VOLUME 8 | NUMBER 1 | 2024

HDIAC JOURNAL

CHEM-BIO, DATA, AND CYBERSCIENCE AND TECHNOLOGY

IN DETERRENCE OPERATIONS PAGE 26

HDIAC JOURNAL

Volume 8 // Number 1 // 2024

Editor-in-Chief:
Gregory Nichols

Sr. Technical Editor:
Maria Brady

Graphic Designers:
Melissa Gestido, Katie Ogorzalek

The HDIAC Journal is a publication of the Homeland Defense & Security Information Analysis Center (HDIAC). HDIAC 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). HDIAC is operated by the SURVICE Engineering Company.

ISSN 2578-0832 (Print) // ISSN 2578-0840 (Online)

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

On the Cover:
Digital Art Rendering *(Source: BlackJack3D [Canva] and billionphotos [Canva]).*

HDIAC Homeland Defense & Security Information Analysis Center

ABOUT HDIAC

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.

HDIAC 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 Homeland Defense & Security Digest, state-of-the-art reports, journals, TI response reports, and more available on our website.

CONTACT HDIAC

IAC Program Management Office

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

HDIAC Headquarters

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

HDIAC Technical Project Lead

John Clements
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600

FEATURED ARTICLE

CHEM-BIO, DATA, AND CYBERSCIENCE AND TECHNOLOGY IN DETERRENCE OPERATIONS

By James Giordano

Recent advancements and interdisciplinary convergence in chemical, biological, data, computational, and engineering fields have enabled creation of chem-bio agents that are not (currently) regulated by international signatory treaties and conventions. When taken together, these agents can establish significant deterrent leverage in nonkinetic and kinetic domains.

IN THIS ISSUE

IMPACT RESISTANCE AND PERFORMANCE OF CUSTOM-FIT,

3-D-PRINTED PROTECTIVE GUARDS

BY MICHAEL E. ZABALA AND JACOB S. LARSON

(PHOTO SOURCE: VECTORFUSIONART [CANVA])

SUMMARY

This article explores the effect of the print method and material on the impact resistance of a custom-fit, three-dimensional (3-D)-printed shoulder guard for use as protective gear by sports or tactical athletes, such as Warfighters or police/fire/first responders. A 3-D scan was performed on the right shoulder of a body opponent bag (BOB) dummy. This scan was used to generate a virtual shoulder guard model that was 3-D printed via fused deposition modeling (FDM) and stereolithography (SLA) using multiple brands and types of materials. Shoulder guards with and without incorporated through-holes were tested. A physical shoulder model was created out of Quikrete concrete and a ShockShield liner. The various shoulder guards were placed on the shoulder model, and a drop assembly was used to impact the guards. The impactor used was a weighted American football helmet, and the weight was set to match the momentum of a National Football League (NFL) tackle at impact. Motion capture and ground-embedded force plates were used to measure impact velocity and force and validate momentum at impact. The holed version of the Hatchbox polylactic acid (PLA) guard fractured at the fifth impact, and the solid version of the Raise3D guard fractured at the second impact. The guards that did not fracture were the SLA-printed Formlabs "Durable" and "Tough" solid guards, the Formlabs Durable holed guard, and the Hatchbox PLA solid guards, both with and without ethylene vinyl acetate (EVA) foam padding. Therefore, these are the suggested combinations of the print method and material for manufacture of custom-fit, 3-D-printed protective gear.

INTRODUCTION

Additive manufacturing (3-D printing) is a process that has become widely adopted in multiple fields over the past decade, with custom-fit protective gear for sports or tactical athletes being one of the most promising use cases. FDM is one of the most common methods of 3-D printing. It involves extruding a polymer filament through a heated nozzle to generate a print on a layer-by-layer basis. Materials commonly used for FDM printing are PLA and acrylonitrile butadiene styrene (ABS). Other materials used for FDM printing are less common but include polyethylene terephthalate glycol (PETG), nylon, polycarbonate, and some filaments with embedded carbon fiber. SLA is another frequently used print method that involves using a light source to cure liquid resin housed in a vat within the 3-D printer. Resin mixtures, which tend to be proprietary, are frequently referred to by their advertised names such as Durable or Tough by Formlabs.

> ***Additive manufacturing (3-D printing) is a process that has become widely adopted in multiple fields over the past decade, with custom-fit protective gear for sports or tactical athletes being one of the most promising use cases.***

The ability to combine 3-D scanning with 3-D printing provides an additional opportunity to manufacture devices with complex curvatures like those needed for the human body. Creating customized medical devices like casts and braces via 3-D printing is becoming more commonplace despite technical challenges associated with the practical logistics of manufacturing these devices. 3-D scanning has traditionally been constrained to expensive handheld scanners such as the Creaform Go!Scan20. However, advancements in scanning capabilities on smartphones like Apple's Face ID technology on their iPhones have made scanning more accessible to large numbers of end users. Multiple pilot studies of the efficacy of custom-fit, 3-D-printed casts and braces have been published in recent years [1–5]. These studies consistently showed that the devices met or exceeded the performance of traditional casts and braces made from plaster or

thermoplastics as related to injury healing and patient comfort and satisfaction.

Another potential application of 3-D-printed devices is in the form of protective body-worn gear. 3-D printing has been used for athletic applications such as shoe soles (although not necessarily custom), custom-fit helmet liners, and even soccer shin guards [6–8]. The prospect of custom-fit protection for sports and tactical athletes is intriguing, as it would provide a low-profile version of athletic equipment likely to increase speed and maneuverability. However, the feasibility of 3-D-printed devices in such an extreme environment is relatively unknown.

Several studies in the literature examined the impact resistance of 3-D-printed devices [9–13]. These studies evaluated the effects of parameters like layer thickness and infill pattern and density. However, they only tested small prints, such as dog bone-shaped samples, rather than full-scale wearable equipment. There have been no known studies to test the effects of the print method and material type on impact strength for a full-scale piece of wearable protective gear. Therefore, the objective of this study is to test the impact resistance of custom-fit, 3-D-printed shoulder guards made by multiple print methods and from multiple materials. The hypothesis is that each shoulder guard would break after the first impact but before the 10th impact.

Another potential application of 3-D-printed devices is in the form of protective body-worn gear.

METHODS

The following methods describe the creation of the shoulder guards, the corresponding shoulder physical model, and the momentum requirements estimation. Additionally, the methods describe the drop guide assembly and method of impact force measurement as well as the drop process and subsequent impact velocity and momentum calculation as a means of verifying achieved momentum requirements.

Shoulder Guard Creation

The BOB dummy was chosen as the "test subject" for creating and testing custom-fit, 3-D-printed shoulder guards (Figure 1). A 3-D scan was performed on the right shoulder of the BOB by an in-house, iPhone-based, 3-D scanning app. The subsequent shoulder guard model (and print file) was also generated with in-house software. Two shoulder guard models were created, both 3 mm thick, with proprietary infill density—a solid version and a "holed" version meant to replicate commonly used lattice-type approaches to 3-D printing. There were two types of print methods used for the 3-D-print-tested shoulder guards: (1) FDM on a Raise3D Pro2 printer and (2) SLA on a Formlabs Form 2 printer. Two brands of filament were used with FDM printing—Raise3D PLA and

Figure 1. Custom-Fit, 3-D-Printed Shoulder Guards Fitting the BOB *(Source: M. Zabala and J. Larson).*

Hatchbox PLA. There were two types of resin used with SLA printing—Formlabs Durable and Tough. The same shoulder guard model was used for each print, except for the holed versions, which involved the same original shoulder model file but with through-holes.

The first round of testing was performed on unpadded shoulder guards (Figure 2). A second round of testing was performed on Hatchbox PLA shoulder guards with and without 3-mm EVA foam padding. This included a special case that involved a 24-hour pause during the 3-D-printing process, which occurred approximately halfway through. This special case was meant to replicate an accidental stoppage midprint, such as the 3-D printer experiencing an unexpected and unmonitored power outage while printing a device with an extended print time.

Physical Shoulder Model Creation

It was determined that use of the BOB dummy for impact testing was not ideal, as the entire BOB setup would attenuate force prior to registration by ground-embedded force plates over which it would be placed during testing. Therefore, a representative physical model of only the BOB's right shoulder was created. This was accomplished by using the shoulder scan to generate a virtual model file of a negative shoulder mold, which was 3-D printed and filled with Quikrete concrete and allowed to harden. The resulting concrete shoulder was then covered with an 8-mm-thick ShockShield liner (similar to ballistics gel) to represent soft tissue. The result of this process was a physical representation of the BOB's right shoulder upon which the shoulder guards could be positioned for impact testing (Figure 3). In the figure, the setup was positioned on top of a concrete footer, which was set upon ground-embedded force plates.

Momentum Estimation

A weighted American football helmet was chosen as the impactor to represent an extreme scenario during athletic activity. Moreover, to produce an adequate representation of impact, an estimation was performed of the momentum of an NFL linebacker's head during a maximum-speed tackle. A 95th percentile male head mass was considered: 5.377 kg (11.85 lbf) [14]. With an assumed tackle velocity of

Figure 2. Shoulder Guards: (Top Row, Left to Right) Formlabs Durable Solid, Durable Holed, Tough Solid, and Tough Holed and (Bottom Row, Left to Right) Hatchbox PLA Solid, Hatchbox PLA Holed, and Raise3D PLA Solid *(Source: M. Zabala and J. Larson)*.

Figure 3. BOB Right Shoulder (Concrete With Overlaid ShockShield) With a Custom-Fit, 3-D-Printed Shoulder Guard *(Source: M. Zabala and J. Larson)*.

20 mph, the resulting momentum of the head at impact during an NFL tackle was ~348 lbm-fps. (Note that this condition represented a legal tackle, with the head upright, and contact was made by the anterior surface of the helmet. This condition did not represent an illegal "targeting" tackle where the entire body was launched at the ball carrier and contact was made with the crown of the helmet.)

Preliminary tests in the Auburn University Biomechanical Engineering Lab provided an estimated impact speed of ~12 mph. Therefore, to match the momentum of an NFL tackle, the impactor (helmet and crossbar) weight needed to be ~19.8 lbf. The helmet used as the impactor for testing was a Schutt Vengeance Pro for adults.

Drop Guide and Impactor Assembly and Force Measurement

A cable-based guide assembly was built to generate an impact velocity of ~12 mph. Two cables were anchored in the ceiling of the 8-foot-tall lab space and at the floor to two 8-inch × 8-inch × 16-inch concrete blocks. The cables were routed through two eyelets at each end of a wooden dowel that was passed through the earholes of the football helmet (Figure 4). This figure shows a weighted American football helmet with a metal rod through the earholes. The rod has eyelets at the ends through which guide wires pass. Weights were added to the helmet such that the helmet, weights, and dowel assembly were ~19.8 lbf. The two concrete blocks and the concrete footer and shoulder assembly were all placed within the footprint of two AMTI ground-embedded force plates (AMTI BP400600, 2,000-lbf capacity) to measure peak impact force from the impacting helmet transferred through the guard, shoulder, and concrete footer. A rope was routed through a pulley mounted to the ceiling, and a release mechanism was attached to the end of the rope connected directly to the helmet/dowel impactor assembly.

Drop Process

Each of the shoulder guards was tested until the 10th impact or until fracture. Prior to each drop, the force plates were zeroed to account for the weight of the two concrete blocks, the concrete footer, and the shoulder model (concrete and ShockShield). A research assistant raised the impactor assembly by pulling on the rope (routed through the pulley). A second research assistant located on a ladder near the top of the drop assembly then engaged the release mechanism to initiate the drop. Drops were performed 10 times or until the guard broke, whichever came first.

Impact Velocity and Momentum Calculation

A 10-camera Vicon motion capture system was used to track three retroreflectors placed with double-sided tape on the left, right, and center of the helmet. Impact was determined by detecting the first z-coordinate (height) minimum of the centroid of all three helmet markers. The slope of the centroid position for 15 frames prior to impact was calculated as the "impact velocity" for each test. Momentum was calculated as the product of impact velocity and impactor mass.

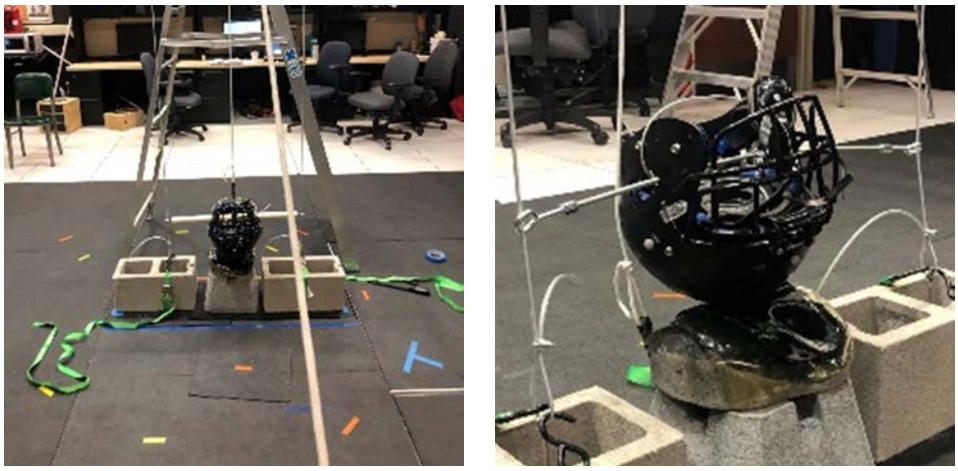


Figure 4. Setup for Impact Testing *(Source: M. Zabala and J. Larson)*.

