadership, enhance operational effectiveness, and spearhead innovation in defense capabilities.

By leveraging AI and ML, defense leaders can ensure more informed decision-making, foster greater collaboration, and drive the development of next-generation defense technologies. As the defense community navigates this digital transformation, the focus must remain on harnessing the power of AI responsibly with a steadfast commitment to ethical principles and safeguarding global security. For leaders willing to embrace this journey, AI and ML not only promise a strategic edge but also the opportunity to redefine what is possible for military operations. The future of defense leadership is inherently linked to the intelligent integration of technology, promising a horizon where AI empowers the defense community to achieve unprecedented levels of readiness and resilience. ■

REFERENCES

[1] AI Policy Exchange. "Anthony Rhem – How to Put AI Ethics into Practice." Video, YouTube, https://www.youtube.com/watch?v=XW4Bc9LLR9Y, 17 October 2020.

[2] Rhem, A. J. "Ethical Use of Data in AI Applications." *Ethics – Scientific Research, Ethical Issues, Artificial Intelligence and Education*, IntechOpen, pp. 95–108, https://doi.org/10.5772/intechopen.1001597, 2023.

[3] Baer, T., and V. Kamalnath. "Controlling Machine-Learning Algorithms and Their Biases." *McKinsey Insights*, https://www.mckinsey.com/business-functions/risk/our-insights/controlling-machine-learning-algorithms-and-their-biases, 2017.

[4] Bistron, M., and Z. Piotrowski. "Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens." *Electronics*, vol. 10, no. 7, p. 871, https://doi.org/10.3390/electronics10070871, 2021.

[5] Schraagen, J. M. "Responsible Use of AI in Military Systems: Prospects and Challenges." *Ergonomics*, vol. 66, no. 11, pp. 1719–1729, https://doi.org/10.1080/00140139.2023.2278394, 2023.

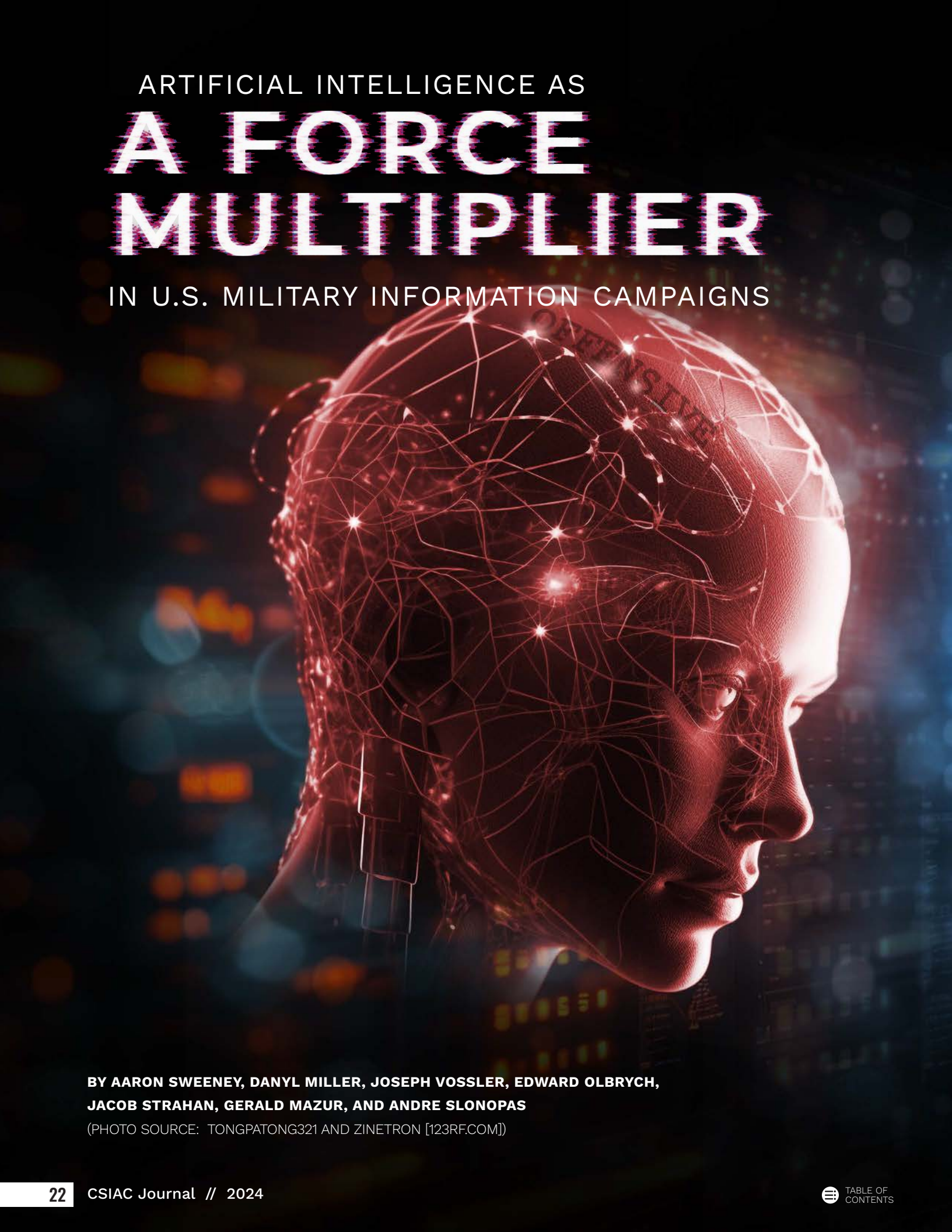
[6] National Academies of Sciences, Engineering, and Medicine. *Human Factors in the Design of Tactical Display Systems for the Individual Soldier*. Washington, D.C.: The National Academies Press, https://doi.org/10.17226/9107, 1995.

[7] van Diggelen, J., K. van den Bosch, M. Neerincx, and M. Steen. "Designing for Meaningful Human Control in Military Human-Machine Teams." *Research Handbook on Meaningful Human Control of Artificial Intelligence Systems*, Edward Elgar Publishing, 2023.

BIOGRAPHY

ANTHONY J. RHEM is a thought leader, author, and consultant in AI, knowledge management (KM), big data, information architecture, and innovation. He has served as chief executive officer/principal consultant of A.J. Rhem & Associates Inc. (AJRA), a system integration consulting, training, and research firm specializing in KM and AI. Through AJRA, he and his staff work with Fortune 1000 companies and federal and state agencies to deliver technology solutions, strategies, governance, and architectures in AI and KM. Dr. Rhem holds a B.S. in marketing/computer science from Purdue University, an M.S. in computer science/AI from DePaul University, and a Ph.D. in KM from Walden University.

ARTIFICIAL INTELLIGENCE AS A FORCE MULTIPLIER IN U.S. MILITARY INFORMATION CAMPAIGNS



BY AARON SWEENEY, DANYL MILLER, JOSEPH VOSSLER, EDWARD OLBRYCH, JACOB STRAHAN, GERALD MAZUR, AND ANDRE SLONOPAS

(PHOTO SOURCE: TONGPATONG321 AND ZINETRON [123RF.COM])

SUMMARY

Military commanders have used information throughout warfare to influence, mislead, disrupt, or otherwise affect the enemy's decision-making and capabilities. This article discusses the history of information operations (IOs) and enduring importance of incorporating actions in the information environment in military strategy.

THE EVOLUTION OF MILITARY IOs

Ancient IOs relied on human intellect and psychology. As early as the 5th century BC, Sun Tzu recognized the importance of employing spies and couriers to collect intelligence on the adversary before engaging in battle [1]. According to Tzu, "All warfare is based on deception," highlighting the importance of information and psychological warfare in ancient military operations [2]. Military deception is one of the oldest information-related capabilities that are leveraged to this day by U.S. military IOs [3].

As communications evolved in the Middle Ages, more advanced societies recognized that just about any physical tool could be used to affect the information environment. Medieval armies used information propagation and security advances with carrier pigeons,

visual signals, and early cryptography. During the Crusades, European and Muslim troops used intricate spies and informants to collect enemy movements and intentions. Most notably, Muslim military commander Sultan Saladin deployed spies to track the Crusaders' activities while also planting false information about the size and location of his main elements [4]. Such information tactics aided his military while significantly degrading Europe's ability to deploy forces effectively.

The printing press revolutionized knowledge distribution throughout the Renaissance and afterward. Governments and military commanders realized the power of public opinion and used propaganda to demoralize their foes. Psychological operations became a systematic military policy in this age, making narrative control as crucial as combat control. Commanders exploited disinformation to discourage those under siege and deceive the opposition about reinforcements and supply lines. A notable example is the siege of Orleans during the Hundred Years' War, where Joan of Arc's presence and disinformation about the French force's strength and morale helped relieve the siege [5]. Another example is how Genghis Khan's Mongol forces applied psychological warfare to undermine opponent resistance before an invasion by spreading dread of their savagery [6].

IOs changed considerably in the 20th century, especially during the World Wars. World War I saw newspapers, posters, and films used for propaganda to affect public opinion and morale. Radio increased the reach of psychological operations. British intelligence from 1917 intercepted and decrypted the Zimmermann Telegram, a secret communication from Germany to Mexico proposing a military alliance. The British then released the telegram to U.S. President Woodrow Wilson. U.S. public exposure to this telegram played a significant role in swaying public opinion and contributed to the nation's decision to enter the war against Germany [7].

In World War II, the Allies' concatenated Operation Bodyguard, which tricked the Axis forces about the D-Day invasion location. This was one of the most famous IOs in which the Allies deceived the Nazis about the D-Day invasion's schedule and location. Phantom armies, radio traffic, and deceptive reconnaissance images increased the confusion among German decision-makers [8]. Operation Fortitude involved creating a fictitious First United States Army Group in southeastern England to suggest an invasion at Pas de Calais, France (Figure 1) [9].

> ***World War I saw newspapers, posters, and films used for propaganda to affect public opinion and morale.***

Television and early computer technologies changed IOs during the Cold War. Both sides engaged in substantial propaganda, espionage, and counterintelligence as information

Figure 1. Dummy Inflatable Sherman Tank Used During Operation Fortitude in WWII *(Source: U.S. Army)*.

warfare advanced. The U.S. government used Voice of America and Radio Free Europe as crucial tools to broadcast news and pro-Western narratives to Eastern Europe and the Soviet Union [10]. These broadcasts aimed to counter communist propaganda narratives and promote Western values and perspectives behind the Iron Curtain. In contrast, the Soviet Union ran extensive radio propaganda campaigns and funded speakers, academics, and other activists in the West to undermine the unity of allegiance to classical Western values—these broadcasts aimed at both domestic and international audiences, promoting communist ideology and countering Western influence [11].

One of the most notable military IOs during the Vietnam War was Operation Eldest Son. Conducted by U.S. Special Forces and Central Intelligence Agency operatives, the operation involved tampering with enemy ammunition to make it look like standard munitions were supplied by China or the Soviet Union—this modified ammo aimed to detonate the inside of weapons, thus inflicting harm or death [12]. Spies secretly inserted it in enemy supply routes or left it behind during retreats. The operation aimed to reduce enemy morale and trust by sowing doubts about the munitions. Disinformation pamphlets, television, and radio broadcasts warned Vietnamese forces of the hazards of "poor" munitions supplied by the Chinese and Soviet suppliers [13]. They planted distrust among adversary groups, boosting the operation's psychological effect.

The Space Race was also a significant part of Cold War IOs. Technological achievements, including the Soviet Union's launch of Sputnik Yur, Gagarin's spaceflight, and the U.S. Apollo moon landings, were heavily publicized on television to demonstrate each superpower's technological and ideological superiority.

Paralleling technological advances in the late 1990s and since the turn of the century, information operations have advanced exponentially. Internet, social media, and modern computers, including mobile platforms, changed how military commanders employed IOs [14]. These platforms increased the reach and precision of information, laid the foundation for cyber warfare, and exponentially increased the speed of spreading digital propaganda over social media.

For example, Operation Glowing Symphony was a significant U.S. cyber operation that marked a notable shift in the approach and tactics employed in cyber and information warfare. Another important component of Operation Glowing Symphony was the official acknowledgment of the U.S. government to using offensive cyber capabilities. This operation was conducted as part of the broader campaign against the Islamic State (ISIS) [15]. These actions disrupted and degraded ISIS's ability to spread its information, recruit members through social media, and carry out its IOs using digital communication networks [16]. The primary objective of Glowing Symphony was to disrupt ISIS's extensive and sophisticated media network to spread its messaging and information. ISIS has been effectively using the internet and social media for information dissemination, recruitment, and radicalization. The U.S. Cyber Command dismantled these capabilities by targeting servers, websites, and data centers used by ISIS. A critical aspect of this operation was gaining access to and control over ISIS's network, which allowed U.S. cyber forces to not only disrupt ISIS's ability to spread information but also implant and execute friendly information aimed at the same audiences that ISIS was targeting [17].

> ***Operation Glowing Symphony was a significant U.S. cyber operation that marked a notable shift in the approach and tactics employed in cyber and information warfare.***

INTRODUCTION

Recent years have seen an unprecedented explosion in AI for a broad range of applications that range from computation, generative AI,

research, and other fields. The rise of AI has the potential to revolutionize the military IOs as well. AI can do the following:

- Transform how militaries conduct information warfare, offering unprecedented capabilities and new challenges.
- Generate outstanding amounts of information aligned to the same narrative that can sway the opinions of the masses in extremely short amounts of time.
- Analyze massive volumes of satellite photos, real-time signal intercepts, and open-source intelligence data.
- Dramatically improve situational awareness and decision-making and risk oversaturating the decision-makers with information.
- Generate content to disseminate over all mediums, making counter-information nearly impossible due to the sheer volume of information the target receives.
- Generate deceptive information, leading adversarial AI to derive wrong conclusions and mislead the decision-maker.
- Analyze massive databases to determine target groups' psychological characteristics, allowing more practical knowledge and focused psychological operations.

AI systems may forecast the future based on historical data and current patterns. Leveraging such technology helps predict adversary maneuvers, grasp complicated conflict zone patterns, and prepare for numerous enemy courses of action.