RESULTS

This section details the achieved impactor momentum, along with other impact results such as impact force, impact velocity, and how many trials a guard withstood prior to breaking. The guard impact performance is provided in the two tables presented in this section.

Momentum

The momentum at impact for all the impact tests with an impactor weight of 19.8 lbf was a minimum of 314.9 lbm-fps and a maximum of 356.2 lbm-fps. The average momentum was 353.9 lbm-fps, which was only 1.7% greater than the target momentum of 348 lbm-fps.

Print Method and Material Type

The shoulder guard prints that withstood impact for all 10 trials were the Formlabs Durable – Solid, Formlabs Durable – Holed, Formlabs Tough – Solid, and the Hatchbox PLA – Solid. The Formlabs Tough – Holed guard broke on the third trial. The Hatchbox PLA – Holed guard broke on the fifth trial. The Raise3D PLA – Solid guard was the only solid guard to break; it broke on the second trial. The results are listed in Table 1.

With and Without Padding and Print Interruption

The shoulder guard prints that withstood impact for all 10 trials were the Hatchbox PLA with and without padding. The shoulder guard that was interrupted during the print process for 24 hours broke on the final 10th trial. A final reported test was added

Table 1. Results of Testing the Effects of Varying Print Methods and Materials and the Presence of Through-Holes

GUARD	VALUE	IMPACT FORCE (LB)	VELOCITY (MPH)	MOMENTUM (LBM-FPS)	BREAK OCCURRED
Formlabs Durable, Solid	**Mean**	**1564.1**	**12.1**	**351.1**	NO BREAK
	Min	1369.7	11.9	345.3	
	Max	1830.0	12.2	353.9	
Formlabs Durable, Holed	Mean	**1610.0**	**12.0**	**348.6**	NO BREAK
	Min	1360.9	11.9	346.8	
	Max	1795.9	12.1	351.5	
Formlabs Tough, Solid	**Mean**	**1400.9**	**12.0**	**348.2**	NO BREAK
	Min	1253.7	11.9	346.1	
	Max	1716.3	12.1	350.7	
Formlabs Tough, Holed	**Mean**	**1458.5**	**12.1**	**351.0**	3rd Trial
	Min	1310.4	12.1	350.0	
	Max	1602.5	12.1	351.5	
Hatchbox PLA, Solid	**Mean**	**1512.8**	**12.1**	**351.1**	NO BREAK
	Min	1242.2	12.0	348.4	
	Max	1840.8	12.3	356.2	
Hatchbox PLA, Holed	**Mean**	**1495.3**	**12.1**	**350.9**	5th Trial
	Min	1355.7	12.0	348.4	
	Max	1625.6	12.1	352.3	
Raise3D PLA, Solid	**Mean**	**1788.8**	**12.1**	**351.9**	2nd Trial
	Min	1757.4	12.1	350.0	
	Max	1820.2	12.2	353.9	

to the process to attempt to break the Hatchbox PLA padded shoulder guard. The impactor weight was increased from 19.8 lbf to 23.8 lbf. Additional impacts, beyond the initial 10 at 19.8 lbf, were conducted. The Hatchbox PLA foam padded guard broke on the 17th trial overall (on the seventh with additional mass – see Table 2 and Figure 5).

DISCUSSION

The hypothesis that the shoulder guards would break after the first but before the 10th impact trial was partially confirmed. All solid shoulder guards, except the interrupted print and the Raise3D brand PLA, withstood the 10 impacts. The holed version of the Formlabs Durable shoulder guard also withstood 10 impacts. However, the holed versions of the Formlabs Tough and Hatchbox PLA fractured during the third and fifth trials, respectively. This was not surprising, as including holes to the shoulder guard reduced the guard surface area and introduced stress concentrations at the locations of the holes. Also not surprising was that the interrupted print broke, albeit during the final 10th trial. This was because the 24-hour interruption likely resulted in a compromised abutment between the final layers prior to the pause and the initial layer upon print reinitiation. Had the interruption not occurred, the two layers would have been at higher temperatures, closer to the melting point of PLA, and formed a higher integrity bond. More surprising was that the solid version of the Raise3D PLA shoulder guard failed at the second impact trial. Although definitive conclusions cannot be drawn

Figure 5. Final Impact of Helmet Weighted to 23.8 lbf Resulting in Fracture of Guard (Hatchbox PLA Solid) and Helmet *(Source: M. Zabala and J. Larson).*

Table 2. Results of Testing of the Effects of Interrupted Printing and the Presence of Foam Padding

ALL SOLID PRINTS	VALUE	IMPACT FORCE (LBF)	VELOCITY (MPH)	MOMENTUM (LBM-FPS)	BREAK OCCURRED
Hatchbox, No Padding	**Mean**	**1656.7**	**11.6**	**337.3**	NO BREAK
	Min	1559.2	11.4	330.5	
	Max	1772.2	11.9	346.1	
Hatchbox, No Padding – Interrupted	**Mean**	**2029.4**	**11.8**	**343.8**	10th Trial
	Min	1469.8	11.4	335.2	
	Max	2392.7	11.9	352.3	
Hatchbox, 3-mm EVA Foam	**Mean**	**1749.2**	**11.8**	**343.8**	NO BREAK
	Min	1575.3	11.4	314.9	
	Max	1854.4	12.1	351.5	
Hatchbox, 3-mm EVA Foam-Increased Mass	**Mean**	**2036.6**	**11.9**	**415.6**	17th Trial[a]
	Min	1817.8	10.8	411.3	
	Max	2160.9	12.1	421.6	

[a] The helmet impactor broke on this trial, along with the guard.

from this singular test, it does seem to suggest that brand influences impact strength of PLA, as no solid Hatchbox PLA shoulder guards broke except during the increased mass condition and at the 17th overall impact (Table 2, Figure 5). It is not clear why there seems to be a difference in performance across brands. However, it is reasonable to assume that various brands of filament manufacturers have unique subingredients and mixture combinations for a specific filament type like PLA that combine to produce different material property characteristics, including impact strength.

The performance of the devices impacted in this study provides evidence to support the feasibility of using custom-fit, 3-D-printed wearable protective guards by both sports and tactical athletes. The potential uses for sports athletes include shoulder guards, thigh pads, and knee pads for American football, hockey, and lacrosse players; shin guards for soccer players; and torso pads for motocross athletes. The potential uses for the tactical athlete are similar—low-profile body/torso protective gear, elbow pads, or knee pads. All these athletes would benefit greatly from protective gear made specifically to their bodies as opposed to discretely sized (small, medium, large, etc.) commercial off-the-shelf gear. It is likely that the custom-fit aspect of 3-D-printed gear would allow athletes to move more comfortably and freely and thus become more effective at their craft. Moreover, the Warfighters' ability to increase speed and maneuverability would improve lethality and survivability.

The findings of this study also provide indirect evidence to support the use of custom-fit, 3-D-printed medical casts, splints, and braces (manufactured with the same methods) in settings like austere environments, as these devices would certainly experience mechanical loading conditions below what was tested. The results are subject to several limitations. First, only two brands of PLA and two types of resin were tested. Second, only a single design device was tested—a 3-mm-thick, custom-fit right shoulder guard for the BOB. Future tests should include multiple designs of multiple devices with various thicknesses. It is probable that parts of different sizes and contours will perform differently. Third, only 3-mm-thick EVA foam was used in the foam-lined conditions. Other types of foams with various thicknesses should also be used in future tests [15]. Fourth, the print orientation was consistent for each of the printed parts. It has been established in the literature that print orientation affects the strength of 3-D-printed parts [13, 16]. Also, infill density was not tested as an independent variable in this study. Future studies would benefit from an analysis of the effect of infill density on impact strength.

The performance of the devices impacted in this study provides evidence to support the feasibility of using custom-fit, 3-D-printed wearable protective guards by both sports and tactical athletes.

Another limitation is the minimal number of tests performed. Additional tests with large numbers of samples and impacts, likely into the hundreds, would provide a more thorough assessment of impact performance.

Finally, it is important to draw attention to the test's design as it relates to what is likely experienced on the field of play due to an NFL tackle. The results of the testing described here included extremely high impact forces, ~1,500 lbf. During an actual tackle, the tackled ball player's body will necessarily move with the tackler due to impact, absorbing the contact. However, the test setup in the lab resulted in an *immobile* shoulder model due to it being placed firmly on the ground and struck downward by the impactor. Therefore, the lab test more accurately represented an NFL tackle by driving the player into a concrete floor. This is obviously more extreme than what is typically experienced on

the field of play but is potentially an improved representation of the degree of impact experienced by the tactical athlete. ■

CONCLUSIONS

This study evaluated the effect of print method (FDM vs. SLA) and material brand (Raise3D, Hatchbox) and type (PLA and Tough and Durable by Formlabs) on impact resistance to fracture. An additional variable was also tested—a 24-hour pause in the print process approximately halfway through the print. Impacts were designed to mimic an NFL tackle, although it was determined that the test setup was more extreme than likely experienced on the field of play. The results indicate that custom-fit, 3-D-printed protective gear can be appropriate for use in high-impact environments and for sports and tactical athletes, even based on the conservative testing conditions used in this study.

ACKNOWLEDGMENTS

The authors would like to thank Grace Gray and Grant Hawkins for their contributions in collecting data in the lab as well as processing results.

REFERENCES

[1] Fang, J.-J., C.-L. Lin, J.-Y Tsai, and R.-M. Lin. "Clinical Assessment of Customized 3D-Printed Wrist Orthoses." *Applied Sciences*, vol. 12, no. 22, 2022.

[2] Schlegl, A. T., R. Told, K. Kardos, A. Szoke, Z. Ujfalusi, and P. Maroti. "Evaluation and Comparison of Traditional Plaster and Fiberglass Casts With 3D-Printed PLA and PLA-CaCO(3) Composite Splints for Bone-Fracture Management." *Polymers* (*Basel*), vol. 14, no. 17, 2022.

[3] Schwartz, D. A., and K. A. Schofield. "Utilization of 3D Printed Orthoses for Musculoskeletal Conditions of the Upper Extremity: A Systematic Review." *J. Hand Ther.*, vol. 36, no. 1, pp. 166–78, 2023.

[4] Van Lieshout, E. M. M., M. H. J. Verhofstad, L. M. Beens, J. J. J. Van Bekkum, F. Willemsen, H. M. J. Janzing, et al. "Personalized 3D-Printed Forearm Braces as an Alternative for a Traditional Plaster Cast or Splint; A Systematic Review." *Injury*, vol. 53 Suppl. 3:S47–S52, 2022.

[5] Waldburger, L., R. Schaller, C. Furthmuller, L. Schrepfer, D. J. Schaefer, and A. Kaempfen. "3D-Printed Hand Splints Versus Thermoplastic Splints: A Randomized Controlled Pilot Feasibility Trial." *Int. J. Bioprint.*, vol. 8, no. 1, p. 474, 2022.

[6] Zastrow, M. "3D Printing Gets Bigger, Faster and Stronger." *Nature*, vol. 578, pp. 20–24, 2020.

[7] Lee, H., R.-I. Eom, and Y. Lee. "Evaluation of the Mechanical Properties of Porous Thermoplastic Polyurethane Obtained by 3D Printing for Protective Gear." *Advances in Materials Science and Engineering*, pp. 1–10, 2019.

[8] Alarifi, M. I., and I. M. Alarifi. "Comprehensive Structural Evaluation of Composite Materials in 3D-Printed Shin Guards." *Journal of Materials Research and Technology*, vol. 27, pp. 6912–6923, 2023.

[9] Othman, F., H. B. Ali, and T. F. Alani. "Influence of Layer Thickness on Impact Property of 3D-Printed PLA." *International Research Journal of Engineering and Technology*, vol. 5, no. 2, pp. 1–4, 2018.

[10] Mishra, P. K., P. Senthil, S. Adarsh, and M. S. Anoop. "An Investigation to Study the Combined Effect of Different Infill Pattern and Infill Density on the Impact Strength of 3D Printed Polylactic Acid Parts." *Composites Communications*, vol. 24, 2021.

[11] Rajpurohit, S. R., and H. K. Dave. "Impact Strength of 3D Printed PLA Using Open Source FFF-Based 3D Printer." *Progress in Additive Manufacturing*, vol. 6, no. 1, pp. 119–131, 2020.

[12] Tanveer, M. Q., A. Haleem, and M. Suhaib. "Effect of Variable Infill Density on Mechanical Behaviour of 3-D Printed PLA Specimen: An Experimental Investigation." *SN Applied Sciences*, vol. 1, no. 12, 2019.

[13] Tezel, T., M. Ozenc, and V. Kovan. "Impact Properties of 3D-Printed Engineering Polymers." *Materials Today Communications*, vol. 26, 2021.

[14] Yoganandan, N., F. A. Pintar, J. Zhang, and J. L. Baisden. "Physical Properties of the Human Head: Mass, Center of Gravity and Moment of Inertia." *J. Biomech.*, vol. 42, no. 9, pp. 1177–92, 2009.

[15] Kao, Y.-T., A. R. Amin, N. Payne, J. Wang, and B. L. Tai. "Low-Velocity Impact Response of 3D-Printed Lattice Structure With Foam Reinforcement." *Composite Structures*, vol. 192, pp. 93–100, 2018.