Adversarial and malicious actors may use AI-generated deepfakes and synthetic media to construct misinformation or disinformation campaigns that are hard to spot, affecting public opinion and degrading morale (e.g., Figure 2). Synthetically produced information could endure for decades as actual occurring events, having long-term collateral effects that will be difficult to challenge and uproot, and creating moral and ethical implications.

APPLICATIONS OF AI IN IOS: A CYBER FORTRESS CASE STUDY

The Cyber Fortress exercise, a critical training and preparedness event held in Virginia, represents a significant evolution in defending critical infrastructure (e.g., Figure 3).

> ***Adversarial and malicious actors may use AI-generated deepfakes and synthetic media to construct misinformation or disinformation campaigns that are hard to spot, affecting public opinion and degrading morale.***

Cyber Fortress creates an interagency response framework incorporating local, state, and federal cooperation and international collaboration. This approach includes partnerships with commercial private entities, state and federal governments, and the military to enable a unified response across multiple domains. Cyber Fortress is pushing beyond cyber defense and everyday operations into more complex scenarios involving extensive IOs. This exercise is a control method designed to stress-test processes and

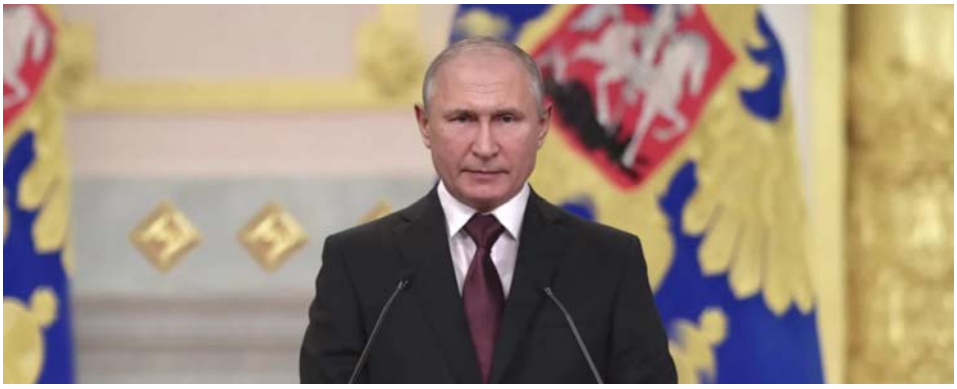


Figure 2. Deepfake of Vladimir Putin Warning Americans on Election Interference and Increasing Political Divide *(Source: RepresentUs/Wikimedia Commons).*

Figure 3. Soldiers Assigned to the 91st Cyber Brigade Work With Civilian Cyber Specialists During the Cyber Fortress Exercise *(Source: Virginia National Guard)*.

institutions, preparing them for cyber response scenarios that may arise in real-world scenarios to include in the information domain. Distinguished by its focus on integrating substantial IOs through the Information Operations Network (ION), this exercise extends beyond conventional cyber defense, presenting a multifaceted approach to cybersecurity and information warfare.

The Cyber Fortress exercise's ION is a groundbreaking innovation in cyber warfare training. It represents a simulated digital environment, often called a "fake internet," meticulously designed to mirror the intricate and multifaceted digital ecosystem of the "real internet." This sophisticated simulation includes various components, such as replicated news websites, social media platforms, and other information dissemination outlets, creating a highly authentic and immersive backdrop for the exercise.

ION's role in Cyber Fortress is pivotal. It is a dynamic battleground where "Red" and "Blue" Teams launch information campaigns at participants while their cyber counterparts fire ones and zeros over wires. The network is not just a static backdrop but a fully interactive landscape that responds and evolves based on the actions of the exercise's participants. This level of realism is essential for training personnel in the nuances of modern digital warfare, where the lines between virtual and physical confrontations are increasingly blurred.

AI is central to the operation of ION. Red Teams leverage this system for offensive roles, and the Blue Teams conduct defense.

RED TEAM AI-DRIVEN IO CAMPAIGNS

In the Cyber Fortress exercise, the Red Teams employ AI to execute intricate and aggressive IOs, demonstrating the evolving nature of digital warfare. Their overarching goal is to disseminate disruptive information to sow seeds of distrust and panic among the public. Several innovative AI applications augment the sophistication of their tactics, each designed to exploit the vulnerabilities inherent in the information ecosystem.

The Red Team leverages AI-driven algorithms and linguistic expertise to create messages in multiple languages, embedding cultural and ethnic nuances. This strategy ensures the messages are translated for linguistic accuracy and are culturally relevant, resonating deeply with various ethnic groups in the United States. AI systems generate more persuasive and impactful content by understanding and tapping into cultural idioms, historical contexts, and social nuances.

This multilingual capability is crucial in a country as ethnically diverse as the United States. It allows the Red Teams to effectively target specific communities, potentially creating rifts and exacerbating existing tensions. In this context, AI demonstrates a sophisticated understanding of the cultural dynamics and targeted information's role in influencing public opinion.

> ***AI systems generate more persuasive and impactful content by understanding and tapping into cultural idioms, historical contexts, and social nuances.***

Another critical aspect of the Red Teams' strategy is using AI for adaptive messaging and real-time feedback. AI systems monitor the public's reaction to the disseminated content and adjust the messaging accordingly. If a particular narrative is gaining traction or causing the desired level of disruption, AI algorithms can amplify it. Conversely, if a message is not having the intended effect, AI can quickly alter the approach, testing different narratives and strategies to achieve the desired impact. This adaptive approach is crucial in maintaining the momentum of the information campaign. It allows the Red Teams to stay one step ahead, continually refining their tactics in response to public reaction and feedback.

Red Teams also employ AI as chat conversation generators to post comments across various digital platforms. These comment chats mimic human interaction, engaging in online conversations and debates to further influence public opinion. These AI-generated discussions amplify the disinformation campaigns' reach by actively participating in social media dialogues, forums, and comment sections, giving an illusion of grassroots support or opposition to viewpoints. This tactic effectively manipulates the perceived public consensus, swaying opinions and deepening divisions within the digital discourse.

AI's role extends beyond content creation to strategically disseminating this tailored content. The Red Teams use AI to identify and utilize various digital platforms within the ION, from social media networks to news websites, ensuring that their disruptive messages achieve maximum reach and impact. This approach mirrors real-world information warfare tactics, exploiting diverse communication channels to spread disinformation and propaganda.

BLUE TEAM AI-DRIVEN IO CAMPAIGNS

In the dynamic arena of the Cyber Fortress exercise, the Blue Teams are also exploring AI to counteract the sophisticated IOs launched by their Red Team counterparts. Their multipronged approach uses the latest advancements in AI to generate rapid responses, analyze data, and detect falsified content.

The main effort of the Blue Teams' strategy is the rapid generation of content for public messaging. AI tools swiftly produce accurate and reliable information to counteract the Red Team's disinformation campaigns. This quick response capability is critical in mitigating the impact of false narratives. The AI systems are sophisticated enough to parse immense volumes of misinformation, distill facts, and craft timely and factual responses. These AI-driven content generation tools can analyze the trending topics and prevalent narratives from the Red Team and instantly generate counternarratives. Such information battles ensure that the public has access to balanced information, helping to prevent the spreading of harmful misinformation.

Blue Teams adeptly employ AI for rapid content generation, strategic communication, and crucial language translation tasks. They utilize advanced AI algorithms to translate an extensive volume of articles and digital content across various languages. ION capability is essential in identifying and analyzing potentially damaging narratives and disinformation campaigns orchestrated by the Red Teams. By breaking language barriers, the AI systems enable the Blue Teams to comprehensively monitor and counteract misinformation across a diverse linguistic spectrum, ensuring a thorough and effective response to their adversaries' multifaceted information warfare tactics.

During Cyber Fortress, the Information Operations Support Cell (IOSC), serves as the analytical and strategic hub for the Blue Teams. Service members of the IOSC serve in various technical civilian roles and bring decades of experience and expertise in AI and other relevant technologies. IOSC oversees the information environment, where AI plays a crucial role in sifting through the vast ocean of data produced by various information outlets. Analyzing this data, the IOSC identifies patterns, trends, and strategies shaping the Blue Team's counterinformation campaigns.

The AI systems in the IOSC utilize advanced algorithms for natural language processing, sentiment analysis, and pattern recognition. This highly sophisticated approach enables them to quickly discern the underlying strategies of the Red Team's campaigns, such as target demographics, message frequency, and thematic content. Understanding these aspects allows the Blue Teams to tailor their countermeasures more effectively, ensuring rapid and strategically targeted responses. This capability is vital in maintaining the integrity of information within the exercise. By quickly identifying and addressing deceptive content, the Blue Teams help safeguard the digital information landscape from being corrupted by falsified narratives. This task is particularly challenging given the sophistication of modern deepfake technology, which requires equally advanced AI tools to combat.

Beyond reactive measures, the Blue Teams also use AI to develop proactive strategic communication plans. By understanding the information environment and tactics used by the Red Teams, AI tools help craft comprehensive communication strategies. These strategies counter existing misinformation and build resilience within the masses against future disinformation campaigns.

AI does not operate in a vacuum in the Blue Teams. It works in tandem with human analysts who provide context, judgment, and creative thinking that AI alone cannot achieve. This collaboration ensures that the counterinformation campaigns remain grounded in ethical and practical considerations, balancing the efficiency of AI with the nuanced understanding of human operators. The Cyber Fortress exercise also serves as a training ground for the Blue Teams to adapt and improve their AI tools. Through iterative deployment, analysis, and refinement cycles, AI systems become more adept at handling the intricacies of information warfare. This continuous learning aspect of AI is crucial in keeping pace with the evolving tactics of the Red Teams.

Understanding that different demographics consume information differently, the Blue Teams use AI to customize the dissemination of their content. AI algorithms determine the most effective channels and formats for different audiences, ensuring that counternarratives reach the right people in the right way. AI in IOs brings with it a host of ethical considerations. The Blue Teams are conscious of the ethical implications of using AI, particularly regarding privacy, transparency, and accountability. Cyber Fortress lays the foundation for ensuring that AI utilization in IOs adheres to strict ethical guidelines, many of which are still unknown and under development.

EMERGING TECHNOLOGIES AND OTHER AI APPLICATIONS

The future of AI in military IOs is at a revolutionary juncture, with emerging technologies set to enhance capabilities and reshape strategic landscapes significantly. Advanced AI algorithms can process vast amounts of data and generate sophisticated psychological profiles, predictive models, and automated information campaigning. These models can forecast potential threats and generate computerized responses to information campaigns, offering military strategists unprecedented insight and foresight.

One of the most groundbreaking advancements is using AI in deep learning and neural networks. This technology enables the creation of vast amounts of highly realistic synthetic media, which gives psychological operations a strategic advantage. Additionally, AI-driven, natural

language-processing and generation tools are becoming sophisticated enough to autonomously create and distribute convincing narrative content at a scale and speed unmatchable by human operatives.

Strategically, AI's continued integration into military operations will profoundly influence global geopolitics. AI-enhanced information campaigns could lead to a new form of warfare where digital battles occur, impacting public opinion and national policies without physical confrontation. Countries with advanced AI capabilities might gain significant leverage in international relations, potentially leading to a new arms race focused on technological supremacy.

Moreover, AI systems' automated monitoring and analysis capabilities are crucial for detecting disinformation and unusual activity early. By continuously scanning digital communications and media, these AI systems can identify and flag potential threats or misinformation campaigns, allowing for rapid response and countermeasures. This automated vigilance enhances defense capabilities and ensures the integrity and effectiveness of IOs. As such, the future of AI in military IOs is not just about advanced technology but also about maintaining the information advantage for strategic decision-makers and countering emerging digital threats in an increasingly interconnected world.

CONCLUSIONS

Military commanders have always relied on information control and manipulation to amplify the effects of the maneuver element. From the tactical deceit of ancient generals to exquisite cyber operations of the modern world, information control is vital.

Integrating AI into U.S. military IOs is not simply an evolution but a necessary transition in contemporary multidomain operations. AI becomes vital when information volume and complexity surpass human-processing skills. AI's capacity to create, analyze, and distribute vast amounts of material faster than humans makes it essential for future IOs. U.S. forces must exploit AI's potential to counter information while effectively exploring ethical implications. The U.S. military must adapt AI technologies if the country wants to maintain and preserve its strategic edge and keep its information campaigns successful and robust against digital arms race rivals who are also leveraging these tools. The strategic use of AI will shape military IOs, allowing the United States to challenge sophisticated threats and influence operations with unparalleled efficiency and scale.

The U.S. military must adapt AI technologies if the country wants to maintain and preserve its strategic edge and keep its information campaigns successful and robust against digital arms race rivals who are also leveraging these tools.

ACKNOWLEDGMENTS

The authors would like to acknowledge invaluable AI assistance from ChatGPT, which provided critical insights and guidance throughout the writing process. AI's ability to process and generate informative content has been indispensable in shaping this article.

The authors would also like to sincerely thank all the human readers and colleagues who provided feedback and suggestions. Your perspectives and insights have been invaluable in ensuring the comprehensiveness and accuracy of this article. ■

REFERENCES

[1] Warner, M. "The Divine Skein: Sun Tzu on Intelligence." *Intelligence and National Security*, vol. 21, no. 4, pp. 483–492, 2006.

[2] Tzu, S. *The Art of War*. China, 5th century B.C.

[3] Kearney, K. "Denial and Deception—Network-Centric Challenge." Unpublished research paper, U.S. Naval War College, 1999.

[4] Craig, J. S. *Peculiar Liaisons: In War, Espionage, and Terrorism in the Twentieth Century*. Algora Publishing, 2005.

[5] Williams, G. "Manipulation and the Maid." *Medieval Warfare*, vol. 4, no. 2, pp. 25–32, 2014.

[6] Narula, S. "Psychological Operations (PSYOPs): A Conceptual Overview." *Strategic Analysis*, vol. 28, no. 1, pp. 177–192, 2004.

[7] Hughes, C. R. "Fighting the Smokeless War: ICTs and International Security." *China and the Internet, Routledge*, pp. 139–161, 2003.

[8] Bendeck, W., C. Elkington, and O. McConnell. "Diversion and Deception in Warfare," 2016.

[9] Donovan, M. J. "Strategic Deception: Operation Fortitude." U.S. Army War College, 2002.

[10] Puddington, A. *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty*. University Press of Kentucky, 2000.

[11] Lovell, S. *Russia in the Microphone Age: A History of Soviet Radio*, 1919–1970. Oxford: OUP, 2015.

[12] Plaster, J. L. "Wreaking Havoc One Round at a Time." *American Rifleman*, pp. 68–72, 2008.

[13] Stanton, S. L. *Green Berets at War: U.S. Army Special Forces in Southeast Asia*, 1956–1975. Ivy Books, 1999.

[14] Yavetz, G., and N. Aharony. "Social Media for Government Information Dissemination: Content, Characteristics and Civic Engagement." *Aslib Journal of Information Management*, vol. 73, no. 3, pp. 473–496, 2021.

[15] Temple-Raston, D. "How the U.S. Hacked ISIS." *National Public Radio*, 26 September 2019.

[16] Donnelly, C., and M. Stolz. "JTF-ARES as a Model of a Persistent, Joint Cyber Task Force." *European Conference on Cyber Warfare and Security*, vol. 22, no. 1, pp. 169–176, 2023.

[17] Randall, J. D. "Crossing Borders in Cyberspace: Regulating Military Cyber Operations and the Fallacy of Territorial Sovereignty." *Army Law*, p. 82, 2021.

BIOGRAPHIES

JOSEPH VOSSLER is a senior cybersecurity engineer currently serving in the Virginia National Guard's IOSC. He has over 14 years of experience in cybersecurity, intelligence, and data science, including a significant tenure in the U.S. Army as an operations and intelligence professional. SFC Vossler's extensive background encompasses roles in cyber network defense, incident response, intelligence analysis, and data science/ML, notably with ec3 Federal Services, Raytheon, Booz Allen Hamilton, U.S. Army Cyber Command, and the Narcotics and Transnational Crime Support Center.

GERALD MAZUR has held tactical, operational, and policy cyberspace and IOs positions with the U.S. Department of Defense (DoD). He has led teams at the U.S. Cyber Command, delivering effects in support of combatant commanders; contributed to DoD Joint Cyberspace Operations doctrine; and held command and key staff positions in the Army National Guard's 91st Cyber Brigade. COL Mazur holds an M.S. in telecommunications and computer forensics from George Mason University.

ANDRE SLONOPAS is a U.S. Army Cyber and IO Officer and former Presidential Management Fellow, with a strong background spanning research, academia, and government. He has led significant software projects, authored numerous publications on cyber and hardware security, and is a committed advocate for the AI and energy revolution. MAJ Slonopas holds a Ph.D. in aerospace engineering from the University of Virginia.

DANYL MILLER serves as a senior cyberspace and electromagnetic activities Command Sergeant Major (CSM) for the 124th Cyber Protection Battalion of the Virginia Army National Guard and a strategic business analyst for the Joint Force Headquarters – DoD Information Network, with over 30 years of military experience. CSM Miller holds an M.S. in organizational leadership from Excelsior University.

EDWARD OLBRYCH serves as an interdisciplinary engineer at the U.S. Army Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance Center focusing on cyber electromagnetic activity technology. He is also an operations planner for the U.S. Army National Guard, where he has contributed to planning and executing multiple joint international and interagency exercises. CPT Olbrych's background includes contributing to defense projects in software engineering and cybersecurity at Lockheed Martin and serving as a lead developer for Task Force Echo under the 780th Military Intelligence Brigade and a team leader in the 134th Cyber Security Company.

AARON SWEENEY is a principal technical specialist at Microsoft and soldier in the 91st Cyber Brigade, with over 20 years of experience in cybersecurity. SFC Sweeney's focus is on developing military cyber exercises and architecting secure cloud deployments for Fortune 500 companies and other high-impact stakeholders.

JACOB STRAHAN works as the cyber resiliency program manager for the Virginia Department of Emergency Management. As an information effects (IO) planner, he has extensive experience in integrating IO effects into domestic and international cyber exercises. SFC (Ret.) Strahan previously served as the noncommissioned officer in charge of the Information Operations Support Center, 91st Cyber Brigade, Virginia Army National Guard.

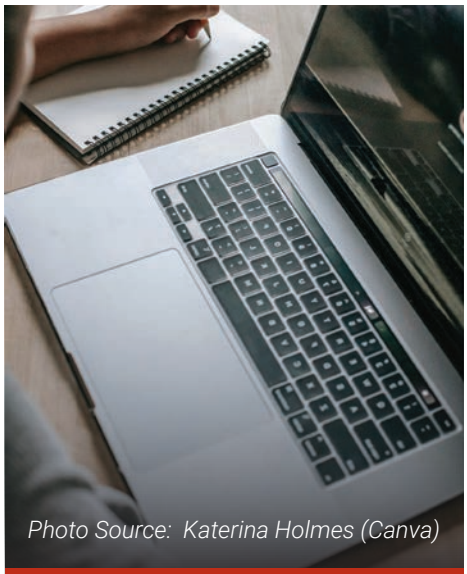


Photo Source: Katerina Holmes (Canva)

A RELEVANCE MODEL FOR THREAT-CENTRIC RANKING OF CYBERSECURITY VULNERABILITIES

BY CORREN MCCOY, ROSS GORE, MICHAEL L. NELSON, AND MICHELE C. WEIGLE

(PHOTO SOURCE: ICONPIX AND ACCOUNTANZ [CANVA])

SUMMARY

The relentless process of tracking and remediating vulnerabilities is a top concern for cybersecurity professionals. The key challenge is trying to identify a remediation scheme specific to in-house, organizational objectives. Without a strategy, the result is a patchwork of fixes applied to a tide of vulnerabilities, any one of which could be the point of failure in an otherwise formidable defense. Given that few vulnerabilities are a focus of real-world attacks, a practical remediation strategy is to identify vulnerabilities likely to be exploited and focus efforts toward remediating those vulnerabilities first.

The goal of this research is to demonstrate that aggregating and synthesizing readily accessible, public data sources to provide personalized, automated recommendations for organizations to prioritize their vulnerability management strategy will offer significant improvements over using the Common Vulnerability Scoring System (CVSS). A framework is provided for vulnerability management specifically focused on mitigating threats using adversary criteria derived from MITRE adversarial tactics, techniques, and common knowledge (ATT&CK). The approach here is tested by identifying vulnerabilities in software associated with six universities and four government facilities. Ranking policy performance is measured using the Normalized Discounted Cumulative Gain (nDCG). Results show an average 71.5%–91.3% improvement toward identifying vulnerabilities likely to be targeted and exploited by cyber threat actors. The return on investment (ROI) of patching using these policies results in a savings of 23.3%–25.5% in annualized costs. The results demonstrate the efficacy of creating knowledge graphs to link large datasets to facilitate semantic queries and create data-driven, flexible ranking policies.

INTRODUCTION

The relentless process of tracking and prioritizing vulnerabilities for patching is a top concern for cybersecurity professionals [1]. Ideally, every organization would apply the security updates for their operating systems and critical applications as soon as possible after updates are released. However, since patches from top vendors are delivered in monthly blocks on "Patch Tuesday," system administrators often find it difficult to select which patches to apply and identify which ones are not applicable [2–4]. Patch Tuesday is the term used to refer to the second Tuesday of each month when Microsoft, Adobe, Oracle, and others regularly release software patches for their software products [5]. Vulnerability prioritization is further hampered when companies delay the automatic installation of security updates in case the patch proves more troublesome than expected [6, 7].

Successful vulnerability management must balance two opposing goals: (1) coverage (fix everything that matters) and (2) efficiency (delay or deprioritize what does not matter) [8]. In industry, the most prevalent vulnerability management strategy identifies the base Common Vulnerability Scoring System (CVSS) scores for all identified vulnerabilities and patches them in descending score order (10 being the highest to 0 being the lowest) [9–11]. Unfortunately, research has shown that CVSS scores are not strongly linked to the emergence of new cyber exploits, and system administrators can be overwhelmed by the volume of vulnerabilities with nearly indistinguishable high scores [12]. While a CVSS score indicates vulnerability severity, it does not predict the exploit potential of the underlying software flaw or the operational impact to the organization.

Aggregating and synthesizing readily accessible, public data sources can provide an automated patch priority ranking by understanding what vulnerabilities and adversaries are relevant to an organization. The proposed relevance-based ranking model enables businesses to adopt a proactive strategy for vulnerability management [13]. Such an approach delivers the most efficient use of people, tools, time, and dollars to address cyber threats that pose the greatest operational risk. Just as search engines provide a better ranking of results based on personalization, so will the ranking of vulnerabilities. Within this context, an approach is sought to define cybersecurity vulnerability mitigation that improves upon rankings employing strategies based on the global CVSS metrics associated with known software vulnerabilities published in the National Vulnerability Database (NVD) [14].

The path to achieve this goal requires gathering, fusing, and analyzing relevant and available data discussed in this article. Specifically, it proceeds as follows. The "Data and Methods" section describes the aggregated public data sources, methods used to synthesize them, and the framework for ranking software vulnerabilities regarding different organizations for patching. The "Evaluation and Results" section evaluates the approach and presents the results. The "Discussions" section examines how the contributions are positioned in the software vulnerability management research landscape and identifies several limitations to the work. Ultimately, the study ends with the "Conclusions" section.

Data and Methods

The goal for this study is to remediate vulnerabilities in the most efficient way possible. This requires leveraging, associating, and analyzing different sources of cyber threat intelligence. The relationships among them need to be understood and organized into a structure for analysis that supports generating prioritized recommendations for effective vulnerability management.

These data sources are used to model software vulnerabilities regarding the skill level of cyber adversaries and their motivation to target a specific industry domain (e.g., national defense, higher education, finance, and health care). The relationships among these data sources and the software vulnerability's life cycle are summarized in Figure 1 to include the following data sets:

1. The Common Weakness Enumeration (CWE) captures data related to the discovery of a software weakness.
2. Data from the Common Vulnerabilities and Exposures (CVE) and CVSS prioritize a vulnerability's severity.
3. The Exploit Database (ExploitDB), Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (KEV) catalog, and Exploit Prediction Scoring System (EPSS) assess the likelihood of a software vulnerability being exploited in the wild.
4. The Common Attack Pattern Enumeration and Classification (CAPEC) and MITRE ATT&CK knowledge base provides data on how to remediate and mitigate published exploits.
5. The NVD catalogs and reports vendor-provided patches to vulnerabilities in commercial or open-source software.

These data sources and their specific leveraged attributes are described in more detail next. Highlighted are how they are synthesized together in a knowledge base to connect data about an adversary's capability to exploit a vulnerability to execute a cyberattack on an organization.

Data

Software Weaknesses Dataset

The Software Weaknesses dataset consists of data from the CWE, which provides a common language for describing security weaknesses in software architecture, design, or code. It is an encyclopedia of hundreds of types of software weaknesses, including buffer overflow, directory traversal, operating system injection,

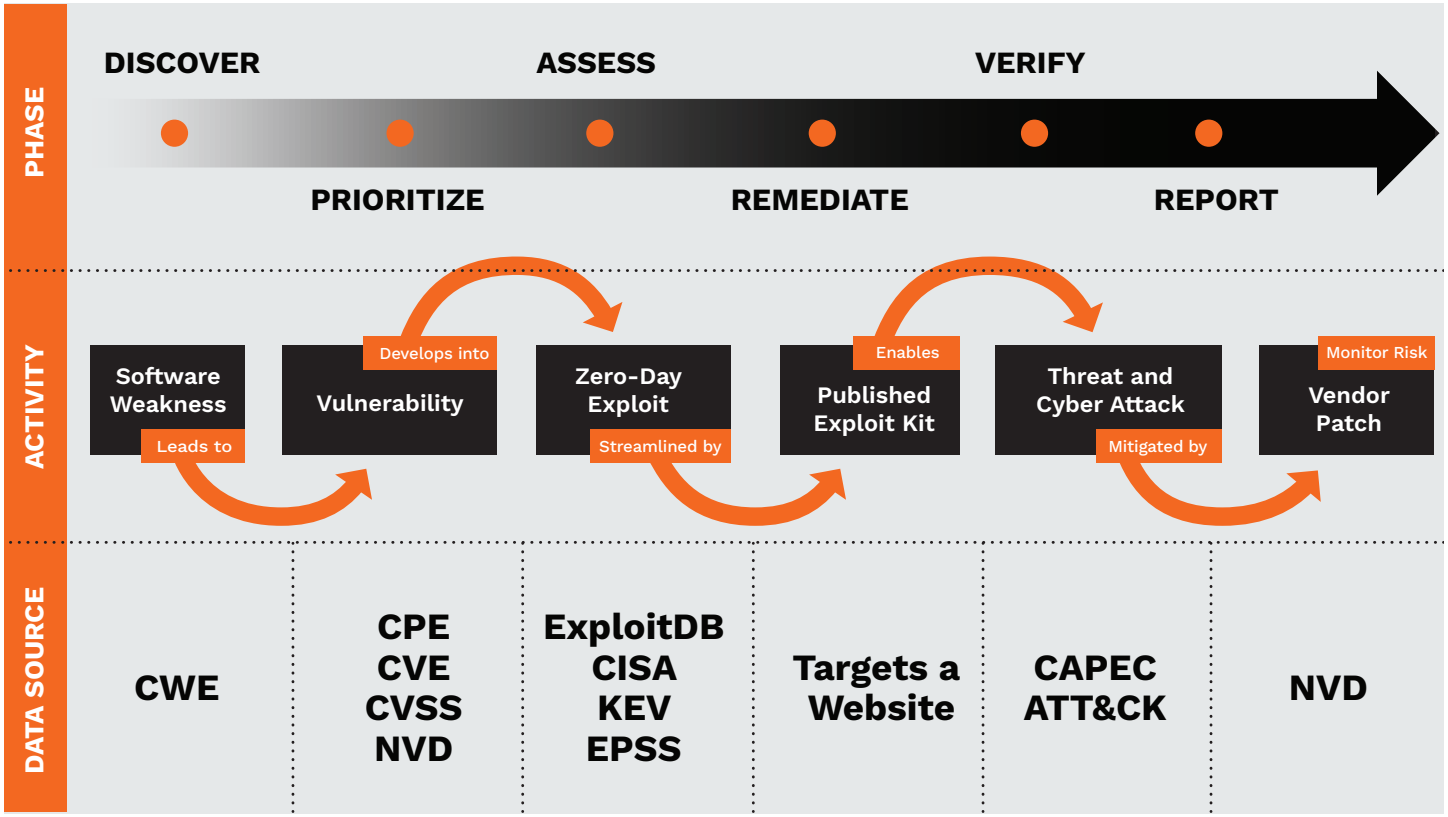


Figure 1. Software Vulnerability Life Cycle Phases and Their Relationships to Public Data Sources *(Source: McCoy [13]).*

race condition, cross-site scripting, hard-coded password, and insecure random numbers. Each software weakness has a technical impact, with eight that lead to failure: (1) read data, (2) modify data, (3–4) deny service - unreliable execution and resource consumption, (5) execute unauthorized code or commands, (6) gain privileges/ assume identity, (7) bypass protection mechanism, and (8) hide activities.