[16] Saini, J. S., L. Dowling, J. Kennedy, and D. Trimble. "Investigations of the Mechanical Properties on Different Print Orientations in SLA 3D Printed Resin." *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science*, vol. 234, no. 11, pp. 2279–2293, 2020.

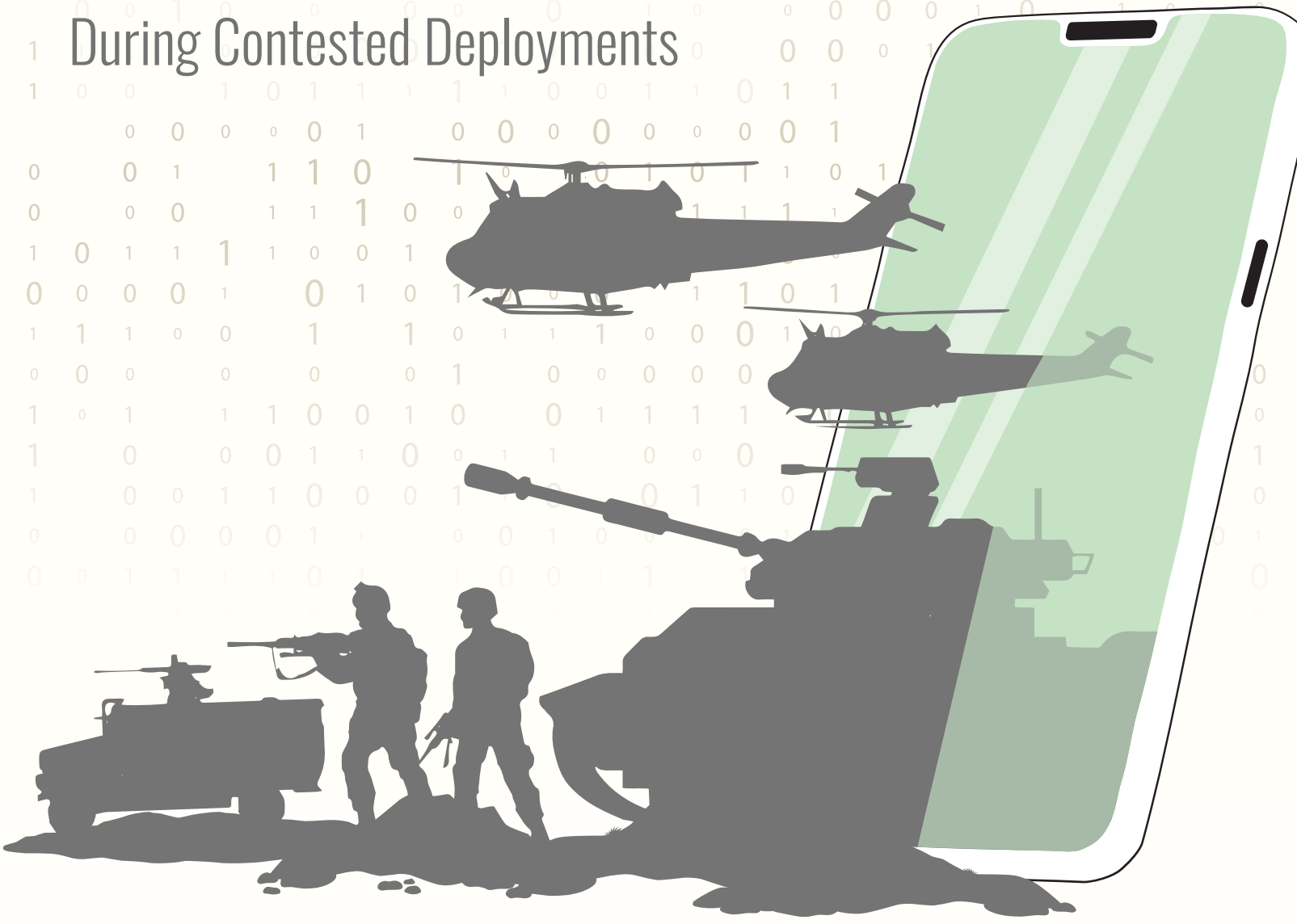
BIOGRAPHIES

MICHAEL E. ZABALA is the director of the Auburn University Biomechanical Engineering Lab, where he focuses on the biomechanics of human performance and injury prevention. He has a long history of research involving 3-D scanning and printing of custom devices for the human body and a strong collaboration history with the Auburn University Football Program. Some of his other research endeavors have included anterior cruciate ligament (ACL) injury prevention and lower-limb prostheses and exoskeleton design and control. Dr. Zabala holds a bachelor's degree in mechanical engineering from Auburn University and a master's degree and Ph.D. in mechanical engineering from Stanford.

JACOB S. LARSON is the director of engineering at XO Armor, where he focuses on developing cutting-edge 3-D scanning and manufacturing capabilities. He has successfully led research teams at XO Armor for 7+ years as a graduate student and the engineering director. His projects range from injury prevention in athletes using nonlinear dynamics analysis to creating custom 3-D-printed medical devices for Veterans Administration hospitals. Dr. Larson holds a bachelor's degree in mechanical engineering from Valparaiso University and a Ph.D. in mechanical engineering from Auburn University.

HOMELAND DEFENSE FOR THE FUTURE FIGHT:

Threats to "Information Advantage" During Contested Deployments



BY JOEL HEWETT (PHOTO SOURCE: JEMASTOCK [123RF.COM], T-REX [CANVA], AND ALEXSL [CANVA])

INTRODUCTION

Over the winter of 1990–1991, military leaders in Washington, D.C., identified a new threat to the security of U.S. armed forces deployed around the globe—pizza, i.e., *delivery* pizza. An enterprising local pizzeria owner noticed that his late-night delivery orders to Central Intelligence Agency Headquarters would spike immediately before an international conflict or to the Pentagon whenever the U.S. Department of Defense (DoD) was preparing to execute a major troop movement [1, 2]. He was also not keeping it confidential. As a result, reporters from *Time* and *The Washington Post*, eager for a byline on the imminent start of the Persian Gulf War, traded mention of his pizzerias' offerings for information. One prominent cable news host reportedly concluded that from then on, the "bottom line" for national security journalists was clear: "always monitor the pizzas" [3].

Whether the story of the "Pentagon Pizza Index" was ever truly a useful means of predicting the deployment of American forces is somewhat irrelevant. Rather, for DoD leadership, the Pizza Index came to symbolize the dawn of a new era of warfare—one dominated by the pervasive use of digital communication devices and constant presence of live, real-time global media streams [4, 5]. The challenges posed by this new "Information Age" in the 1990s demanded an organized and concerted response from strategic thinkers within the DoD. They answered, in part, by developing new military doctrine—the fundamental principles, ideas, methods, and practices that guide the use of force. New doctrinal concepts and field manuals for both "Information Warfare" and "Information Operations" soon emerged [4].

Since the 1990s, the DoD and the service branches alike have repeatedly reviewed, codified, and revisited what constitutes *information* and what role it might play in the future of combat [4–6]. By the late 2010s, this perennial cycle of revision began anew. The doctrinal concepts and manuals on applying "informational power" or working in the cognitive realm had become a mere afterthought to the military planning process—they were either overly broad in scope or had been written to such a level of specificity that they were all but indistinguishable from the technologies that enabled them [4, 6].

In the last five years, however, information doctrine has seen a renaissance within the DoD, and the U.S. Army has largely led the way. As the Joint Force's largest component, and given its remit for land operations, the Army is central to the DoD's strategic focus on preparing for the possibility of conventional, large-scale combat operations (LSCOs) against a peer threat. It is within this backdrop that the U.S. Army promulgated Army Doctrine Publication (ADP) 3-13, *Information* [7], in late 2023. This publication guides soldiers on how to best think about the military use of information and gives detailed direction on how to exploit it to build and apply combat power. It also introduced an important new phrase to the lexicon—*information advantage* (IA). Its definition is deceptively simple: IA is "the use, protection, and exploitation of information to achieve objectives more effectively than enemies and adversaries do" [7].

> ***In the last five years, information doctrine has seen a renaissance within the DoD, and the U.S. Army has largely led the way.***

OVERVIEW

This article explores the IA concept as it functions within the U.S. Army's broader operational concept—multidomain operations (MDOs). It explores the ways in which threat actors might, at the outset of an LSCO-sized conflict, use nonkinetic and antiaccess information-based attacks to disrupt, hinder, and degrade U.S. efforts to generate and deploy expeditionary military force from the homeland—a strategy sometimes referred to as "preclusion" (see Figure 1). This is a critical area of study because

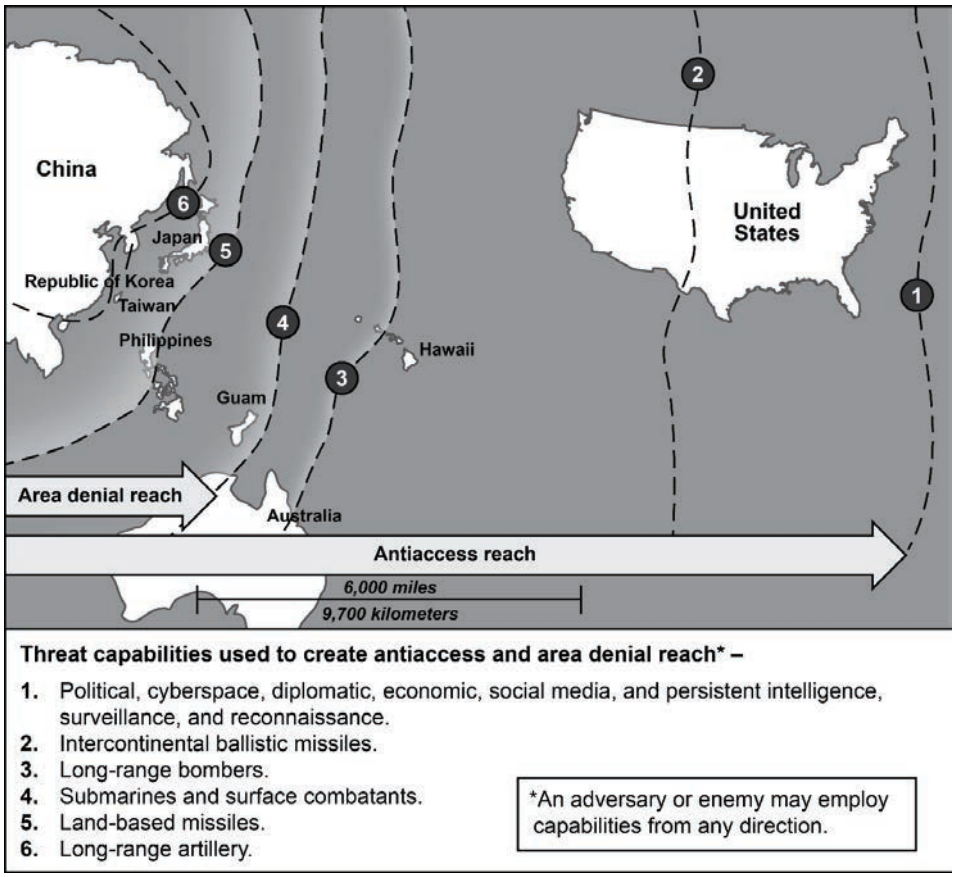


Figure 1. Notional Example of Threat Adversary Preclusion of U.S. Force Projection Using NonLethal, NonKinetic Informational Means (ⓘ) to Isolate and Demoralize the United States, Kindle Civic Instability, and Manipulate Public Opinion *(Source: U.S. Army [10]).*

adversaries now possess powerful and effective cyberspace, media, and psychological stand-off capabilities that threaten the Joint Force's freedom of action at the very outset of a military engagement.

In the future fight, U.S. forces will have to "fight for, defend, and fight with information" even before a conflict escalates into a kinetic battle [7]. This coming challenge is further complicated by the fact that American force projection operations from the homeland have never been truly contested by adversary forces. U.S. military leadership now sees the contestation of future deployments as all but inevitable, and such attacks are expected to come primarily from the information dimension. As DoD strategic documents routinely point out, the defense of traditional power projection capabilities from nonkinetic cyber and informational effects may well be the deciding factor in determining who will prevail [8, 9].

This article proceeds in three parts. First, it traces how U.S. Army doctrine and practice have considered the role of information (especially computerized knowledge-management systems) during deployment exercises in the 1970s–1980s and how they enabled the "spectacular" success of projecting U.S. forces into Saudi Arabia during the Persian Gulf War. For military planners, these events underscored the fact that the DoD's ability to mass and deploy forces is underpinned by its information-based communication and logistics systems, many of which were seen as either inadequate or insecure.

Second, the article presents a review of the MDO operational concept's core and traces how the information dimension functions within and across its domains in U.S. Army doctrine. It notes that the task of achieving and preserving IA emerged as a counter to the nonkinetic cyber and information-based threats developed by peer states since the 1990s. Recognizing that future adversary actions will target public and private media to offer false narratives, it also highlights the centrality to the IA concept of subjective perception.

Third, three avenues are explored through which threat actors might seek to generate harmful cognitive effects in service members and the public to preclude U.S. force projection. As a recounting of a fictionalized digital attack on a deploying soldier's family helps illustrate, adversaries will conduct persistent reconnaissance and intelligence on soldiers and their loved ones to gain advantages; they will exploit DoD and other information systems to directly influence soldier

action; and they will interfere with the public to hinder or degrade U.S. Army force projection activities.