Vulnerability Dataset

The Vulnerability dataset is based on linking entries in the CVE with scoring information from the CVSS. The CVE is the authoritative source of publicly known vulnerabilities. The CVSS is an international standard for measuring the severity of a vulnerability. The CVSS base score is composed of metrics that reflect the intrinsic characteristics of the vulnerability. Each CVE entry includes a unique identifier (CVE number), a short free-text description, and a list of references for additional details of the vulnerability (in the form of URLs). This information is included in the dataset and linked with the CVSS base scores for the vulnerability.

Vendor Product Dataset

The Vendor Product dataset is based on the Common Platform Enumeration (CPE). Each entry (i.e., CPE-ID) defines a specific hardware device, operating system, or application software. Entries marked as deprecated are excluded, and the CPE-IDs of interest restricted to those are written in U.S. English. This dataset contains more than 15,000 CPE entries representing more than 3,000 products from ~200 vendors.

Attack Pattern Dataset

The Attack Patterns dataset includes 545 unique instances of CAPEC identifiers. CAPEC is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defense sponsored by the U.S. Department

of Homeland Security. A CAPEC identifier can be linked to the MITRE ATT&CK enterprise tactics, techniques, and subtechniques. ATT&CK provides a common taxonomy for both offense and defense and has become a standard across many cybersecurity disciplines to convey threat intelligence, perform testing through red teaming or adversary emulation, and improve network and system defenses against intrusions.

ExploitDB Database

ExploitDB is based on a one-to-many mapping between an identified exploit kit (ExploitDB) to the vulnerabilities that are the target of that exploit (CVE). It is updated daily and provided by MITRE. It is augmented with the data from the Cybersecurity and Infrastructure Security Agency's (CISA's) KEV and the EPSS. The CISA KEV provides real-time updates via email alerts when a newly identified CVE-ID is exploited. The EPSS model is based on observations of exploitation attempts against vulnerabilities and analysis of ancillary information about each of those vulnerabilities and then uses historical events to make predictions about future ones. The EPSS score associated with a CVE-ID represents the probability [0–1] of exploitation in the wild in the next 30 days (following score publication) and the percentile of the current score compared to all scored vulnerabilities with the same or lower EPSS score.

> ***ATT&CK provides a common taxonomy for both offense and defense and has become a standard across many cybersecurity disciplines.***

Adversary Tactics and Techniques Dataset

The combination of MITRE ATT&CK and CAPEC datasets forms the adversary Tactics and Techniques dataset. The MITRE ATT&CK matrices are focused on network defense and describe the operational phases in an adversary's life cycle. The matrices also detail the specific tactics, techniques, and procedures that advanced persistent threat (APT) groups use to execute their objectives while targeting, compromising, and operating inside a network. Attack patterns enumerated by CAPEC are employed by adversaries through specific techniques described by MITRE ATT&CK. The dataset is formed by linking the CAPEC attack patterns and related MITRE ATT&CK techniques together, enabling contextual understanding of the attack patterns within an adversary's operational life cycle.

Synthesizing Data Sources Into a Knowledge Graph

The datasets described in the "Data" subsection can be combined to form a knowledge graph. The purpose of this graph is to support queries to effectively rank vulnerabilities for mitigation. This organizational structure is needed as a wealth of information about what vulnerabilities are targeted, who exploits those vulnerabilities, and how they currently exist. However, this information is not organized into a structure that comprehensively defines the relationships among the datasets. The knowledge graph and its schema described in Figure 2 and Table 1 address this deficiency.

Leveraging the Knowledge Graph to Link Vulnerabilities to Sector-Specific Threat Actors

The knowledge graph enables linking the vulnerabilities to APTs that target sectors within and outside the United States. It describes what data processing is required to populate the knowledge graph and how it links the data together once populated.

Defining a Standard Set of Sectors

The critical infrastructure (CI) sectors denoted by the Department of Homeland Security (DHS) reflect assets, systems, and networks that are vital enough to the United States that when incapacitating or destroying them, it would have a debilitating effect on national security, economics, public health, or public safety [15]. Sectors can also be divided into subsectors [16]. The CI sectors and subsectors are

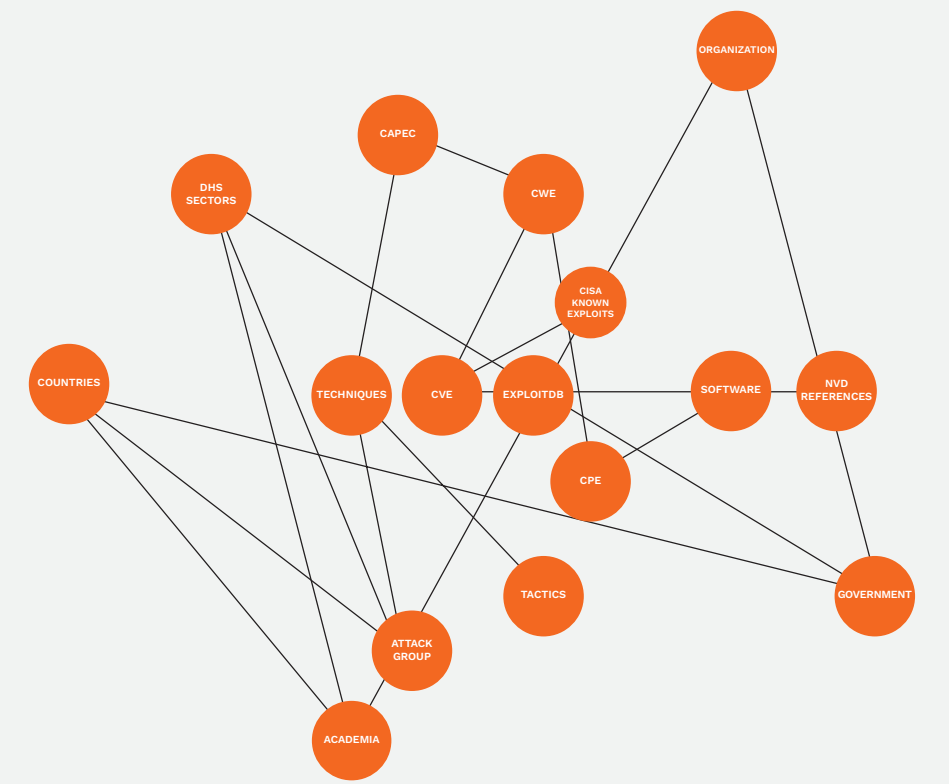


Figure 2. Graph Schema Representing the Entities of the Knowledge Graph and the Relationships Between Them *(Source: McCoy [13])*.

used to provide an affiliation for both threat actors and the organizations they target in the knowledge graph.

Defining Standard Locations

The knowledge graph requires a standard nomenclature to determine the country or region of origin for cyber threat actors and country of residence for organizations they target for attack. To meet this requirement, the U.S. State Department's list of independent states is leveraged. In this list, the term "independent state" refers to people politically organized into a sovereign state, with a definite territory recognized as independent by the United States.

Table 1. Legend for Node Labels and Relationships in Knowledge Graph Schema

LABEL	RELATIONSHIP	LABEL
NVD CVE	Reference exploit	ExploitDB
NVD CVE	Exploits known	CISA Exploit Catalog
NVD CVE	Weakened by	CWE
CWE	Known attack	CAPEC
CAPEC	Employs	Attack enterprise techniques
Attack groups	Achieves goal	Attack enterprise techniques
Attack groups	Originates	Countries
Attack groups	Targets	Countries
Attack groups	Focuses on	DHS sectors
Attack enterprise techniques	Achieved through	Attack enterprise techniques
NVD CVE	Affects	CPE
DHS sectors	Affiliated with	Organizations
Organizations	Operates in	Countries
Organizations	Installs	Software
Software	Has version	CPE
NVD CVE	Informs	NVD references

Assigning Attributes to Adversary Groups

APTs are an extension of nation-states' military forces because of the potential damages and chaos caused by successful critical infrastructure cyberattacks. MITRE keeps track of the APTs. Currently, it lists 129 threat groups [17] in their Enterprise Framework that can be associated with known techniques. Using their defined threat profiles, adversaries or threat groups employing the same tactics and techniques are identified.

Where Attacks Originate

For each APT group description provided by MITRE, natural language processing is used to extract keywords to determine the country or independent state from which the group operates. For example, a North Korean state-sponsored threat group would be assigned to North Korea with the mapping. The descriptions were also mined to determine year of origin (e.g., 2008) to ascertain each group's potential longevity. If a year was not explicitly stated in the description, the creation date of the MITRE description (e.g., has been active since at least 2009) was used.

Who Attacks Each Sector

Adversarial groups relevant to organizations based on who they target for attacks were identified next by mapping APTs and their country to DHS critical infrastructure sectors. To accomplish this, the subject of the term "targets," "targeted," or "targeting" was extracted in the group description from MITRE. The knowledge graph includes those where the United States is a targeted country, thus focusing on those attacks. The attribution of APTs to sectors is shown in Table 2. Note that some groups target more than one sector.

Relevance-Based Ranking Model

The goal here is to define an approach to cybersecurity vulnerability mitigation that improves upon rankings that employ strategies based on the global CVSS metrics associated with known software vulnerabilities published in the NVD. The outcome is a relevance-based ranking model that can be employed before an adversary takes advantage of a particular vulnerability. The model requires the following components:

For each APT group description provided by MITRE, natural language processing is used to extract keywords to determine the country or independent state from which the group operates.

Table 2. DHS Sectors Ranked by the Number of Attack Groups Targeting Those Sectors Based on Mentions in MITRE ATT&CK

SECTOR	GROUPS TARGETING
Government facilities	50
Information technology	33
Financial services	19
Healthcare and public health	17
Defense industrial base	14
Energy	14
Critical manufacturing	10
Communications	9
Transportation systems	7
Chemical	2
Water and wastewater systems	1
Nuclear reactors, materials, and waste	1
Emergency services	0
Dams	0
Commercial facilities	0
Food and agriculture	0

- Profiles that describe the organization under evaluation in terms of the DHS sector and country in which they operate.
- Collection and normalization of a complete software inventory for each organization.
- Threat-centric ranking policy definitions based on attack groups of interest and their skill levels.
- Scoring method for each ranking policy.

Creating Organizational Profiles

A vulnerability ranking policy needs to consider the installed software for the organization under evaluation. A representative set of organizations is identified and defined in government and education facilities to serve as organizational benchmarks for evaluating the vulnerability management approach.

Software Used in the Education Subsector

CollegeSimply [18] provides a list of Virginia colleges and sources public domain college data from the U.S. Department of Education National Center for Education Statistics. Using the list, six universities of varying sizes and funding sources (public and private) were chosen. The public universities were the University of Virginia (UVA), Virginia Tech (VT), Old Dominion University (ODU), and William & Mary University (W&M). The private universities were Regent University (REGENT) and Washington and Lee University (WLU). For each university, a published list of supported academic software was located on the university's website, and CPE-IDs were assigned to each piece of software. The full academic software listing is provided in McCoy [13]. A summary of the number of vulnerabilities found in the academic software associated with each university is shown in Table 3. A "size designation" (small [S], medium [M], large [L], and extra-large [XL]) was assigned based on the number of software products publicly listed. However, this did not reflect the size of the university or the number of software products used by the university.

Software Used by Government Facilities

Government facilities do not routinely publish the software they use. However, the "National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11" requires government agencies to purchase only commercial security products that have met specified third-party assurance requirements and have been tested by an accredited national laboratory [19]. The list of certified products is available at https://www.commoncriteriaportal.org/products/. In accordance with NSTISSP, the "Common Criteria" is an internationally recognized set of guidelines (International Organization for Standardization [ISO] 15408) that defines a common framework for evaluating security features and capabilities of information technology (IT) security products against functional and assurance requirements [20].

The Common Criteria was reduced to the set of products certified for use in the United States. CPE-IDs across all categories were then searched based on the vendor and product name. The software list shown in Table 4 consists of applications and operating systems. It was generated by randomly selecting software from the Common Criteria with assigned CPE-IDs in groups of 14, 24, 30, and 47 to approximately

Table 3. Academic Software Associated With Vendor Product CPE-ID

UNIT OF MEASURE	W&M	ODU	VT	REGENT	UVA	WLU
CPEs assigned	24	47	12	23	30	13
Software listed	33	69	22	31	49	23
Size designation	M	XL	S	M	L	S

Table 4. Government (GOV) Facility Software Associated With Vendor Product CPE-ID

NUMBER OF SOFTWARE PRODUCTS	GOV-S	GOV-M	GOV-L	GOV-XL
Software assigned	14	24	30	47
Common criteria	57	57	57	57

match the cardinality of the S, M, L, and XL university software lists.

Ranking Policy Definitions

Deciding which vulnerabilities to remediate is a daunting task. In a perfect world, all vulnerabilities would be remediated as they were discovered; unfortunately, this does not happen. An exploit observed in the wild is the most relevant proxy for the probability that an exposed vulnerability can be used to compromise an organization's network. To that end, the predictive ranking policies evaluated identify candidate vulnerabilities that fit the pattern of known attack groups. Formally, this is the intersection of vulnerabilities in the software used by an organization and vulnerabilities being actively targeted by threat actors.

> ***An exploit observed in the wild is the most relevant proxy for the probability that an exposed vulnerability can be used to compromise an organization's network.***

The criteria for the ranking policies using the attacker characteristics and targets is discussed in the "Synthesizing Data Sources Into a Knowledge Graph" subsection. Each policy leverages data points in the knowledge graph to provide a scoring methodology that considers the following:

- Which threat actors use the same technique to initiate an attack?
- Given an industry, which threat actors target it?
- Given a type of attack, which vulnerabilities does it exploit?
- At present day, what is the probability of exploit?
- Given an organization, which vulnerabilities are present in the installed software?

Four different ranking policies were created to answer these questions. Each policy prioritizes different information based on organizational information preferences regarding specific threats. The policies also include knowledge on whether an exploit for the CVE-ID has been observed.

- **Policy 1: CVSS Base Score Ranking –** Vulnerabilities are remediated based on the assigned CVSS base score ranking from most severe ("critical") to least severe ("low").
- **Policy 2: APT Threat Ranking –** Vulnerabilities are remediated based on the likelihood of present-day exploit and the existence of a technique employed by an attack group that targets the industry in the country where the organization operates.
- **Policy 3: Generalized Threat Ranking –** Vulnerabilities are remediated based on the likelihood of exploit by a low-skilled or highly-skilled adversary that has high impact on the organization.
- **Policy 4: Ideal Ranking –** The ideal ranking employs the same criteria as the APT and generalized threat rankings, Policies 2 and 3, but has the foreknowledge that a vulnerability has already been exploited using information from the ExploitDB and CISA KEV databases.

Ranking Policy Implementations

For each CVE-ID, 16 features using the cyberintelligence data sources are examined. The features, which inform each policy and create a set

of relevance scores for ranking CVE-IDs as they are published, are as follows: (1) CVE-ID, (2) CVSS base score metrics, (3) publication date, (4) modification date, (5) CAPEC-ID, (6) CAPEC skill level, (7) ATT&CK technique name, (8) MITRE ATT&CK group ID, (9) MITRE ATT&CK group country of operation, (10) risk appetite, (11) EPSS probability of exploit, (12) CISA known exploit catalog, (13) ExploitDB, (14) organization identifier, (15) critical infrastructure sector, and (16) organization's country of residence. The source code used in implementing the ranking policies is available in McCoy [21].

Based on the policy definitions, the CVSS V3.1 base score is the only feature needed to implement Policy 1. The features needed to implement Policy 2 and its ideal version in Policy 4 are listed in Table 5.

For Policies 2–4, a binary weighting [0,1] is used for each feature to determine its existence as applicable to a specific CVE-ID. The sum of the categorical values is presented as the relevance score to rank the associated CVE-IDs using the logic shown in the algorithm provided in McCoy [13]. The minimum assigned relevance score is set to 1 using this algorithm to avoid a long tail of nonrelevant CVE-IDs and ensure only relevant CVE-IDs associated with the organization's installed software are candidates for ranking.

When determining what to patch, the setup and business disruption costs must be considered and weighed against the potential exploitation cost and when and how often to patch an enterprise system or application decided. The total costs of a vulnerability are the sum of its direct costs (level of effort employed by human resources) and indirect costs (productivity losses and interruption of production processes after patching). Previous research has established that these costs can be measured in nonmonetary units based on the severity of the vulnerability where low = 0.25, medium = 1, high = 1.5, and critical = 3 units [22]. The economic cost of remediating vulnerabilities is evaluated using these established units.

EVALUATION AND RESULTS

Candidate Generation

In this study, 55,939 CVE-IDs published between 2019 and 2021 were used as the corpus from which to identify a much smaller subset of candidate vulnerabilities for ranking. The CVE modification date was used to simulate examining the vulnerabilities as they were published. A total of 3,079 unique CVE-IDs applied across all the government facilities and education subsector software lists. The data and source code used in this evaluation are available in McCoy [21].

Table 5. Policies 2 and 4 Scoring Features Using MITRE ATT&CK Data Feed to Characterize the Threat to the Organization

FEATURE	SPECIFIC THREAT RELEVANCE RANK	IDEAL RANK VALUE
CVSS base metric (attack vector)	Network	Network
DHS sector	Government facilities education	Government facilities education
Organization's country	United States	United States
Attack group's country	China, Russia, Iran	China, Russia, Iran
Risk appetite	[0, 100]	[0, 100]
EPSS probability	0.876	NA
CISA KEV or ExploitDB entry exists	NA	True
Software affected	True	True
Scoring range	[1–6]	[1–6]

For the government facilities shown in Table 6, low annual vulnerability counts for three of the four proxy organizations were less than 2% of all CVE-IDs analyzed. Even the largest government organization, GOV-XL, which was designed to mirror the breadth of software (i.e., 47 products) of its counterpart ODU in the education subsector, experienced less than 4% of all CVE-IDs analyzed. The low number of vulnerabilities in the sector may be attributed to the selection process for software products assigned to government facilities in this study, which were selected exclusively from the certified product list approved by the Common Criteria [19]. This outcome may provide an indication that the rigor imposed upon these products in terms of security requirements and ongoing evaluation may potentially reduce their exposure to published vulnerabilities.

For the education subsector shown in Table 7 vulnerability counts of less than 2% were observed for organizations with small amounts of reported software, such as VT and WLU. Conversely, it was noted that universities who reported more software in use such as ODU, REGENT, and WM need to evaluate hundreds of vulnerabilities as candidates for remediation during any given year.

Figures 3 and 4 show the accumulated vulnerabilities by month and year for each organization in this study. It is important to note the unpredictable way newly published and modified CVE-IDs can present themselves for analysis and remediation to an organization. Similarly, Tables 8 and 9 show the vulnerabilities for the government and education subsectors. Note that WM, ODU, and REGENT experienced a steady stream of vulnerabilities across all three years of this study. They also experienced an increase in the number of weeks per year during which a continuous remediation policy would be advantageous. For ODU, note an increase from 42 weeks per year in 2019 to 50 weeks per year in 2021.

Normalized, Discounted Cumulative Gain

Within the field of cybersecurity,

Table 6. Total Vulnerabilities by Year for Government (GOV) Facilities Sector

YEAR	GOV-S	GOV-M	GOV-L	GOV-XL
2019	8	41	51	102
2020	11	34	55	144
2021	16	84	140	285
Total vulnerabilities	35	159	246	531
Percentage of all vulnerabilities	0.25%	1.15%	1.77%	3.85%

Table 7. Total Vulnerabilities by Year for Education Subsector

YEAR	VT	WLU	REGENT	WM	UVA	ODU
2019	14	3	1,396	1,370	188	1,457
2020	6	57	565	556	279	751
2021	15	144	1,721	1,704	639	2,026
Total vulnerabilities	35	204	3,682	3,630	1,106	4,234
Percentage of all vulnerabilities	0.25%	1.45%	26.56%	26.19%	7.98%	30.54%

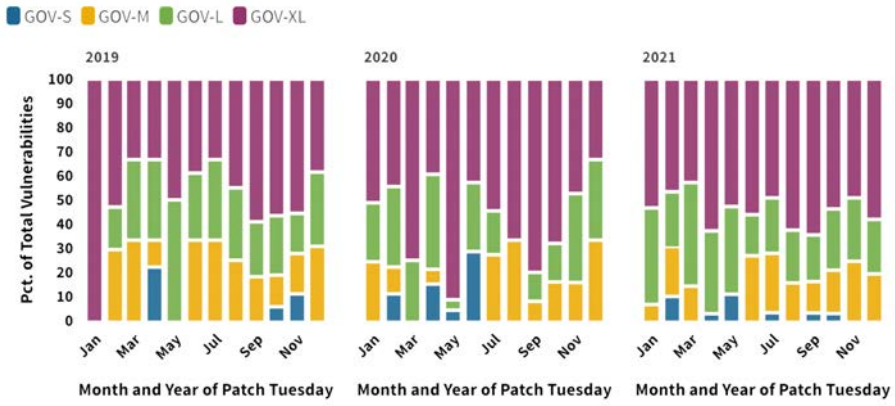


Figure 3. Vulnerabilities by Month and Year for CVE-IDs Between 2019 and 2021 for the Government Facilities Sector *(Source: McCoy [13])*.

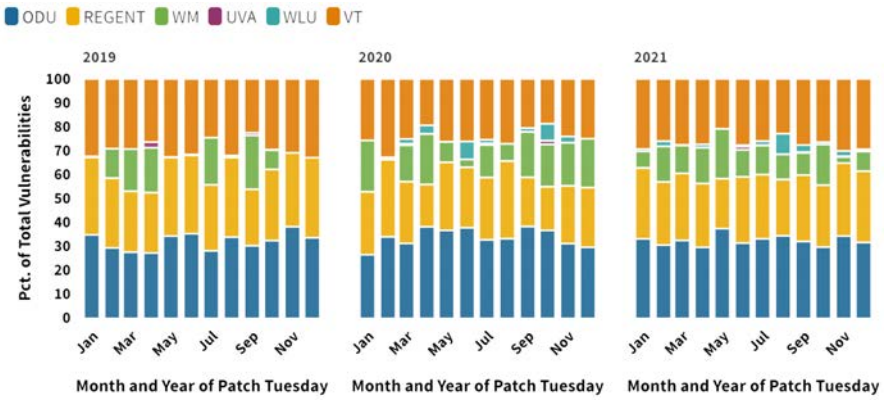


Figure 4. Vulnerabilities by Month and Year for CVE-IDs Between 2019 and 2021 for the Education Sector *(Source: McCoy [13])*.

Table 8. Weekly Vulnerability Traffic by Year for the Government (GOV) Facilities Subsector

AVERAGE VULNERABILITY			MINIMUM VULNERABILITY	MAXIMUM VULNERABILITY	WEEKS
Year	Organization	Per Week	Per Week	Per Week	Per Year
2019	GOV-S	4	1	20	32
2019	GOV-M	3	1	9	24
2019	GOV-L	2	1	4	23
2019	GOV-XL	2	1	2	5
2020	GOV-S	4	1	13	40
2020	GOV-M	3	1	10	23
2020	GOV-L	3	1	10	16
2020	GOV-XL	2	1	3	6
2021	GOV-S	7	1	25	43
2021	GOV-M	4	1	14	40
2021	GOV-L	3	1	11	29
2021	GOV-XL	2	1	3	10

> ***Within the field of cybersecurity, there is no consensus approach for measuring, testing, and comparing the accuracy of a ranking model.***

there is no consensus approach for measuring, testing, and comparing the accuracy of a ranking model. Therefore, this research, like others discussed in the "Discussion" section, builds upon measurements derived from the information retrieval (IR) field. Evaluation measures for IR assess how well the search results from a recommender satisfy a given query. Specifically, recommender systems use the nDCG [23] score to evaluate the ranking of items (e.g., individual vulnerabilities) in a collection (e.g., NVD).

The nDCG varies from 0.0 to 1.0, with 1.0 representing the ideal ranking order. The nDCG is commonly used to evaluate search engine result pages (SERPs), where the position of an entry indicates its search result relevance. Higher ranked pages are more likely to gain the consumer's attention. The same approach is applied toward creating a ranking list for patching vulnerabilities. Order is important to ensure higher ranked CVE-IDs are considered first. The main difficulty encountered when using nDCG is

Table 9. Weekly Vulnerability Traffic by Year for the Education Subsector

AVERAGE VULNERABILITY			MINIMUM VULNERABILITY	MAXIMUM VULNERABILITY	WEEKS
Year	Organization	Per Week	Per Week	Per Week	Per Year
2019	WM	2	1	4	7
2019	ODU	1	1	1	3
2019	REGENT	35	1	442	40
2019	UVA	43	1	441	32
2019	VT	11	1	44	18
2019	WLU	35	1	444	42
2020	ODU	1	1	1	6
2020	REGENT	5	1	20	12
2020	WM	15	1	57	40
2020	UVA	15	1	58	39
2020	WLU	9	1	34	33
2020	VT	18	1	59	43
2021	ODU	3	1	4	7
2021	REGENT	7	1	23	21
2021	WM	36	1	264	48
2021	UVA	36	1	258	48
2021	WLU	15	1	120	43
2021	VT	41	1	315	50

the availability of an ideal ordering of results when feedback (e.g., human judgment) is unavailable. This shortcoming was faced by SERPS with Policy 4, introduced in the "Ranking Policy Implementations" subsection as a data-driven proxy of an ideal ordering of vulnerabilities.

To compare the results of rankings between each relevance policy and the ideal ranking (Policy 4), the nDCG of each CVE-ID for every organizational interaction was calculated with the ranking system. The nDCG values were averaged for each weekly collection of CVE-IDs to obtain a measure of the average performance of the ranking algorithms. The application of nDCG in this study is interpreted as follows:

1. "G" is for gain – it corresponds to the magnitude of each vulnerability's relevance.
2. "C" is for cumulative – it refers to the cumulative gain, or summed total, of every vulnerability's relevance score.
3. "D" is for discounted – it divides each vulnerability's scored relevance by the scored relevance of the associated ideal policy to reflect the goal of having the most relevant vulnerabilities ranked toward the top of the mitigation lists.
4. "n" is for normalized – it divides discounted cumulative gain (DCG) scores by ideal DCG scores calculated for a ground truth data set, as represented by the relevance scores and ranking resulting from the ideal policy (i.e., Policy 4), which used foreknowledge of exploited vulnerabilities contained within historical ExploitDB and CISA KEV intrusion detection reports.