FORCE PROJECTION AT THE START OF THE INFORMATION AGE

As military historians and active-duty generals point out, the U.S. Army undergoes a major transformation roughly every 40 years [10, 11]. Its most recent overhaul began in the 1970s, partly because of Gen. Donn A. Starry, a four-star armored cavalry commander who took the reins of the U.S. Army Training and Doctrine Command (TRADOC) in 1977. Starry arrived to find TRADOC in a phase of considerable transition. Although U.S. involvement in Southeast Asia was then in the rearview mirror, the easing of tensions in American-Soviet relations (known as détente) had begun to deteriorate, and the threat of Soviet antiarmor weapons loomed large [12]. Starry played an outsized role in rethinking the Army's warfighting framework, known as "AirLand Battle." By the mid-1980s, its tactics had been reformed to contend with the nonlinear battlefields of the future—ones marked by using long-range reconnaissance technologies and complex, computerized command and control (C2) systems [12, 13].

Command Post Exercise (CPX) "Nifty Nugget"

Starry's emphasis on the role of C2 in enabling rapid maneuver and force sustainment was an apt one, for the general was familiar with the baleful consequences of subpar C2 capabilities [14]. In 1978, the DoD convened a massive, 21-day-long CPX that simulated a full-scale, whole-of-government effort to project U.S. military force into the European theater (see Figure 2) [15, 16]. CPX Nifty Nugget aimed to stress-test the Pentagon's force generation and mobilization plans, military-civilian coordination at the federal level, and the DoD's logistical information technology (IT) systems—and stress

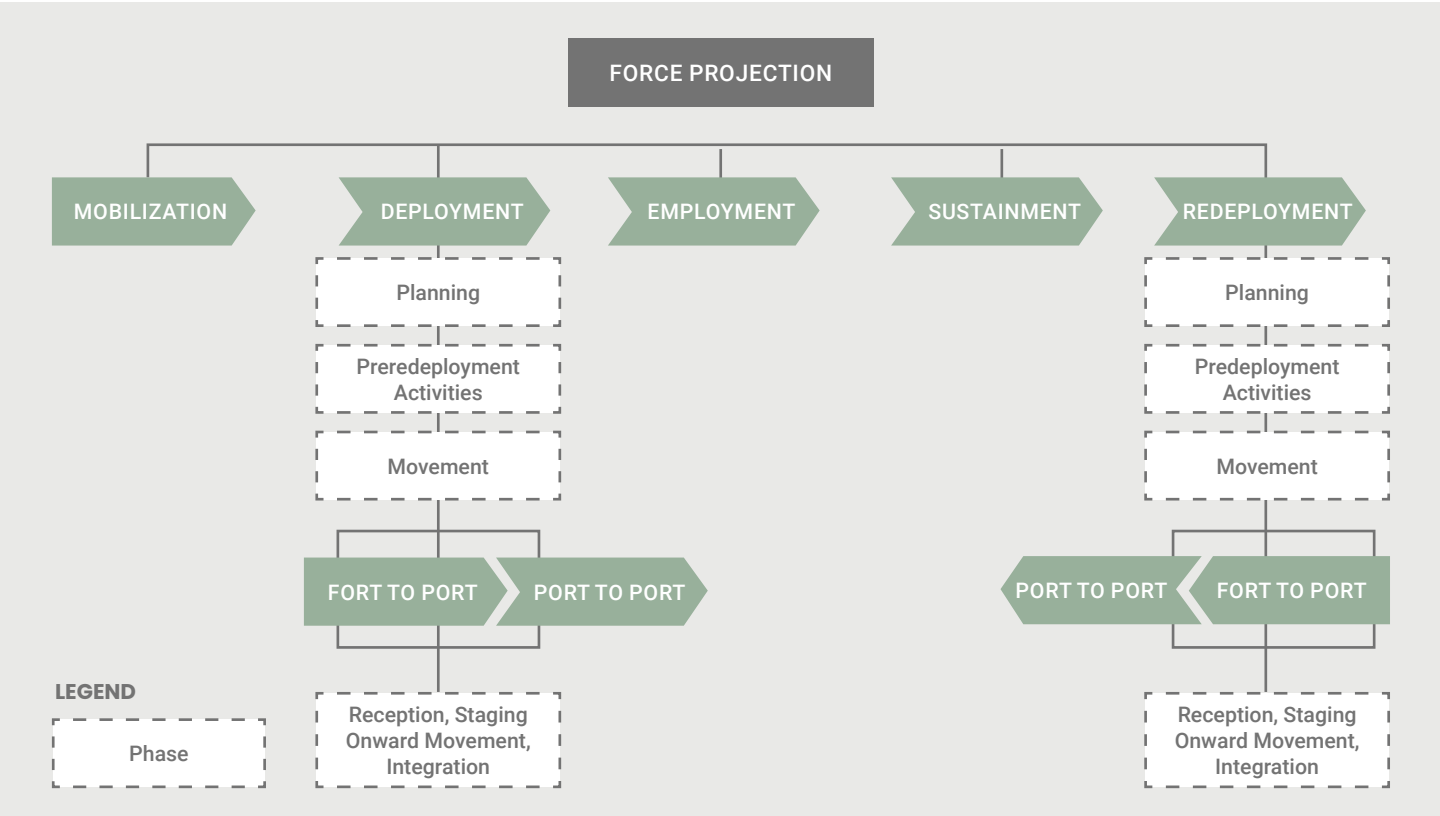


Figure 2. U.S. Army Force Projection Operations in 2023 Extend From Bringing Personnel to a State of Readiness for War to Their Eventual Redeployment to the Home Theater *(Source: U.S. Army [18])*.

was just about all that Nifty Nugget uncovered. The DoD was unable to "locate" ~350,000 of the ~800,000 fictional troops that the scenario called for, and exercise participants "could not even agree on the meaning of the word 'mobilization' " [15, 17].

Nifty Nugget was also the first exercise to thoroughly examine the World-Wide Military Command and Control System (WWMCCS), a computerized C2 system developed in the 1960s to coordinate and control operational activities along the entire chain of command. WWMCCS was found to not be able to "walk and chew gum at the same time" [19]. The system posted slow response times, could not keep up with Nifty Nugget's computing tempo, and suffered from a lack of flexibility. Because its preset deployment orders were issued automatically, any change was likely to hamstring multiple units for days [19]. In one instance, an airlifting team "received 27 validated requests to move the same unit to 27 different places" [15].

Operation Desert Shield

The DoD took Nifty Nugget's logistical failures to heart. The Joint Chiefs of Staff created a Joint Deployment Agency (JDA) soon thereafter and charged it with consolidating deployment tasks across the department [15, 18]. To underscore its authority to task units from other forces, the JDA was later elevated to combatant command status as the U.S. Transportation Command (USTRANSCOM). In 1990, its information-management capabilities played a critical role in executing Operation Desert Shield, the largest projection of expeditionary military force—by any nation—since the end of World War II [20].

In just over two months, USTRANSCOM oversaw the movement of more than 120,000 troops, 700 armored tanks, 1,400 fighting vehicles, and 600 artillery pieces into the seaports and deserts of Saudi Arabia [20]. With Iraqi forces unable to contest U.S. force projection tasks via stand-off attacks, American forces embarked for the Middle East by any means available to them, sometimes even via chartered commercial flights (see Figure 3). U.S. equipment and personnel were dispatched *so* rapidly—three times the rate achieved during the War in Vietnam [21]—that many soldiers arrived to find insufficient accommodations present in theater. Some even turned to sleeping in the open sand [20, 22].

Its hiccups notwithstanding, Operation Desert Shield was seen as a "spectacular" success, and USTRANSCOM's synchronization of airlift, sealift, prepositioned stocks, and in-theater resources was hailed as a "logistical marvel" [15]. Central

Operation Desert Shield was seen as a "spectacular" success, and USTRANSCOM's synchronization of airlift, sealift, prepositioned stocks, and in-theater resources was hailed as a "logistical marvel."

Figure 3. U.S. Marines Board a Commercial Aircraft Chartered by U.S. Military Airlift Command at an Undisclosed Location During Operation Desert Shield, September 1990 *(Source: DVIDS [23])*.

to this effort was the command's computerized Joint Operation Planning and Execution System (JOPES), a subsystem of the WWMCCS, which had been developed specifically to solve the transportation C2 problems seen during CPX Nifty Nugget. However, at the outset of operations in 1990, many officers did not trust JOPES. It lacked in-transit visibility of cargo and passenger movements, and many senior commanders opted to bypass JOPES entirely. It was seen as a bureaucratic tool that had "no place in a real war" until a major on-the-fly software overhaul—and orders for stricter adherence to JOPES procedures—made it an essential part of Desert Shield's logistical success [15].

The First Information War

It did not take the hindsight of history for the Persian Gulf War to become known as "the Computer War." It was the first conflict determined by modern technology, and it became closely identified with American precision-guided munitions, night-vision goggles, and stealth aircraft [24]. However, many strategic analysts regarded the conflict as the first Information War, more attuned as they were to the contribution made by more mundane systems like the WWMCCS and JOPES. They recognized that for all her technological might, the American way of warfare relied far more heavily on logistical data and IT systems than it did on "smart" bombs or stealth [24, 25].

It did not take the hindsight of history for the Persian Gulf War to become known as "the Computer War."

This reliance, however, was also recognized as a source of vulnerability. As one retired U.S. Air Force colonel opined in 1992, coalition forces had come to see information "as a utility; ubiquitous, commonly shared, commonly financed, uncommonly reliable, and always available or almost always...forgotten are those infrequent but terrifying moments when global finance or air traffic control networks are halted by momentary lapses in computer or human behavior" [25]. Adversarial militaries across the world took similar note. In direct response to the war's outcome, the People's Liberation Army (PLA) of the People's Republic of China (PRC) began to aggressively expand its capabilities in technical reconnaissance, offensive cyberspace operations, and warfare in the electronic, psychological, communications, and information spaces [26, 27].

In 2015, the PLA established the Strategic Support Force (SSF) as a theater command-level organization to centralize its assets in "informationized" warfare. Current PLA information doctrine calls for it to wage warfare on an adversary's morale, psychology, public opinion, legal structures, and media narratives to "disrupt [its] military operations"—especially during the initial stages of a conflict [27]. For adversarial nations, the ability of U.S. forces to deploy to the Persian Gulf freely was instructive. The conflict's lesson for the PLA was the importance of significantly improving its counter-C2 and information warfare capabilities to disrupt hostile deployment actions that might target PLA forces.

INFORMATION ADVANTAGE IN MDO

The MDO framework originated in the mid-2010s, the partial product of Commander Gen. David G. Perkins's pushing for TRADOC to grapple with the growing threat from peer states in the cyber and space domains [28]. The 2018 *National Defense Strategy's* pronouncements that the "homeland is no longer a sanctuary" and that the DoD must achieve "information superiority" over its adversaries codified the need to develop a new operational concept for the Army [28].

In its simplest form, MDO is built upon a fundamental recognition that cyber and information technologies made "traditional methods" of offensive action (in one or two domains) all but obsolete [10]. Adversary courses of action (COAs) will instead combine effects throughout the land, maritime, air,

space, and cyberspace domains, as well as strike across the physical, information, and human dimensions of military action (see Figure 4). (Note that Joint and U.S. Army terminology for MDO and IA differs in places.) MDO functions as a type of prompt for commanders to fully understand and visualize the complexity of the modern operational environment relative to their position in it.

The Army's conception of IA presented in ADP 3-13 is similarly positioned. Many of the technical tasks that fall within its scope pertain to the DoD's equipment and systems: soldiers are to protect friendly data, information, and systems; counter adversarial efforts at electronic or cyber surveillance; and follow operational security practices to conceal friendly capabilities and intentions [7]. Even so, if ADP 3-13's definition of information as "data in context to which a receiver assigns meaning" comes to find more widespread adoption than its doctrinal predecessors, it will be, in part, because it stresses the practical and subjective nature of the information dimension [4, 5]. As one student of doctrinal history explained, IA will go "to the side that possesses better information and uses that information more effectively" [4].

One underappreciated aspect of the Army's information doctrine is recognizing that because ADP 3-13 is freely accessible online, the document may itself change what COAs in information warfare our adversaries may pursue. The PLA's information warfare officers in the SSF have unquestionably studied ADP 3-13 and are monitoring how the Army plans to implement its guidance. The SSF has also studied another Army doctrinal publication, FM 3-0, *Operations*, and paid close attention to its guidance on how to "conduct deployment operations contested by a peer threat" [10]. Central to preserving IA during a contested deployment is maintaining awareness that, to a considerable extent, the chance of a surprise attack of a previously unknown nature approaches the inevitable [29].