Once the relevance value is computed for each CVE-ID, each entry is ranked based on the relevance value and the nDCG is computed using the following formulas:

$$DCG_k = \sum_{i=1}^{k} \frac{2^{rel_i - 1}}{\log_2(i+1)} . \quad (1)$$

The cumulative gain at K is the sum of gains of the first K items recommended. *iDCGk* is the maximum possible (ideal) *DCG* for a given set of queries, vulnerabilities, and relevance scores.

$$nDCG_k = \frac{DCG_k}{iDCG_k} . \quad (2)$$

The chart in Figure 5 illustrates the average values of nDCG for each position K based on weekly vulnerability collections. K reflects the number of CVE-IDs to remediate. The number of observations ranges from 383 when K = 1 to 16 when K = 100.

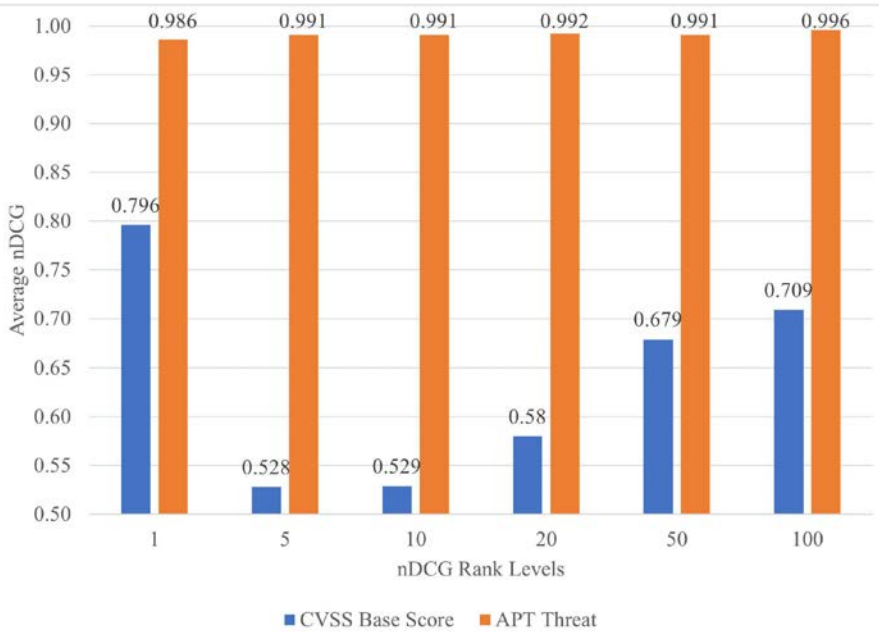


Figure 5. Average Value of nDCG at Different Rank Levels (K) for CVSS Base Score vs. APT Threat Policy for the ODU, REGENT, and WM Organizations *(Source: McCoy [13])*.

The x-axis reports the rank (from 1 to 100), while the y-axis displays the respective value of nDCG@K. Figure 5 shows that the CVSS base score performs moderately well at the ends of the spectrum when K = 1 and K = 100. However, the performance decreases when $5 \leq K \leq 50$. Policy 2 is not impacted by the number of weekly CVE-IDs; it performs at a consistent level regardless of the number of CVE-IDs encountered.

Testing and Evaluating the Policies

Within the evaluation, the number of CVE-IDs to be evaluated each week can vary for each organization. Therefore, to calculate nDCG, the cumulative gain needs to be normalized at each ranking position for a chosen number of vulnerabilities. Tables 8 and 9 show that the average weekly vulnerability traffic across all organizations establishes a natural threshold of 20 CVE-IDs during a given week as the minimum number needed to apply a relevance ranking policy.

The GOV-XL, ODU, REGENT, UVA, WLU, and WM organizations consistently met this threshold. However, GOV-XL, UVA, and WLU were excluded from further examination in this section, as there were numerous weeks where no published CVE-IDs applied to the organization's installed software.

For the remaining organizations with more than 50 weekly observations (ODU, REGENT, and WM), the necessary features were collected using the cyberintelligence data sources identified in the "Data" subsection to compute a relevance score, rank the CVE-IDs, and calculate nDCG using Policy 4 as the ideal ranking. Only the CVSS V3.1 base score was needed to evaluate Policy 1. For all ranking policies, the set of applicable CVE-IDs was ranked in descending order by relevance score and then subsequently ordered by CVE-ID to avoid ties. The performance of Policy 1 was evaluated against the threat-centric policies (Policies 2 and 3). Finally, the patch cost (in nonmonetary units) for the top 20 CVE-IDs was determined, where low = 0.25, medium = 1, high = 1.50, and critical = 3.00 [22].

Measuring Ranking Quality

For the threat-centric policies (Policies 2 and 3), the average performance was measured across all three years of the evaluation period using nDCG@20. China was chosen as the APT group of interest for vulnerabilities impacting ODU, REGENT, and WM since it contained the most frequent origin of APT threats against the United States [24].

The nDCG is measured on a scale of 0.0 to 1.0, and a score of 1.0 indicates the ideal ranking order has been achieved. The goal is to obtain an nDCG score close to 1.0 for each threat policy. Table 10 shows the average nDCG@20 for each organization. The average nDCG@20 of 0.99 indicates Policy 2 performs better than Policy 1. The average

Table 10. Average Performance of Policy 1 vs. Policy 2, Where China Is the Source Region of Interest (nDCG@20)

SCHOOL	YEAR	CVSS BASE SCORE	APT THREAT CHINA	AVG. DIFF. IN nDCG	KNOWN EXPLOITS
ODU	2019	0.601	0.996	0.394	4
ODU	2020	0.557	0.998	0.441	2
ODU	2021	0.571	0.986	0.415	12
REGENT	2019	0.592	0.999	0.407	2
REGENT	2020	0.557	0.998	0.441	1
REGENT	2021	0.585	0.985	0.399	12
WM	2019	0.598	0.998	0.400	3
WM	2020	0.565	0.998	0.433	1
WM	2021	0.585	0.985	0.399	12

difference in nDCG@20 of 0.41 indicates that Policy 2 performs 71.5% better than Policy 1 as an indicator of vulnerabilities that might be targeted by an APT group.

In the results, the nDCG@20 measures for Policy 1 were in the range of [0.343, 1], as shown in Figure 6. Lower values for nDCG@20 were observed with Policy 1 when the number of vulnerabilities collected exceeded the minimum threshold (i.e., 20) by more than 1,000% (e.g., 200+). Higher nDCG@20 values were observed when the number of vulnerabilities were closer to the threshold (e.g., 20 to 30). Policy 2 was minimally impacted by the number of vulnerabilities and was in the range of [0.878, 1].

Table 11 shows similar results for Policy 3. The average difference in nDCG@20 of 0.35 indicates Policy 3 performs 91.3% better than Policy 1 as an indicator of vulnerabilities that might be targeted by a highly skilled cyber threat actor. This is highlighted as well in Figure 7.

Using all the weekly observations (n = 163) across organizations, a paired t-test was performed to compare the mean of the nDCG for Policy 1 against Policy 2 [25]. Results of this test indicated that there was a significantly large difference between Policy 1 [mean = 0.58, STDEV = 0.1] and Policy 2 [mean = 0.992, STDEV = 0.02], and the p-value equaled 0. The Policy 2 population's nDCG@20 average was greater than the Policy 1 population's average, and the difference

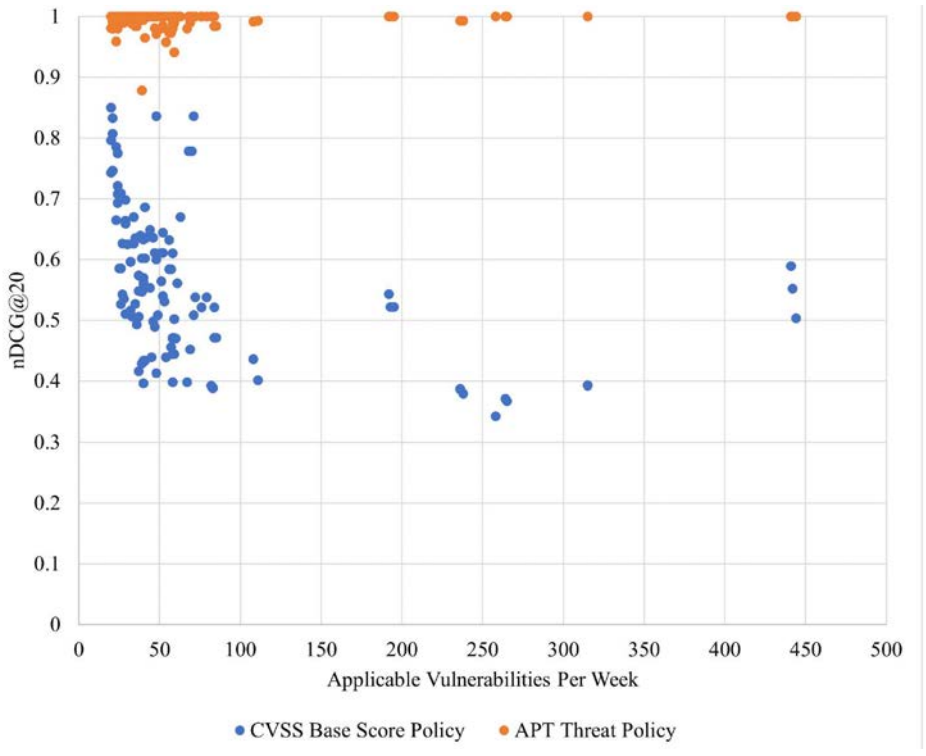


Figure 6. nDCG@20 for Policy 1 vs. Policy 2 for the ODU, REGENT, and WM Organizations *(Source: McCoy [13])*.

Table 11. Average Performance of Policy 1 vs. Policy 3, With a Highly Skilled Adversary (nDCG@20)

SCHOOL	YEAR	CVSS BASE SCORE	GENERAL THREAT HIGHLY SKILLED	AVG. DIFF. IN nDCG	KNOWN EXPLOITS
ODU	2019	0.543	0.988	0.444	4
ODU	2020	0.548	0.998	0.450	2
ODU	2021	0.474	0.986	0.511	12
REGENT	2019	0.528	0.995	0.467	2
REGENT	2020	0.512	0.999	0.487	1
REGENT	2021	0.500	0.984	0.484	12
WM	2019	0.538	0.992	0.454	3
WM	2020	0.520	0.999	0.478	1
WM	2021	0.499	0.984	0.485	12

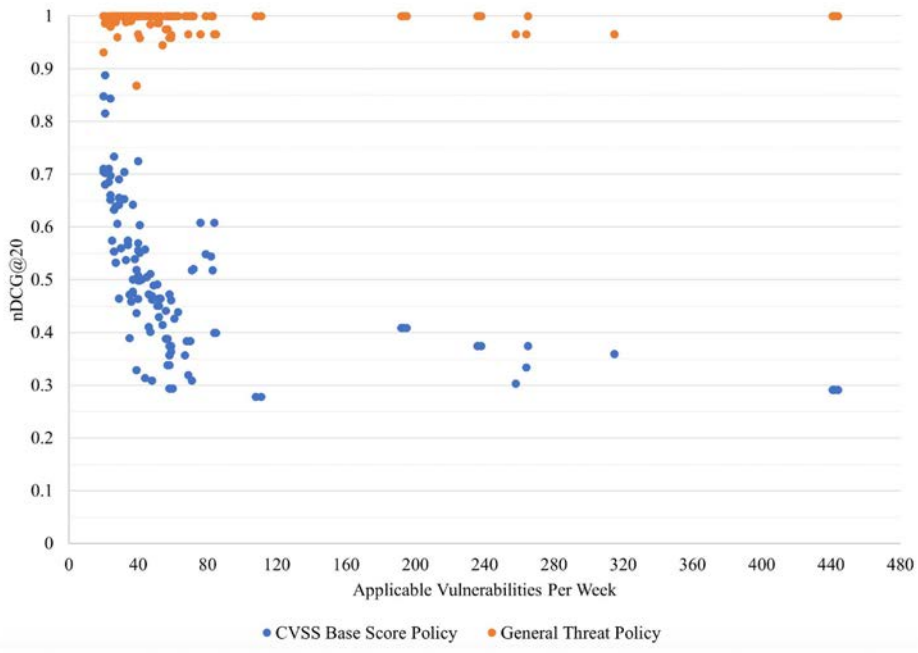


Figure 7. nDCG@20 for the Policy 1 vs. Policy 3 for the ODU, REGENT, and WM Organizations *(Source: McCoy [13])*.

was large enough to be statistically significant.

A similar test to compare the mean of the nDCG for Policy 1 against Policy 3 was performed. Results of the paired t-test indicated that there was a significantly large difference between Policy 1 [mean = 0.512, STDEV = 0.139] and Policy 3 [mean = 0.99, STDEV = 0.022], and the p-value equaled 0. The Policy 3 population's average nDCG@20 was greater than the Policy 1 population's average, and the difference was large enough to be statistically significant.

These results showed that CVSS base score metrics did not contain a data element or scoring component that allowed enumeration of a specific threat. The paired t-test indicated that the difference in the recommended ranking positions of CVE-IDs between policies was statistically significant (p-value equaled 0). Therefore, any relevance ranking based solely on the CVSS base score would fall short of the organization's specified goals. These results also provided another indication that the severity of a vulnerability, as measured by its CVSS base score, might not be the optimal ranking approach for every organization.

Cost of Patch Prioritization

Past research has shown that organizations cannot fix all their known vulnerabilities. Instead, they can fix 5%–20% of known vulnerabilities per month [26]. Here, the annualized cost of remediating the top 20 vulnerabilities produced by the different ranking Policies 1–3 was examined. Defined by Fruhwirth et al., the nonmonetary units were used

with patching [22]. The results of this analysis are shown in Table 12. In all cases, there is a decreased average cost of 23.3% when Policy 2 is used for prioritizing CVE-IDs for remediation. Specifically, Policy 2 realizes decreases 498 units for ODU, 390.5 units for REGENT, and 455.75 units for WM over the three-year evaluation period when compared to Policy 1.