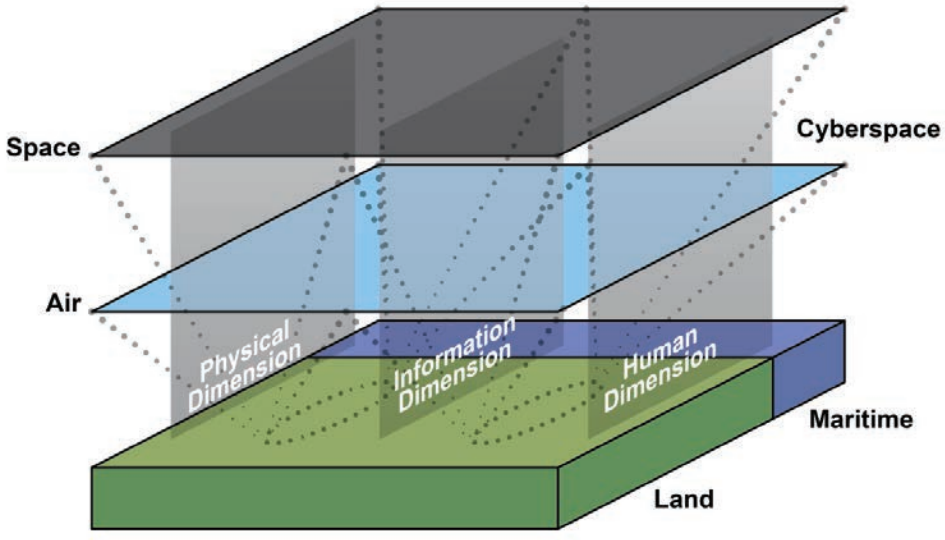


Figure 4. Domains and Dimensions of the MDO Operational Environment as Defined in U.S. Army Field Manual (FM) 3-0, Operations *(Source: U.S. Army [10])*.

Threat Courses of Action

In a fictionalized account written in 2021 for the U.S. Army Future Warfare Writing Program, Maj. Timothy M. Dwyer paints a truly chilling—and utterly plausible—tale. Soon, all the narrator's electronic devices, systems, networks, and digital accounts have been penetrated by the PLA's information forces [30]. On the morning he is to deploy to Hawaii, the internet-connected smart speaker in his daughter's room intones that "your mommy, your daddy, your sister, they will all die." After the soldier smashes it into oblivion, he finds that his home's other smart devices have been capturing indecent photos of his family—now uploaded to their social media accounts. His personal vehicle will not start, and then the electricity to his home is turned off. "I could barely get out of my house," the soldier recalls [30]. "Fat lot of good our carriers and tanks are when the fighting was all virtual."

The initial threat from a peer state will come in the form of cyber-based attacks on critical infrastructure nodes in the homeland. Hostile actors will

seek to incapacitate energy production networks, transportation, government administration, and other critical public services like water treatment systems [31]. Threat COAs will then use nonkinetic information attacks to disable DoD deployment systems like JOPES or the Defense Manpower Data Center and to delay or stop troop and materiel movements by disrupting key highways, bridges, and ports (see Figure 5) [32].

A peer threat may then turn to information warfare tactics to generate harmful cognitive effects in U.S. service members and the public at large [10]. Specifically, an information-capable adversary will (a) keep U.S. service members and units under constant reconnaissance, (b) seek to influence individual troops to preclude their mobilization, and (c) manipulate the public to possibly interfere with deployment operations.

> ***The initial threat from a peer state will come in the form of cyber-based attacks on critical infrastructure nodes in the homeland.***

Persistent Reconnaissance and Intelligence

Most adversarial efforts to contest a deployment will rely first on the ability to continuously fix and track U.S. forces. This is easier done than may be credibly imagined. Already, the battlefield has become "data-swept," littered with billions of networked devices that continuously share information. Like the smart speaker of Maj. Dwyer's story, such devices now create more cyberspace activity than people do directly; of that activity, an estimated 95+% of traffic remains unencrypted [34].

Writing in the *Military Review* in 2020, Army Cpt. T. S. Allen argues that we will soon "live in a world where most movement generates a cyberspace signature" [34]. The use of smartphones in Ukraine to record and share graphic clips of progress in combat is but one example of how media-enabled, open-source intelligence can be used to find and fix target locations and identify combatants [35]. More consequentially, as one DoD contractor recently demonstrated, capabilities currently exist to track smartphones in real time, without the aid of spyware, and to tie their data streams to discrete individuals even if anonymized. As a result, "smartphones can be repurposed as sensors without [the user] even being aware" [36].

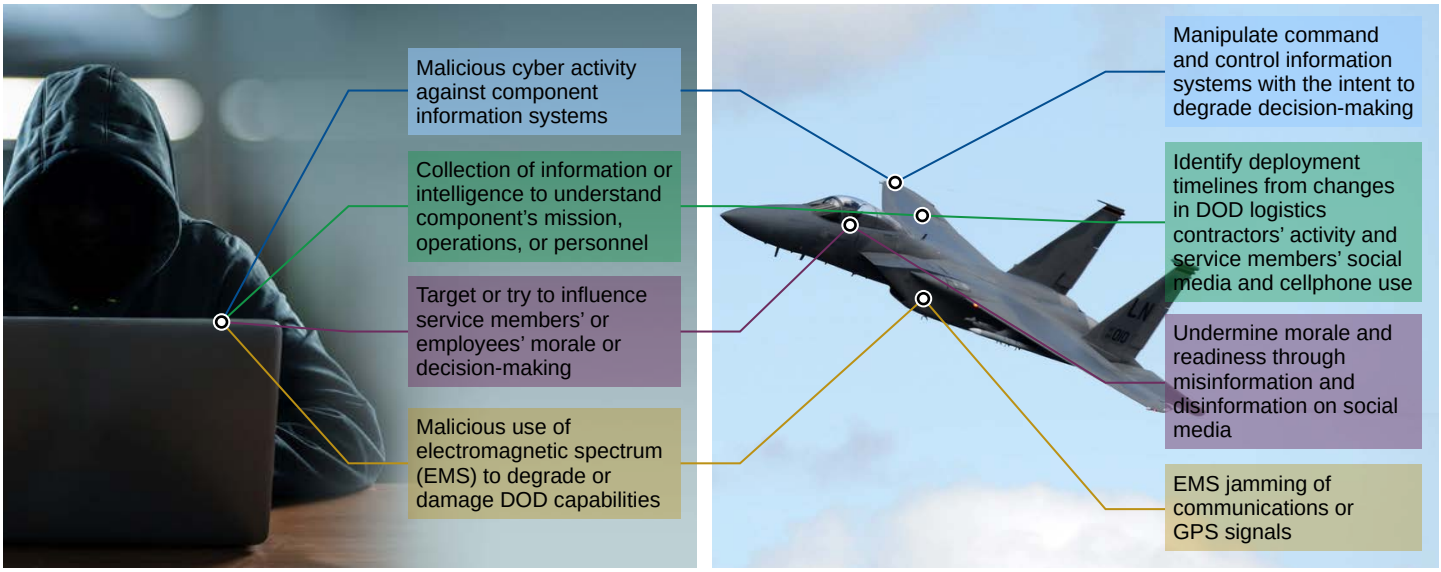


Figure 5. Example Threat Actions in the Information Dimensions *(Source: GAO [33])*.

The defense community has long recognized that U.S. military units generate a considerable degree of nonvisual signatures. While the use of the run-logging application Strava by troops in the Middle East in 2018 likely did not reveal any sensitive information about U.S. bases, it stands as a good reminder that American units are highly "trackable, traceable, and predictable" [37]. Similar geotagging practices were used in 2022 to trace the buildup of Russian infantry units prior to their ultimate invasion of Ukraine. Even if an American unit can shield themselves from any signature emissions during a deployment mission from fort to port, just the absence of the unit's normal routine patterns of life around its home installation will alert adversaries to its intentions. As Cpt. Allen notes, "every 'hidden' action … sparks an easily monitored reaction" [34].

Direct Influence

Persistent surveillance enables another COA—directly influencing Warfighters to preclude them from reporting for duty. While Maj. Dwyer's tale was fiction, his story has already found at least one analogue in the real world. During a 2019 NATO exercise, a "red team" of communications experts used open-source data to spoof the social media accounts of soldiers' loved ones. They then "catfished" many into leaving their posts—all for the princely sum of about $60 [38]. Russian forces have used similar tactics for deadly effects in Ukraine [39]. In one scenario, the parents of a targeted soldier will receive a text message that their child is dead, prompting them to call. Thus shaken, the soldier receives a text imploring them to "retreat and live" by heading to a marked location. A deadly artillery strike soon follows.

The sources of soldier coercion may be as simple as the previous example or based on highly specific information. In 2023, Duke University researchers found that detailed personal data on thousands of active-duty U.S. troops were readily accessible through data brokers, some via commonplace *.org* or *.asia* domains. Health data, financial records, and even religious affiliations could be bought as cheaply as $0.12 per record [40]. Elsewhere, U.S. intelligence leaders have pointed to efforts by genomics institutes in the PRC to tap into DNA databases of U.S. citizens as a first step toward future coercion [37]. In late 2023, hacks of two high-profile, family-history, genetic testing firms sought to extract the identities of those with Ashkenazi Jewish and Chinese heritage, seeking an as-of-yet unknown but chilling advantage over them [41].

Elsewhere, multiple active-duty troops (and veterans) have been radicalized through online forums in recent years, with some of them suborned into firing upon their colleagues [42]. During the stress of an LSCO deployment, the risk of prior nonviolent but still latent radicalization

resulting in a call to action—or simply of Warfighters falling prey to malign phishing attacks—will be acute [33]. Soldier ability to maintain the highest levels of cognitive understanding may also suffer (see Figure 6). In Maj. Dwyer's story, he recounts a scene in which the narrator hears an unconfirmed radio report of the PLA sinking two American carrier strike groups (CSGs) near Guam. Properly incredulous at first, the narrator then hears the same news from his father via text message before seeing expertly simulated video footage of the carrier group's destruction played on a major news outlet. His commander concludes that he "must assume that two CSGs were destroyed" [30].

Public Interference

As real-time information streams have come to dominate global media-content consumption, it has become commonplace to say that "contemporary wars are largely wars of influence" or ones fought by narratives [43]. Russian disinformation campaigns are produced for

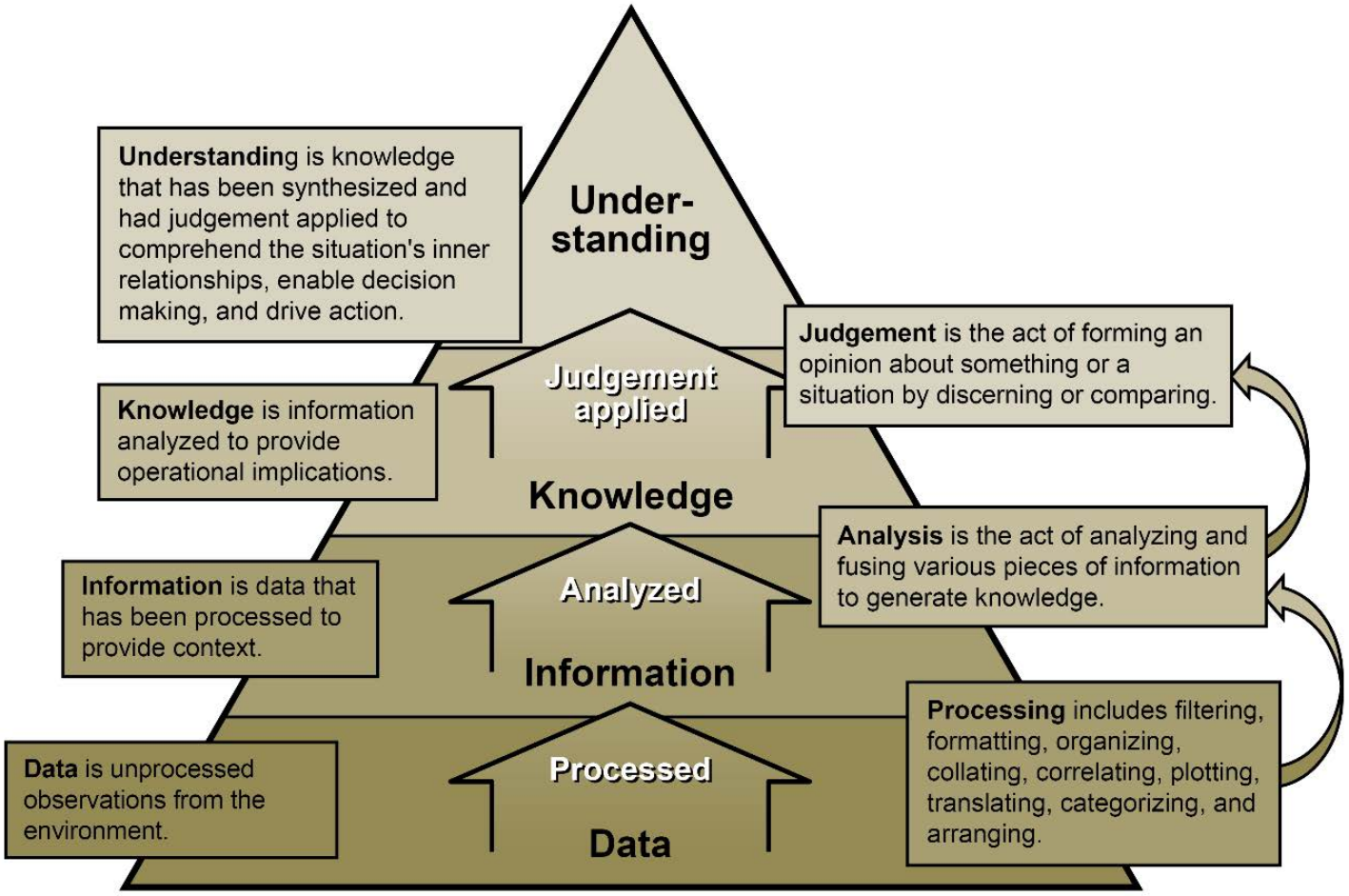


Figure 6. Cognitive Hierarchy: How Humans Progressively Assign Meaning to Data Into Understanding *(Source: U.S. Army [7]).*

dissemination in large volumes and often push grand, overarching stories to gradually influence public opinion [44]. Indeed, this has already been done to great effect, stretching over decades of time. In the 1970s and 1980s, a Russian disinformation campaign effectively spread whispers that the HIV/AIDS epidemic was the secret product of U.S. government biological research [45]. The distrust in public health officials caused by this still lingers today.