Table 13 shows increased savings in patch costs using Policy 3. The cost of patching remains the same across all organizations using the CVSS base score. However, for each organization, there are additional savings over using Policy 2. Decreases of 548.25 units for ODU, 500.75 units for REGENT, and 499.75 for WM represent an average 25.6% improvement over the CVSS base score approach. Policy 2 only provided a 23.3% improvement.

Using all the weekly observations (n = 163) across organizations, a paired t-test was performed to compare the mean of the patch costs for Policy 1 against Policy 2 [25]. Results of this test indicated that there was a significantly large difference between Policy 1 [mean = 37.025, STDEV = 10.291] and Policy 2 [mean = 28.362, STDEV = 5.475], and the p-value = 7.45e-27. The population of Policy 2's average patch cost was less than Policy 1's, and the difference was large enough to be statistically significant.

Similarly, a paired t-test to compare the mean of the patch costs for Policy 1 against Policy 3 was performed [25]. Results of this test indicated that there was a significantly large difference between Policy 1 [mean = 37.025,

Table 12. Difference in the Cost of Patching the Top 20 CVE-IDs for Policy 1 vs. Policy 2, Where China Is the Source Region of Interest

SCHOOL	YEAR	CVSS BASE SCORE	APT THREAT CHINA	AVERAGE SAVINGS
ODU	2019	631.50	449.25	185.25
ODU	2020	531.00	439.00	92.00
ODU	2021	994.50	770.00	244.50
REGENT	2019	604.75	422.25	182.50
REGENT	2020	375.50	308.50	67.00
REGENT	2021	960.00	752.00	208.00
WM	2019	603.75	424.75	179.00
WM	2020	374.00	308.50	65.50
WM	2021	960.00	748.75	211.25

Table 13. Difference in the Cost of Patching the Top 20 CVE-IDs for Policy 1 vs. Policy 3 From a Highly Skilled Adversary

SCHOOL	YEAR	CVSS BASE SCORE	GENERAL THREAT COST	AVERAGE SAVINGS
ODU	2019	631.50	438.50	193.00
ODU	2020	531.00	424.50	106.50
ODU	2021	994.50	745.75	248.75
REGENT	2019	604.75	412.00	192.75
REGENT	2020	375.50	294.50	81.00
REGENT	2021	960.00	733.00	227.00
WM	2019	603.75	412.50	191.25
WM	2020	374.00	296.50	77.50
WM	2021	960.00	729.00	231.00

STDEV = 10.291] and Policy 3 [mean = 27.523, STDEV = 4.905], and the p-value = 9.989e-30. The population of Policy 3's average patch cost was less than Policy 1's, and the difference was large enough to be statistically significant.

Predicting Exploits

Only a small subset (2%–7%) of published vulnerabilities are exploited in the wild [26]. Given that such a small number of CVE-IDs are exploited, it is advantageous for organizations to leverage as much insight as possible to identify potential threats. How Policy 2 can be used to prioritize a vulnerability with a known exploit is demonstrated here. The ODU organization identified 39 CVE-IDs to mitigate during the week of 23 November 2021.

In this case study, the top 20 are ranked according to Policy 2, as shown in Table 14. Note that three CVE-IDs in this group, CVE-2021-38000, CVE-2021-30632, and CVE-2021-30633, have known exploits. The CISA known exploits entry for CVE-2021-38000, which impacts Google Chrome, is shown in Figure 8. The entries in Table 14 show that all three CVE-IDs are identified as relevant using Policy 2. However, CVE-2021-38000 is ranked at position 29 using Policy 1 based on its CVSS base score of 6.1 (medium severity). This highlights that when using Policy 1, CVE-2021-38000 falls outside the top-20 range for remediation by IT administrators at ODU. In contrast, Policy 2 elevates this CVE-ID to position no. 3 because of its high relevance score.

Table 14. Application of Ranking Policies by ODU for Vulnerabilities Published During the Week of 23 November 2021 (Known Exploits Are Bolded and Highlighted in Grey)

CVE-ID	CVSS BASE SCORE	RELEVANCE SCORE	POLICY 1 RANK	POLICY 2 RANK	EXPLOIT
CVE-2021-37966	4.3	6	34	1	—
CVE-2021-37999	6.1	6	28	2	—
CVE-2021-38000	**6.1**	**6**	**29**	**3**	**Yes**
CVE-2021-30542	8.8	2	5	4	—
CVE-2021-30543	8.8	2	6	5	—
CVE-2021-30626	8.8	2	7	6	—
CVE-2021-30627	8.8	2	8	7	—
CVE-2021-30628	8.8	2	9	8	—
CVE-2021-30629	8.8	2	10	9	—
CVE-2021-30630	4.3	2	31	10	—
CVE-2021-30632	**8.8**	**2**	**11**	**11**	**Yes**
CVE-2021-30633	**9.6**	**2**	**2**	**12**	**Yes**
CVE-2021-34423	9.8	2	1	13	—
CVE-2021-34424	7.5	2	26	14	—
CVE-2021-37956	8.8	2	12	15	—
CVE-2021-37957	8.8	2	13	16	—
CVE-2021-37958	5.4	2	30	17	—
CVE-2021-37959	8.8	2	14	18	—
CVE-2021-37961	8.8	2	15	19	—
CVE-2021-37962	8.8	2	16	20	—

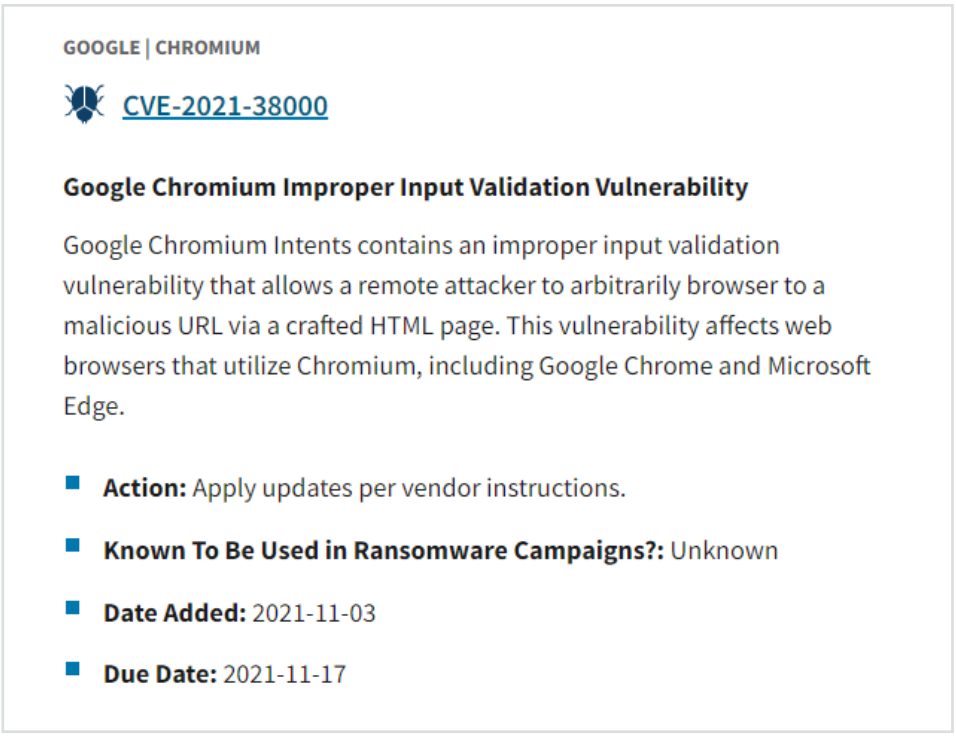


Figure 8. ACISA Known Exploits Catalog Entry for CVE-2021-38000 *(Source: CISA [27])*.

DISCUSSION

There is a myriad of existing research that falls within the scope of this work. Related research is discussed, limitations of the work identified, and provided contributions highlighted.

Related Research

Multiple researchers have created ontologies to represent the cybersecurity domain by aggregating multiple sources of information [28–33]. This work provides the foundation for building automated tools, which reduce the scope, complexity, and volume of security data that must be managed by security professionals leveraged in this approach. However, this research differs from these efforts in that more information and sources are extracted to achieve completeness in the knowledge graph. In addition, categorization is a necessary precursor to the ranking policies for vulnerability management. Multiple research efforts have shown that identifying and categorizing additional metadata about vulnerabilities, exploits, attacks, and targets can be beneficial [22, 34–36]. More recently, applying text mining to extra additional data about these entities has led to models which predict the severity of a vulnerability using only text-based data [37–40].

Even with an organized understanding of the cyber threat domain, understanding how to minimize the cost of managing and protecting information assets is a challenge. A core component of this challenge is adopting a vulnerability management process that can detect and remediate known vulnerabilities [12]. A common approach is to remediate all vulnerabilities above a certain severity score. However, this approach has been found to be suboptimal [41] and, in some cases, no better than randomly choosing vulnerabilities to remediate [42]. Furthermore, in many cases, it is infeasible to patch all the CVEs with the highest CVSS base scores due to the time and resources required for remediation actions. This is because 13.5% of the NVD vulnerabilities are scored between 9 and 10 [43].

This has led to extensive work in evaluating if the CVSS score can be a good predictor for vulnerability exploitation [44] and whether it can be improved by additional information [45–47]. Machine-learning approaches have been explored [48, 37] as well as exploit prediction models that leverage data from online sources generated by the white-hat community (i.e., ethical hackers) [39]. Vulnerability exploitation can also be modeled as a transition between system states [49–55]. However, these graphs often tend to be unwieldy as network size grows, making the identification of realistic paths to compromise difficult to achieve [56]. Customized and target specific ranking approaches also exist [43, 12, 57, 42]. However, these approaches assume the existence of site-specific threat intelligence information.

Contributions of the Approach

Prior research has demonstrated the ability to examine adversary capabilities and vulnerability management and exploit prediction at a particular point in time or with isolated threat scenarios. However, little research has been done to create an end-to-end prioritization approach that encompasses the entire vulnerability management life cycle. This gap is addressed by the following:

- Extracting dozens of essential features about the vulnerability, including its potential for harm, the degree to which it is exploitable, and how frequently the vulnerability is targeted by adversaries.
- Leveraging the ability of property graphs to offer a flexible schema where attributes can be added to extend the data model, creating hierarchies with different levels of granularity, and combining multiple dimensions to better manage big data.
- Performing an assessment of current and predicted future attacker activity based on known tactics and techniques.
- Correlating threat and exploit intelligence from publicly available authoritative sources.
- Devising an approach to convert raw data about threat indicators into contextual risk scores.
- Identifying how important the affected asset is to an organization in any industry.
- Inferring indirect facts and hidden relationships, which can further inform the results.

Parsing real-time, open-source cyber threat intelligence data cannot be accomplished by a human analyst. Therefore, its correlation and analysis are automated using a knowledge graph. Application programming interfaces (APIs) and data feeds maintained by the National Institute of Standards & Technology (NIST) can also be leveraged to provide awareness of the changing threat landscape while allowing dynamic and continuous assessment of the underlying network architecture. This research provides benefits to organizations seeking to create high-level strategies to examine cybersecurity posture in a manner that is predictive and not just reactive.

Known Limitations

This work is not without limitations. To apply the approach here, organizations must have a methodology to accurately construct a software inventory that can be correlated with an entry in the CPE database. Vulnerabilities cannot be allocated without a CPE-ID, and low fidelity inventory reporting may result in residual cyber risk. The relevance ranking policies identified can only be effectively applied to a known software architecture. Furthermore, it is important to note that the attack group list in MITRE ATT&CK is not all encompassing. A Google search will identify emerging APT groups that are not included in the MITRE's enterprise matrices. In addition, the proof-of-concept code entries collected via ExploitDB do not include a time component indicating when the POC entry was made. As a result, it is not possible to discretely link the CVE-ID's publication or modification date with the subsequent appearance of an intrusion report. The inclusion of a timestamp would have allowed evaluating the predictive portion of the policies based on a timeline of events. The approach here is naive regarding exploitation and does not consider the publication date for exploit code maturity using ExploitDB. The ExploitDB to CVE mapping webpage is also not well covered in the internet archives.

Time lapse dynamics related to data sources also exist. The EPSS probability scores and percentiles are dynamic and should be collected near the time of the CVE publication date. To maintain consistency in the

> ***Vulnerabilities cannot be allocated without a CPE-ID, and low fidelity inventory reporting may result in residual cyber risk.***

dataset, all cyberintelligence data was collected and frozen for analysis as of 31 December 2021. Future work can utilize the API provided by the EPSS team to dynamically collect the scores and percentiles in real-time. This is a candidate for future work. Finally, the prescribed optimum ordering approach may not ease patch hesitancy or prevent a culture of "wait and see" regarding patching vulnerabilities. The policies also cannot control the quality of vendor patch distributions on Patch Tuesday that, in some cases, can lead to recalls later in the month. These scenarios are outside the scope of this research. However, the ranking policies here can reduce the amount of unnecessary work spent patching CVE-IDs that are neither applicable nor associated with a known cyber threat actor.

CONCLUSIONS

The process of tracking and remediating vulnerabilities is relentless. The key challenge is trying to identify a remediation scheme specific to in-house, organizational objectives. Without a strategy, the result is a patchwork of fixes applied to a tide of vulnerabilities, any one of which could be the point of failure in an otherwise formidable defense. The goal of this research is to demonstrate that aggregating and synthesizing readily accessible, public data sources to provide personalized, automated recommendations for organizations to prioritize their vulnerability management strategy will offer significant improvements over the current state-of-the art solutions. Results showed an average 71.5%–91.3% improvement toward identifying vulnerabilities likely to be targeted and exploited by cyber threat actors. The ROI of patching using the policies results in a savings in the 23.3%–25.5% range for annualized costs. A paired t-test demonstrates these findings are statistically significant and offer an improvement over the industry standard approach to vulnerability management.