As social media-based information warfare matures, however, an aperture has opened for adversaries to deploy targeted, specific influence campaigns to achieve near-term objectives. Indeed, the PLA's SSF believes that warfare in the cognitive dimension is most effective when "telling partial truths" and in small doses [46]. Doing so helps recruit the widest possible range of adherents and may better spur them to action.

An emerging concern stems from as-of-yet-unclear future uses of artificial intelligence (AI). In 2019, the PLA added the AI-enabled "intelligentized" warfare to its already-robust informationized warfare capabilities [47]. The widespread use by young Americans of the Chinese-owned mobile phone app TikTok (now notorious for its rapid spread of propaganda), combined with the propensity of existing chat-based, generative-AI, large language models to report false statements, has created an exceptionally large information space for public manipulation [48].

The opportunities for turning public opinion against U.S. deployment operations will scale with the size of the expeditionary force mobilized. Threat COAs may inflame antiwar sentiments among local groups and push them to rush military convoys

> ***An emerging concern stems from as-of-yet-unclear future uses of artificial intelligence (AI).***

in transit or to occupy naval vessels or airframes set to embark. Indeed, a group of protestors in November 2023 achieved just such an aim, albeit for only a few hours [49]. They blocked the Ready Reserve Force supply ship *MV Cape Orlando* from departing Oakland before they were arrested and perimeter control was restored (note that there is no known evidence of foreign interference or influence upon the group).

Some aspects of the DoD's force projection architecture are particularly vulnerable to this type of event. For instance, a scholar at the Brookings Institution estimated in 2013 that nearly 50% of military cargo needed in the early stages of an overseas contingency operation would flow through a single point—the Port of Beaumont [32]. Outside of targeting military installations directly, peer adversaries are likely to stage small, irregular attacks at major public events like a Major League Baseball game or the Indianapolis 500 to tie up countless law enforcement and National Guard assets and further hinder the normal flow of traffic and commerce.

CONCLUSIONS

Improved technology can certainly help the DoD protect its forces and the American public from malign narratives from adversarial threats. The Army Research Office is already funding advanced research into applying high-speed computational servers to the task of processing large volumes of multimodal online media content in real time to quickly identify and combat coordinated cognitive attacks like those envisioned by the PLA [50].

However, IA's emphasis on the value of turning data, information, and knowledge into understanding is a strong hint toward another solution set. The risk of overreliance on big data analytics may be to downplay critical thought, adaptive expertise, and creativity in warfare to predict or perceive that the threat is being fully tracked and managed [51]. At a minimum, U.S. Warfighters might first dust off their analog tools of yore and refamiliarize themselves to the chalkboards, printed maps, and spoken-word orders that currently remain unhackable [52]. For the central virtue of IA rests not in the digital realm but in the soldier—its critical tasks are "seeing yourself" and understanding the operational environment "while denying the same to your adversary" [53]. ■

REFERENCES

[1] Stapleton, R. A. "Three Perspectives on the Information Technologies and National Security: War Fighting, Diplomacy and Intelligence." Computer Professionals for Social Responsibility, http://cpsr.org/prevsite/conferences/cfp93/stapleton.html, June 1993.

[2] Warriner, A. "The Pizza Meter." http://home.xnet.com/~warinner/pizzacites.html, 1997.

[3] Miller, M. "What Can Pizza Tell Us About Ourselves?" *Slate*, https://slate.com/human-interest/2016/07/the-pizza-meter-was-a-staple-of-1990s-pop-pseudoscience-we-should-revive-it.html?pay=1701964280669&support_journalism=please, 29 July 2016.

[4] White, S. P. "The Organizational Determinants of Military Doctrine: A History of Army Information Operations." *Texas National Security Review*, vol. 6, no. 1, pp. 51–78, http://dx.doi.org/10.26153/tsw/44440, Winter 2022–2023.

[5] Ross, R. J. "Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art During Multi-Domain Operations." *Cyber Defense Review*, https://cyberdefensereview.army.mil/Portals/6/Documents/2021_fall/06_Ross_CDR_V6N4-Fall_2021.pdf?ver=aj3AhXhZLEGojxeZ2Gb42A%3d%3d, Fall 2021.

[6] Harper, J. "Pentagon Unveils New Strategy for Operating in the Information Environment." *DefenseScoop*, https://defensescoop.com/2023/11/17/pentagon-unveils-new-strategy-for-operating-in-the-information-environment/, 17 November 2023.

[7] U.S. Army. *Information*. ADP 3-13, Washington, D.C.: Headquarters, Department of the Army, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39736-ADP_3-13-000-WEB-1.pdf, November 2023.

[8] U.S. DoD. 2022 *National Defense Strategy of the United States of America*. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF, 27 October 2022.

[9] U.S. Department of the Navy. *The Department of the Navy Cyber Strategy*. https://media.defense.gov/2023/Nov/21/2003345095/-1/-1/0/DEPARTMENT%20OF%20THE%20NAVY%20CYBER%20STRATEGY.PDF, 21 November 2023.

[10] U.S. Army. *Operations*. FM 3-0, Washington, D.C.: Headquarters, Department of the Army, https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1025593, 1 October 2022.

[11] Gamble, D. A. "Driving Modernization, Maintaining Readiness: Aligning Sustainment's Role and Efforts in the Push to 2035." *Army Sustainment*, PB 700-21-03, Headquarters, Department of the Army, pp. 6–7, https://alu.army.mil/alog/ARCHIVE/PB7002103FULL.pdf, July–September 2021.

[12] Kretchik, W. E. *U.S. Army Doctrine*: *From the American Revolution to the War on Terror*. Lawrence: University Press of Kansas, 2011.

[13] Ancker, C. J. "The Evolution of Mission Command in U.S. Army Doctrine, 1905 to the Present." *Military Review*, Fort Leavenworth, KS: Army University Press, pp. 42–52, https://usacac.army.mil/sites/default/files/documents/mccoe/TheEvolutionOfMissionCommandInArmyDoctrine.pdf, March–April 2013.

[14] Endress, C. A. "Mobilization (Historical Bibliography No. 7)." Fort Leavenworth, KS: U.S. Army Command and General Staff College, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/endress.pdf, 1987.

[15] Matthews, J. K., and C. J. Holt. *So Many, So Much, So Far, So Fast*: *United States Transportation Command and Strategic Deployment for Operation Desert Shield/Desert Storm*. Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, and Research Center, U.S. Transportation Command, https://apps.dtic.mil/sti/pdfs/ADA323609.pdf, 1996.

[16] Canan, J. W. "Up From Nifty Nugget." *Air & Space Forces Magazine*, https://www.airandspaceforces.com/article/0983nifty/, 1 September 1983.

[17] Getler, M. "Make-Believe Mobilization Showed Major Flaws." *The Washington Post*, https://www.washingtonpost.com/archive/politics/1980/07/24/make-believe-mobilization-showed-major-flaws/e6d0c81b-22a3-4ac0-9b46-2e334d5d3f70/, 24 July 1980.

[18] U.S. Army. "Army Deployment and Redeployment Processes and Procedures." Pamphlet 525–93, Washington, D.C.: Headquarters, Department of the Army, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34280-PAM_525-93-000-WEB-1.pdf, 6 October 2023.

[19] Pearson, D. E. *The World Wide Military Command and Control System*: *Evolution and Effectiveness*. Maxwell Air Force Base, AL: Air University Press, https://apps.dtic.mil/sti/pdfs/ADA379709.pdf, June 2000.

[20] U.S. Army Center of Military History. *War in the Persian Gulf*: *Operations Desert Shield and Desert Storm*, CMH Pub 70-117-1, Washington, D.C., https://history.army.mil/html/books/070/70-117-1/CMH_70-117-1.pdf, 2010.

[21] Isreal, E. M. "Operational Logistics During the First Gulf War." Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, https://apps.dtic.mil/sti/trecms/pdf/AD1159141.pdf, May 2020.

[22] Kindsvatter, P. S. "VII Corps in the Gulf War: Deployment and Preparation for Desert Storm." *Military Review*, Army University Press, pp. 1–16, https://www.armyupress.army.mil/Portals/7/PDF-UA-docs/Kindsvatter-UA.pdf, January 1992.

[23] Air Mobility Command Public Affairs. "20 Years After Operations Desert Shield, Desert Storm: Airlift Effort Was Compared to 'Moving a Small City' [Image 2 of 3]." DVIDS: Defense Visual Information Distribution Service, Photo ID 900901-F-AB111-001, https://www.dvidshub.net/image/376190/20-years-after-operations-desert-shield-desert-storm-airlift-effort-compared-moving-small-city, 1 September 1990.

[24] Mansky, J. "Operation Desert Storm Was Not Won By Smart Weaponry Alone." *Smithsonian Magazine*, https://www.smithsonianmag.com/history/operation-desert-storm-was-not-won-smart-weaponry-alone-180957879/, 20 January 2016.

[25] Reardon, T. M. "Information Warfare: Protecting Force Sustainment." *Military Intelligence Professional Bulletin*. U.S. Army Intelligence Center of Excellence, https://irp.fas.org/agency/army/mipb/1997-1/reardon.htm, January–March 1997.

[26] Dahm, M. "China's Desert Storm Education." *Proceedings*, vol. 147/3/1,417, U.S. Naval Institute, https://www.usni.org/magazines/proceedings/2021/march/chinas-desert-storm-education#:~:text=PLA%20lessons%20learned%20from%20the%20Gulf%20War%20led,war%20that%20drives%20PLA%20force%20structure%20and%20strategy, March 2021.

[27] U.S. DoD. 2023 *Military and Security Developments Involving the People's Republic of China*: *Annual Report to Congress*. Washington, D.C., https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF, November 2023.

[28] Fawcett, G. S. *History of US Army Operating Concepts and Implications for Multi-Domain Operations*." Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, https://apps.dtic.mil/sti/pdfs/AD1083313.pdf, 2019.

[29] Horner, C. A. "What We Should Have Learned in Desert Storm, But Didn't." *Air & Space Forces Magazine*, https://www.airandspaceforces.com/article/1296horner/, 1 December 1996.

[30] Dwyer, T. M. "The American Maginot Line." Fort Leavenworth, KS: Army University Press, *Military Review*, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2021/Dwyer-American-Maginot-Line/, September–October 2021.

[31] U.S. Army. "The Operational Environment and the Changing Character of Warfare (TRADOC Pamphlet 525-92)." Fort Eustis, VA: Training and Doctrine Command, https://adminpubs.tradoc.army.mil/pamphlets/TP525-92.pdf, 7 October 2019.

[32] Tussing, B. B., J. E. Powell, and B. C. Leitzel. *Contested Deployment*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College Press, U.S. Army War College, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1944&context=monographs, 2022.

[33] U.S. Government Accountability Office. "Information Environment: Opportunities and Threats to DOD's National Security Mission." GAO-22-104714, https://www.gao.gov/assets/gao-22-104714.pdf, September 2022.

[34] Allen, T. S. "Finding the Enemy on the Data-Swept Battlefield of 2035." *Military Review*, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2020/Allen-Data-Swept-2035/#:~:text=On%20the%20data%2Dswept%20battlefield%2C%20the%20armed%20force%20best%20postured,to%20win%20in%20these%20conditions, November–December 2020.

[35] Perrigo, B. "How Open Source Intelligence Became the World's Window Into the Ukraine Invasion." *Time*, https://time.com/6150884/ukraine-russia-attack-open-source-intelligence, 24 February 2022.

[36] Ford, M. "Ukraine, Participation and the Smartphone at War." *Political Anthropological Research on International Social Sciences*, vol. 4, no. 2, pp. 219–247, https://brill.com/view/journals/pari/4/2/article-p219_005.xml, December 2023.

[37] Smith, M., and N. Starck. "Open-Source Data Is Everywhere—Except the Army's Concept of Information Advantage." Modern War Institute at West Point, https://mwi.westpoint.edu/open-source-data-is-everywhere-except-the-armys-concept-of-information-advantage, 24 May 2022.

[38] Pickrell, R. "NATO Troops Were Located, Tricked Into Disobeying Orders in Research Experiment." *Military.com*, https://www.military.com/daily-news/2019/02/20/nato-troops-were-located-tricked-disobeying-orders-research-experiment.html, 20 February 2019.

[39] Collins, L. "Russia Gives Lessons in Electronic Warfare." Association of the United States Army, https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare, 26 July 2018.

[40] Sherman, J., H. Barton, A. Klein, B. Kruse, and A. Srinivasan. "Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security." Sanford School of Public Policy, Duke University, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf, November 2023.

[41] Katersky, A. "Connecticut Attorney General Presses 23andMe for Data Breach Answers." *ABC News*, https://abcnews.go.com/US/connecticut-attorney-general-presses-23andme-data-breach-answers/story?id=104510476, 31 October 2023.

[42] Posard, M. N., L. A. Payne, and L. L. Miller. "Reducing the Risk of Extremist Activity in the U.S. Military." PE-A1447-1, RAND Corporation, https://doi.org/10.7249/PEA1447-1, September 2021.

[43] Maan, A. "Narrative Warfare." Weaponized Narrative Initiative, Arizona State University, https://weaponizednarrative.asu.edu/publications/narrative-warfare, 3 April 2018.

[44] OECD. "Disinformation and Russia's War of Aggression Against Ukraine: Threats and Governance Responses." https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/#boxsection-d1e348, 3 November 2022.

[45] Kramer, M. "Lessons From Operation 'Denver,' the KGB's Massive AIDS Disinformation Campaign." *The MIT Press Reader*, https://thereader.mitpress.mit.edu/operation-denver-kgb-aids-disinformation-campaign/, May 2020.

[46] Davis, C. "Cognitive Warfare: China's Effort to Ensure Information Advantage." *Military Intelligence*, https://mipb.army.mil/articles/jul-dec-2023/cognitive-warfare, July–December 2023.

[47] Takagi, K. "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine." *War on the Rocks*, https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine, 22 July 2022.

[48] Tucker, P. "How Often Does ChatGPT Push Misinformation?" *DefenseOne*, https://www.defenseone.com/technology/2024/01/new-paper-shows-generative-ai-its-present-formcan-push-misinformation/393128/?oref=d1-skybox-hp, 4 January 2024.

[49] Castaneda, C. "Pro-Palestinian Protesters Delay Military Supply Ship From Departing Port of Oakland." *CBS San Francisco*, https://www.cbsnews.com/sanfrancisco/news/pro-palestinian-protesters-block-military-supply-ship-at-the-port-of-oakland, 3 November 2023.

[50] Talk Business & Politics. "UA Little Rock Receives $5 Million From U.S. Army to Study Information Campaigns." https://talkbusiness.net/2023/11/ua-little-rock-receives-5-million-from-u-s-army-to-study-information-campaigns, 27 November 2023.

[51] Ross, C. "The Unknowable Future of Warfare." *The Strategy Bridge*, https://thestrategybridge.org/the-bridge/2023/3/20/the-unknowable-future-of-warfare, 30 March 2023.

[52] Nelson, C., and A. Rhodes. "Embrace Analog Tools in a Digital Intelligence Age." *Proceedings*, vol. 146/10/1,412, U.S. Naval Institute, https://www.usni.org/magazines/proceedings/2020/october/embrace-analog-tools-digital-intelligence-age, October 2020.

[53] Myatt, S. "Impending TRADOC Document Outlines Pathway for Army to Achieve Information Advantage; Lt. Gen. Maria Barrett Quoted." *GovConWire*, https://www.govconwire.com/2022/07/arcyber-document-explores-army-information-advantage, 13 July 2022.

BIOGRAPHY

JOEL HEWETT is an energy policy and national defense researcher, writer, and analyst for KeyLogic, where he applies more than 15 years of experience in assessing the utility of advancements in science and technology. In his role, he supports multiple federal agencies in studies addressing energy systems and critical infrastructure protection issues. Among his published works is a state-of-the-art report for the Homeland Defense & Security Information Analysis Center on military microgrids, "Resilience by Design: Microgrid Solutions for Installation Energy." Mr. Hewett holds an M.S. from the Georgia Institute of Technology in the history and sociology of technology and science and an A.B. in literature from Davidson College.

CHEM-BIO, DATA, AND CYBERSCIENCE AND TECHNOLOGY

IN DETERRENCE OPERATIONS

BY JAMES GIORDANO (PHOTO SOURCE: BLACKJACK3D [CANVA] AND BILLIONPHOTOS [CANVA])

INTRODUCTION

"… the very spark that marks us as a species … our tool-making, our ability to bend [nature] to our will … also give us the capacity for unmatched destruction."

—*Barack Obama* [1]

The twentieth century evidenced the increasing use of state-of-the-art science and technology (S&T) in warfare. Included in this S&T armamentarium were new chemical and biological agents that could be yoked to extant forms of S&T (e.g., aircraft, ordnance, etc.) to facilitate delivery in kinetic engagements [2]. Such changes in the instruments of warfare served as impetus for formulating international signatory treaties and conventions (e.g., The Chemical Weapons Convention [CWC] and Biological Toxins and Weapons Convention [BTWC]) to govern these agents' development and use [3]. However, recent advancements and interdisciplinary convergence in chemical, biological, data, computational, and engineering fields have enabled creation of chem-bio agents that are not (currently) regulated by these governances and, when taken together, can establish significant deterrent leverage in nonkinetic and kinetic domains [4, 5].

THE 5 D's OF DETERRENCE

Deterrence involves insight, planning, development of structural and functional resources, engagement of personnel and services, and use of methods and tools aimed at influencing (in multidirectional ways) the intent and activities of individual and collective others. In the main, deterrence entails and obtains five essential domains of effect (i.e., the 5 D's of Deterrence), which are not mutually exclusive and can and arguably should be interactive, complimentary, and reciprocal in both articulation and effect as follows:

Definition of those enterprises and efforts that can be identified as representative foci (i.e., targets) for deterrent influence. The nature and extent of these targets are important to terminating the directionality of deterrence, i.e., by suppressing certain elements, factors, endeavors, and effects and/or fortifying others to shape the trajectory and valence of desired outcomes.

Detection of those burdens, risks, and threats that constitute relevant fields and forces that are to be defined, identified, and targeted. Detection of the targetable elements should include both quantitative and qualitative descriptive metrics and qualitative metrics that describe what, why, and how certain factors pose burden, risk, and threat requiring deterrent intervention. Quantitative metrics

provide evidentiary support for the currency and extent of burden, risk, and threat incurred.

Determination of required tactics and strategies of deterrent engagement. Such methods are aimed at qualifying and quantifying required resources, services, and personnel necessary to maintain a defensible status quo vs. those variables necessary to induce and enable protracted directional change. In both cases, calculation of gains and losses incurred by omission of deterrent intervention, as well as commission of deterrent intervention, can and should be incorporated into the overall relative cost projections of fiscal, temporal, personnel expenditures, and losses.

Disruption of relative status quo to induce and sustain deterrent action and effect upon identified targets. Disruption is directional, and the trajectory of disruptive intent and plotting of effects should focus upon the valent goal(s), as well as possible off-goal effects that could occur because of disruptive drift and/or postdisruptive reaction by the targeted source. It is important to recognize and plot as best possible those disruptive effects incurred by deterrent intervention in the short term (within 2 to 12 months), intermediate term (13–36 months), delayed (37–60 months), and possible long-term (60–120 months) manifestations. Modeling and forecasting deterrent and disruptive effects beyond the 120-month horizon have become difficult, if not impossible, in certain cases because of (1) fractal diffusion of applied deterrent interventions and effects and (2) multifactorial reaction and response patterns (both by the target of deterrence and affiliated allied and/or interactive entities within the dynamic system affected) [5].

Diminution of risk and threat, either by eliminating or revising threat sources and resources, or by instituting countering resources and variables that redirect laws, intentions, activities, and outcomes of the identified target focus. Diminution of threat can be (1) mitigative (i.e., decreasing existing burdens and risks that pose current or future term threat) or (2) preventive (i.e., proactively impeding activities that can and likely will pose risk and/or threat). In both instances, such diminution can involve destructive and disruptive (i.e., restructuring) elements and activities to eliminate or reestablish constructs, conditions, and contexts of effect within the target and its zone(s) of operational influence.

DIMENSIONS OF DETERRENT EFFECT(S)

Deterrence methods can be engaged proactively, reactively, nonkinetically, or kinetically based upon exigencies, contingencies, and particular allowances and constraints of the engagement space and (geo-socio-political) environment.

Deterrence methods can be engaged proactively, reactively, nonkinetically, or kinetically.

Proactive deterrence seeks to provide means and methods that exert influential force upon identified targeted burdens, risks, and threat resources to suppress, if not eliminate, current and ongoing development of force strengths and capabilities that have been identified as posing current and/or near-term problems and/or danger to the deterring agents (and/or the stability and security of an identified system/environment).

Reactive deterrence is directed activity against an identified clear and present burden, risk, or threat to mitigate the extent of negative impact, redirect current and near-term manifestations, and/or influence current and future conduct of same or similar activities; it can reduce the relative calculus of burden, risk, and/or incurred threat.

Nonkinetic deterrence involves influence operations to include soft weapons (of economics, policy, law, and/or ecological and environmental influence) to leverage relative power in ways relevant to exercising hegemonic control.

Kinetic deterrence involves the use of military and intelligence force, characteristically by the actual employment of methods and tools (i.e., as weapons) of disruption and/or destruction in accordance with defined parameters of hostile activity (in either defensive or offensive postures).

CHEM-BIOSCIENCE AND TECHNOLOGY IN/FOR DETERRENCE OPERATIONS: EFFECTS AND VECTORS

During the 20th century, chemical and biological agents have emerged as viable elements in national deterrence initiatives. Various chemicals, toxins, and microbes (e.g., sarin, ricin, and anthrax) have been considered as tools for political and military deterrence. The potential for chemical and bioterrorism via the use of such agents by states and nonstate actors poses significant challenges to current and near-term global security [6, 7].

Chemical and biological deterrence obtains the following three primary dimensional effects:

1. Fear factor - The primary aim of using chemical and biological agents for deterrence is to instill fear in adversaries. The threat of chemical or biological attacks can make opponents reframe intentions and actions considering (real or perceived) burdens, risks, and threats induced by nonkinetic or kinetic use of such implements. Additionally, fear(s) that a competitor or adversary has such agents can influence narratives, attitudes, and actions about the relative viability and value of existing treaties and signatory conventions aimed at governing their development and use and, in ways, foster implicit or explicit brinksmanship in this space.
2. Ambiguity and uncertainty - The mere possession of these agents, or ambiguous statements regarding their potential use, can create uncertainty and deter competitors and potential adversaries. The fear of a recognized or unknown chemical/biological threat can significantly influence decision-making processes—and resultant political, economic, and military postures—of opposing parties.
3. Economic (e.g., low cost and high impact) - Chemical and biological agents can be relatively inexpensive to produce and deploy compared to more "conventional" weapons. Their potential to cause widespread disruptive effects with plausibly destructive (ripple) manifestations and limited investment (i.e., "costs") and considerable impact (i.e., "gain) makes them attractive tools for nonkinetic or kinetic (pro- and/or reactive) deterrence [8–10].

These effects can be employed and leveraged in and across several engagement vectors and settings, which include the following:

Nations' dual-use research projects and programs - The dual-use nature of many nations' chemical/biological research enterprises, which can have benevolent biomedical and more "grey zone" if not explicitly disruptive (and manifestly destructive) effects, complicates international efforts to satisfactorily surveille, assess, and govern their development and use [11, 12]. Such dual-use research of concern (DURC), while defined by extant multinational conventions, remains somewhat problematic to evaluate given (1) categorical limitations of those research directions and products currently identified as potentially problematic and of concern, (2) growing progress in gene editing and synthetic biologic methods that could render currently "innocuous" substances and agents as pathogenic and disruptive, and (3) the architecture(s) and activities of competitor nations' industrial/commercial efforts that remain veiled and thus shielded by corporate proprietary interests and protections [13, 14].

Development and use by nonstate actors - An increasing number of nonstate actors are active in this Chem-Bio and Data and Cyberscientific and Technological (CB-DCST) space either as

independent entities or designated proxies for nation-states' operations [10]. Nonstate actors can acquire chemical/biological capabilities via (1) acquisition of nation state-developed tools and products, (2) provision/acquisition of nation states' methods for developing and deploying such agents, and/or (3) specifically dedicated efforts of research, development, and utilization of these agents. These variables further complexify international efforts at oversight and deterrence (of such groups' operations) while concomitantly fortifying their collectives' deterrence capabilities [15].

Verifying nations' and nonstate actor groups' compliance with international treaties and conventions regarding chemical and biological agents (e.g., BTWC, CWC, Declarations of Helsinki, EU Exportation Regulations, etc.) presents challenges of oversight and enforcement. Access to accurate intelligence is crucial to assessing iterative developments in chem-bio S&T (CBST) that pose current risk and potential threats and effectively deterring their use [16]. However, relatively seamless infrastructures and functions of trans-Pacific and Atlantic peer competitor nations' "triple helix" of government, academic research, and commercial/industrial enterprises, as fortified by their national legal parameters, makes direct insight to potential DURC difficult and fosters impediments to "deep surveillance"—absent what would constitute apparent violations of internationally recognized intellectual property law(s) [17, 18].

Verifying nations' and nonstate actor groups' compliance with international treaties and conventions regarding chemical and biological agents presents challenges of oversight and enforcement.

In light of such gaps in regulatory oversight and governance, and as evidenced by the COVID crisis, there is a real risk of accidental release of chem-bio agents leading to unintended consequences and significant disruption of public health, national stability, and biosecurity, with proximate and more distal destructive effects in a variety of dimensions (e.g., economic, social, political, military) and on a range of scales (e.g., organizational, institutional, local, regional, national, and global) [19–23]. This risk underscores the importance of and need for deterrence postures to mitigate or prevent such trajectories of probable and possible effect, which could be intentionally or unintentionally incurred by competitor groups' activities in this space.

The use of chemical and biological agents for political and military deterrence operations is a complex and contentious issue which remains a serious concern for reasons of (1) ongoing enterprises in this space by peer-competitor, proxy nations, and nonstate actors; (2) the relative facility of research and development (R&D) capabilities facilitated by current innovations in gene editing, synthetic biology, and reciprocal engagement of data/cyber S&T; and (3) relative opacity of extant (international) policy, treaties, and laws of oversight, surveillance, regulation, and governance. Thus, the potential—if not probability—for such methods, tools, and products to be employed and leveraged in nonkinetic and/or kinetic deterrence operations is clear and present and hence poses demonstrable risk and threat(s) to U.S. and allied biosecurity and biodefense. This risk and threat become forever viable given the capabilities conferred by using data and computational S&T in ways that fortify and augment research, development, and use applications and venues of chem-bio methods and agents.