Overall, the relevance ranking strategy described in this study emphasizes the capability of threat-centric scenarios for ranking and prioritizing vulnerabilities with due consideration to the threat environment. A network defender, who typically must address thousands of exposed vulnerabilities, can spend fewer resources to patch more vulnerabilities that are much more likely to be exploited and of interest to a specific set of cyber threat actors. The automated data aggregation within the knowledge graph allows the user to submit queries to identify new vulnerabilities that affect the most important software and servers. This ability to differentiate among vulnerabilities and how they might be targeted by an adversary enhances the state of the art in vulnerability management.

NOTE

This work was unfunded and performed as part of Corren McCoy's Ph.D. work at ODU in Norfolk, VA. ■

REFERENCES

[1] Sheyner, O., J. Haines, S. Jha, R. Lippmann, and J. M. Wing (editors). "Automated Generation and Analysis of Attack Graphs." Proceedings of the 2002 IEEE Symposium on Security and Privacy, 2002.

[2] Krebs, C. C. "Emergency Directive 20-03 (ED 20-03), Mitigate Windows DNS Server Vulnerability From July 2020 Patch Tuesday." https://www.cisa.gov/news-events/directives/ed-20-03-mitigate-windows-dns-server-remote-code-execution-vulnerability-july-2020-patch-tuesday, 2020.

[3] Coble, S. "CISA Issues Emergency Vulnerability Warning." https://www.infosecurity-magazine.com/news/cisa-issues-emergency/, 2020.

[4] Dulaunoy, A. "CVE-Search Vulnerability Lookup." Social media post, *Mastodon*, https://infosec.exchange/@adulau/112013472555767369, 2024.

[5] Wikipedia. "Patch Tuesday." https://en.wikipedia.org/wiki/Patch_Tuesday, 2020.

[6] Schmeidler, N. "Microsoft Patch Tuesday: All or Nothing Patches." https://blog.morphisec.com/microsoft-patch-tuesday-all-or-nothing-patching, 2016.

[7] O'Donnell, L. "Microsoft Pulls Bad Windows Update After Patch Tuesday Headaches." https://threatpost.com/microsoft-windows-update-patch-tuesday/163981/, 2021.

[8] Foreman, P. "Vulnerability Management: Taylor and Francis Group," 2010.

[9] Forum of Incident Response and Security Teams (FIRST). "Exploit Prediction Scoring System v2022.01.01." https://www.first.org/epss/, 2022.

[10] Romanosky, S., and J. Jacobs. "Probability, Percentiles, and Binning – How to Understand and Interpret EPSS Scores." FIRST, https://www.first.org/epss/articles/prob_percentile_bins, 2022.

[11] Mell, P., K. Scarfone, and S. Romanosky (editors). "A Complete Guide to the Common Vulnerability Scoring System Version 2.0." FIRST-Forum of Incident Response and Security Teams, 2007.

[12] Allodi, L., and F. Massacci. "Comparing Vulnerability Severity and Exploits Using Case-Control Studies." *ACM Transactions on Information and System Security* (*TISSEC*), vol. 17, no. 1, pp. 1–20, 2014.

[13] McCoy, C. G. "A Relevance Model for Threat-Centric Ranking of Cybersecurity Vulnerabilities." Ph.D. dissertation, Old Dominion University, Norfolk, VA, 2022.

[14] NIST. "National Vulnerability Database. https://nvd.nist.gov/, 16 November 2022.

[15] CISA. "Critical Infrastructure Sectors." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors, 2020.

[16] Commission USEA. "CI Scoop: What Are Sectors and Sub-Sectors?" https://web.archive.org/web/20181105225720/https://www.eac.gov/ci-scoop-what-are-sectors-and-sub-sectors/, 2017.

[17] Infoblox. "An Introduction to MITRE ATT&CK." https://blogs.infoblox.com/security/an-introduction-to-mitre-attck/, 2019.

[18] CollegeSimply. "Virginia Colleges Ranked by Largest Enrollment." https://www.collegesimply.com/colleges/rank/colleges/largest-enrollment/state/virginia/, 2021.

[19] CNSS. "National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11." https://www.hsdl.org/?view&did=487791, 2003.

[20] ISO. "Information Technology — Security Techniques — Evaluation Criteria for IT Security — Part 1: Introduction and General Model." https://www.iso.org/standard/50341.html, 2022.

[21] McCoy, C. "oduwsdl/CyberThreatRelevanceRank: CyberThreatRelevanceRank." https://github.com/oduwsdl/CyberThreatRelevanceRank, 2024.

[22] Fruhwirth, C., and T. Mannisto (editors). "Improving CVSS-Based Vulnerability Prioritization and Response With Context Information." Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement, 2009.

[23] Järvelin, K., and J. Kekäläinen. "Cumulated Gain-Based Evaluation of IR Techniques." *ACM Transactions on Information Systems* (*TOIS*), vol. 20, no. 4, pp. 422–446, 2002.

[24] Utterback, K. "An Analysis of the Cyber Threat Actors Targeting the United States and Its Allies." Utica College, 2021.

[25] Wikipedia. "Student's T-Test." https://en.wikipedia.org/wiki/Student%27s_t-test, 2022.

[26] Jacobs, J., S. Romanosky, B. Edwards, M. Roytman, and I. Adjerid. "Exploit Prediction Scoring System (EPSS)." arXiv preprint arXiv:190804856, 2019.

[27] CISA. "Known Exploited Vulnerabilities Catalog." https://www.cisa.gov/known-exploited-vulnerabilities-catalog, 16 November 2022.

[28] Hemberg, E., J. Kelly, M. Shlapentokh-Rothman, B. Reinstadler, K. Xu, N. Rutar, et al. "Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting." arXiv preprint arXiv:201000533, 2020.

[29] Bridges, R. A., C. L. Jones, M. D. Iannacone, K. M. Testa, and J. R. Goodall. "Automatic Labeling for Entity Extraction in Cyber Security." arXiv preprint arXiv:13084941, 2013.

[30] Jones, C. L., R. A. Bridges, K. M. T. Huffer, and J. R. Goodall (editors). "Towards a Relation Extraction Framework for Cyber-Security Concepts." Proceedings of the 10th Annual Cyber and Information Security Research Conference, 2015.

[31] Iannacone, M., S. Bohn, G. Nakamura, J. Gerth, K. Huffer, R. Bridges, et al. (editors). "Developing an Ontology for Cyber Security Knowledge Graphs." Proceedings of the 10th Annual Cyber and Information Security Research Conference, 2015.

[32] Bizer, C., T. Heath, and T. Berners-Lee. "Linked Data: The Story So Far." *Semantic Services, Interoperability and Web Applications: Emerging Concepts: IGI Global*, pp. 205–227, 2011.

[33] Wang, J. A., and M. Guo (editors). "OVM: An Ontology for Vulnerability Management." Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, 2009.

[34] Frei, S., M. May, U. Fiedler, and B. Plattner (editors). "Large-Scale Vulnerability Analysis." Proceedings of the 2006 SIGCOMM Workshop on Large-Scale Attack Defense, 2006.

[35] Alberts, C. J., and A. J. Dorofee. *Managing Information Security Risks: The OCTAVE Approach*." Addison-Wesley Professional, 2003.

[36] Tsukerman, E. "Cybersecurity Threat Modeling With OCTAVE," September 2020.

[37] Jacobs, J., S. Romanosky, I. Adjerid, and W. Baker. "Improving Vulnerability Remediation Through Better Exploit Prediction." *Journal of Cybersecurity*, vol. 6, no. 1, 2020.

[38] Chen, T., and C. Guestrin (editors). "XGBoost: A Scalable Tree Boosting System." Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016.

[39] Almukaynizi, M., E. Nunes, K. Dharaiya, M. Senguttuvan, J. Shakarian, and P. Shakarian (editors). "Proactive Identification of Exploits in the Wild Through Vulnerability Mentions Online." Proceedings of the 2017 International Conference on Cyber Conflict (CyCon US), 2017.

[40] Khazaei, A., M. Ghasemzadeh, and V. Derhami. "An Automatic Method for CVSS Score Prediction Using Vulnerabilities Description." *Journal of Intelligent & Fuzzy Systems*, vol. 30, no. 1, pp. 89–96, 2016.

[41] Dey, D., A. Lahiri, and G. Zhang. "Optimal Policies for Security Patch Management." *INFORMS Journal on Computing*, vol. 27, no. 3, pp. 462–77, 2015.

[42] Allodi, L., F. Massacci, and J. Williams. "The Work-Averse Cyberattacker Model: Theory and Evidence From Two Million Attack Signatures." *Risk Analysis*, vol. 42, no. 8, pp. 1623–1642, 2022.

[43] Alperin, K., A. Wollaber, D. Ross, P. Trepagnier, and L. Leonard (editors). "Risk Prioritization by Leveraging Latent Vulnerability Features in a Contested Environment." Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, 2019.

[44] Allodi, L., and F. Massacci (editors). "A Preliminary Analysis of Vulnerability Scores for Attacks in Wild: The EKITS and SYM Datasets." Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, 2012.

[45] Tatarinova, Y., and O. Sinelnikova. "Extended Vulnerability Feature Extraction Based on Public Resources." *Theoretical and Applied Cybersecurity*, vol. 1, no. 1, 2019.

[46] Notess, G. R. *The Wayback Machine: The Web's Archive*. Vol. 26, no. 2, pp. 59–61, 2002.

[47] Horawalavithana, S., A. Bhattacharjee, R. Liu, N. O. Choudhury, L. Hall, and A. Lamnitchi (editors). "Mentions of Security Vulnerabilities on Reddit, Twitter and GitHub." Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence, 2019.

[48] Jacobs, J., S. Romanosky, I. Adjerid, and W. Baker. "Improving Vulnerability Remediation Through Better Exploit Prediction." The 2019 Workshop on the Economics of Information Security, 2019.

[49] Singhal, A., and X. Ou. "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs." *Network Security Metrics*, Springer, pp. 53–73, 2017.

[50] Ou, X., W. F. Boyer, and M. A. McQueen (editors). "A Scalable Approach to Attack Graph Generation." Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006.

[51] Ou, X., S. Govindavajhala, and A. W. Appel (editors). "MulVal: A Logic-Based Network Security Analyzer." Proceedings of the USENIX Security Symposium, 2005.

[52] Homer, J., X. Ou, and D. Schmidt. "A Sound and Practical Approach to Quantifying Security Risk in Enterprise Networks." Kansas State University Technical Report, 2009-3, http://people.cs.ksu.edu/~xou/publications/tr_homer_0809.pdf, 2009.

[53] Gallon, L., and J. J. Bascou (editors). "Using CVSS in Attack Graphs." Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security, 2011.

[54] Noel, S., E. Harley, K. H. Tam, and G. Gyor. "Big-Data Architecture for Cyber Attack Graphs." MITRE Case Number 14-3549, https://csis.gmu.edu/noel/pubs/2015_IEEE_HST.pdf, 2014.

[55] Noel, S., E. Harley, K. H. Tam, and G. Gyor (editors). "Big-Data Architecture for Cyber Attack Graphs Representing Security Relationships in NoSQL Graph Databases." Proceedings of the IEEE Symposium on Technologies for Homeland Security (HST), 2015.

[56] Obes, J. L., C. Sarraute, and G. Richarte. "Attack Planning in the Real World." arXiv preprint arXiv:13064044, 2013.

[57] Allodi, L., and S. Etalle (editors). "Towards Realistic Threat Modeling: Attack Commodification, Irrelevant Vulnerabilities, and Unrealistic Assumptions." Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense, 2017.

BIOGRAPHIES

CORREN MCCOY serves as adjunct faculty to several universities, where she instructs courses in the information systems, computer science, and cybersecurity curriculums. She has earned multiple industry certifications and has been a frequent presenter at technology conferences across the country. Dr. McCoy holds a bachelor's degree in computer science from Pennsylvania State University, a master's degree in computer science from ODU, an M.S. in management from Regent University, and a Ph.D. in computer science from ODU, where her research focused on data-driven approaches for assessing cyber vulnerabilities.

ROSS GORE is a research associate professor at the Virginia Modeling, Analysis and Simulation Center (VMASC) at ODU. His current work focuses on data science and predictive analytics. Dr. Gore holds a bachelor's degree in computer science from the University of Richmond and a master's degree and Ph.D. in computer science from the University of Virginia.

MICHAEL L. NELSON is the deputy director of the School of Data Science at ODU, where his research interests include web science, web archiving, digital libraries, and information retrieval. Prior to his current position and teaching at ODU, he was an electronics engineer at NASA's Langley Research Center. He also received a joint appointment with VMASC. Dr. Nelson holds a B.S. in computer science from Virginia Tech and M.S. and Ph.D. degrees in computer science from Old Dominion University.

MICHELE C. WEIGLE is a professor of computer science at ODU, where her research interests include web science, social media, web archiving, and information visualization. She currently serves on the editorial boards of the *Journal of the Association for Information Science and Technology* and the *International Journal on Digital Libraries*. She has published over 115 articles in peer-reviewed conferences and journals and served as PI or Co-PI on external research grants totaling $6M from a wide range of funders, including the National Science Foundation, the National Endowment for the Humanities, the Institute of Museum and Library Services, and the Andrew W. Mellon Foundation. Dr. Weigle holds a B.S. in computer science from Northeast Louisiana University (now University of Louisiana at Monroe) and an M.S. and Ph.D. in computer science from the University of North Carolina.

CSIAC Cybersecurity & Information Systems Information Analysis Center

TECHNICAL INQUIRY SERVICES

FOUR FREE HOURS

Research within our four focus areas available to academia, industry, and other government agencies. Log in to csiac.dtic.mil to submit your inquiry today.

TECHNICAL AREAS

Cybersecurity

Knowledge Management & Information Sharing

Modeling & Simulation

Software Data & Analysis

Photo Source: U.S. Air Force and 123.com

CS IAC JOURNAL

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a component of the U.S. Department of Defense's (DoD's) Information Analysis Center (IAC) enterprise, serving the defense enterprise of DoD and federal government users and their supporting academia and industry partners.

WWW.CSIAC.DTIC.MIL
CONNECT WITH US ON SOCIAL MEDIA.