DATA AND CYBERSCIENCES AND TECHNOLOGY: MACHINE LEARNING (ML) AND ARTIFICIAL INTELLIGENCE (AI)

As previously noted [24, 25], big data and cyberscientific and technological tools and methods (e.g., ML and iterations of AI) are force multipliers for research, development, and use of various types of CBST. Ongoing progress in neurocognitive S&T has

facilitated further development of ML/AI via innovations in neuromorphic computing systems' design and construction [26, 27]. As shown in Figure 1, this has created an "operationalizable omnibus" of S&T wherein impacts are generated by the constituent parts as fortified by a de-siloed, force-multiplied approach to R&D and utility in practice (i.e., a mereoform typology) and the entirety (i.e., a holoform typology)—as a combinatory entity (CB-DCST).

The military domain has witnessed significant advancements and applications of DCST-powered systems inclusive of data and ML/AI-optimized analytics (if/when coupled to aforementioned tools and methods of CBST) to develop "precision pathologies" capable of maximally disruptive effects on targeted individuals and/or groups and the development (and increasing use) of weaponry with varying degrees of human-dependent and governed independence and autonomy [28]. The iterative superiority and deployment of such DCST-driven capabilities can exert significant deterrent influence over peer-competitor/potential adversarial nations' nonkinetic and/or kinetic engagement and activities in this space (see Figure 2). In the figure, the interactive domains and dimensions of DC/CBST, when taken individually or in combination, can be utilized in (1) nonkinetic ("soft weapon") influence/deterrent operations to affect economics, biopsychosocial narratives, sentiments, and actions of targeted individuals and groups (engaging and influencing social and physical ecologies on various scales and levels) and (2) kinetic ("hard weapon") operations, in which disruption characteristically involves/incurs more destructive effect(s) by using information, cyber- and/or chem-bio warfare. (Note that DCST and/or CBST can be used nonkinetically and/or kinetically in covert, clandestine, overt, or combinatory ways.)

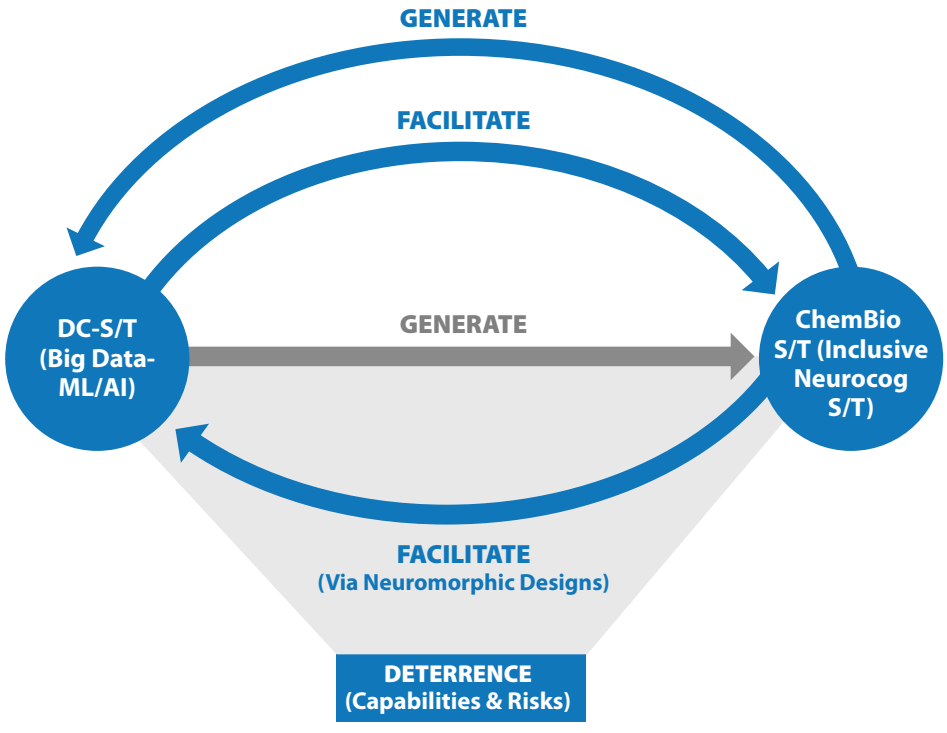


Figure 1. Diagram of the Interaction(s) and Reciprocity of Force Multiplication of Big Data, Cyber, and CBST *(Source: J. Giordano)*.

> ***The military domain has witnessed significant advancements and applications of DCST-powered systems inclusive of data and ML/AI-optimized analytics to develop "precision pathologies" capable of maximally disruptive effects on targeted individuals and/or groups.***

TOWARD PREPAREDNESS

Considering ongoing developments in CB-DCST, it is both reasonable and realistic to presume and acknowledge that current (radical levelling) and emergent methods and tools can and will be employed for deterrence initiatives and operations on the 21st century global stage. Furthermore, the

Figure 2. Diagram of Interactive DCST and CBST Domains and Dimensions *(Source: J. Giordano).*

multinational engagement of scientific and technological research establishes a basis for many states to exercise capabilities in this sphere. Current efforts in the CB-DCST spaces have been described in a series of advisory reports from the National Research Council commissioned by the United States Army and Defense Intelligence Agency during the early part of the 21st century [29, 30]. These reports offered recommendations for the military intelligence communities to identify and pursue CB-DCST for operational use. Subsequent reports, including several white papers of the Strategic Multilayer Assessment Branch of the Joint Staff, Pentagon have acknowledged that CB-DCST has high potential for present operational use in a variety of security, intelligence, and defense deterrent enterprises [31–34].

Of note is the imposing possibility to incur deterrence through "changing minds and hearts" by altering the will or capacity to fight and/or idiosyncratic and collective cognitive, emotional, and behavioral domains using singular or combined use of CB-DCST tools and methods [35]. Such applications and effects include, but would not be limited to, the following:

1. Modifying cognitive constructs and resultant emotions and behaviors,
2. Mitigating aggression and directing or influencing cognitions and emotions of affiliation or passivity,
3. Incurring disruptive effects (e.g., resource paucity and resultant burden of lifestyle) and directly incurring morbidity and/or disability; in these ways, neutralizing competitors' and/or potential opponents' capacities in multiple domains of social and international engagement, and
4. Inducing indirect or direct destructive effects, (against infrastructures, resources, various functions, and mortal effects against humans, agricultural stocks, etc.).

It is important to recognize that even nonkinetic engagement of deterrence means and methods can be provocative, if not contentious, as these may be regarded as elements and activities of biopower [36]. In this light, it is opined that when attempting to balance benefits, burdens, risks, and harms of deterrence operations in the context of nonkinetic, preemptive, and preventative activity (defensible under a construct of justification to prevent war, i.e., jus contra bellum), as well as kinetically (within operational parameters of just war theory, i.e., jus ad bello/jus in bellum), any such methods and outcomes will need to be considered compared to those produced by more traditional means, inclusive of policy and warfare (with the latter entailing consideration of past and present availability and use of existing armaments like explosive, radiological, and nuclear devices and emergent developments in CB-DCST) [37].

Given multinational enterprises in CB-DCST, it is naive to think that the same trends that compelled the development and use of these tools for disruptive and deterrent influence will be impeded merely by considerations of (1) burdens and risks that might arise as S&T advances ever farther into frontiers of the unknown, (2) potential harms that such advances could

intentionally or unintentionally occur, and (3) ethical legal and sociopolitical issues instantiated by positive and negative effects of implications of S&T advances for deterrent aims and ends. Thus, a simple precautionary principle in which risk benefit ratios determine the trajectory and pace of scientific and technological advancement is not tenable on an international level. This is because there is real possibility—if not probability—that competitive nations and/or insurgent groups could fund and clandestinely, if not covertly, conduct research, development, test, and evaluation (RDT&E) of such S&T beyond the auspices and influences of the United States and its allies' guidelines and policies.

Instead, a process that entails some measure of precaution together with significant preparedness will be required [38, 39]. Such preparedness mandates knowledge of what technological accomplishments can be achieved given incentives and resources currently available and afforded; whether such work is being prepared and/or conducted; what groups are involved in such efforts; overt and/or covert intentions and purposes of these activities; possible scenarios, effects, and consequences that could arise from various levels of scientific and technological progress and their use; and what (deterrent) measures can and should be taken to counter risks and threats posed by such progress and its effects [40, 41]. For this approach to work, surveillance is necessary, although international oversight and governance of novel CB-DCST RDT&E may be difficult. What can be governed and regulated are those ways in which these aspects of S&T efforts are conducted in and employed by U.S. agencies in conjunction and cooperation with international (political, economic, and military) allies.

CONSIDERATION OF ETHICO-LEGAL AND SOCIAL ISSUES

Ethical questions need to be pragmatically posed and prudently addressed in balance with the interests of the public (i.e., national) security and protection, as well as key elements of global standing and global power [42, 43]. CB-DCST can and will be engaged to evoke outcomes relevant to national security, intelligence, and defense operations by countries and nonstate entities to achieve goals that may be contrary to the public welfare interests of the United States and its allies. As history has shown, a dismissive posture that fails to recognize and acknowledge the reality of these risks and threats increases the probability of susceptibility to possible, if not probable, harm in an open society.

In an open society, it is the responsibility of government to protect the polis [44]. This will necessitate efforts to establish proactive defensive knowledge of those S&T capabilities and the vulnerabilities that they exploit to recognize how CB-DCST could be used to leverage deterrent power and develop stances in readiness and response to such realities. A meaningful stance of preparedness requires rigorous analysis and addressing of the technical and ethical, legal, and social issues that the use, nonuse, or misuse of CB-DCST generate. Guidelines and policies must be informed and formulated by realistic appraisal and addressing of each and all these issues consistent with core precepts of other international deliberations upon using various S&T implements in deterrent military and intelligence operations. Such consideration would need to evaluate those ways that S&T should or should not be studied, developed, and employed. Key questions include whether the use of certain CB-DCST approaches incurs greater or lesser risks and harms than other methods of deterrent operations and if—and what—limits should be applied to any possible development and use of such S&T in current and near-term deterrence initiatives [45].

CONCLUSIONS

The development and employment of CB-DCST in agendas of influence and deterrence are a certainty on the 21st century global stage. Undoubtedly, such S&T can influence the norms and conduct of multinational interactions, competition, and conflict. The future

engagement space will depend not only upon achieving S&T dominance but of establishing national and international resources necessary to exercise intelligence surveillance, oversight, and engagement of discourse and dialectic toward establishing international policy and law.

Currently, the development and use of such S&T are somewhat underregulated and not included in dual-use export safeguards, thus making effective oversight of potential dual-use research of concern difficult. This combination of "blank slate" and "unknown terrain" dimensions creates additional difficulties in realistic biosecurity forecasting and preparedness. It is important to acknowledge that the rapidity of advances in these fields often outpaces securitization. Thus, efforts to more accurately define, detect, and direct deterrent capabilities of CB-DCST can and should be rightly viewed as a clear and present exigency. ■

REFERENCES

[1] Obama, B. "The Memory of the Morning of August 6, 1945, Must Never Fade." *NY Times*, CLVX: no. 57246; p. 82016, 8 March 1996.

[2] Stockholm International Peace Research Institute (SIPRI). "The Problem of Chemical and Biological Warfare." *Vol. 1*: *The Rise of CB-Warfare*, Stockholm: Almqvist and Wiksell, 1971.

[3] Stockholm International Peace Research Institute (SIPRI). "The Problem of Chemical and Biological Warfare." *Vol. 3*: *CBW and the Law of War*, Stockholm: Almqvist and Wiksell, 1971.

[4] Gerstein, D., and J. Giordano. "Re-Thinking the Biological and Toxin Weapons Convention?" *Health Security*, vol. 15, no. 6, pp. 1–4, 2017.

[5] DeFranco, J. P., M. Rhemann, and J. Giordano. "The Emerging Neurobioeconomy: Implications for National Security." *Health Security*, vol. 18, no. 4, pp. 66–80, 2020.

[6] Snow, J. J., and J. Giordano. "Aerosolized Nanobots: Parsing Fact From Fiction for Health Security – A Dialectical View." *Health Security*, vol. 17, no. 1, pp. 74–76, 2019.

[7] Snow, J. J., and J. Giordano. "Public Safety and National Security Implications of the Horsepox Study." *Health Security*, vol. 16, no. 2, pp. 1–3, 2018.

[8] Dando, M. R. "Neuroscience and the Problem of Dual Use." *Cham. CH*: Springer, 2020.

[9] Dando, M. R., M. Crowley, M. R. Dando, and L. Shang (editors). *Preventing Chemical Weapons*: *Arms Control and Disarmament as the Sciences Converge*. London: Royal Society of Chemistry, 2018.

[10] Dando, M. R. *Neuroscience and the Future of Chemical-Biological Weapons*. Basingstoke: Palgrave-Macmillan, 2015.

[11] Dando, M. R. "Biologists Caught Napping While Their Work Militarized." *Nature*, vol. 460, p. 933, 2009.

[12] Dando, M. R. "The Impact of Modern Biology and Medicine on the Evolution of Offensive Biological Warfare Programs in the Twentieth Century." *Defense Analysis*, vol. 15, no. 1, pp. 43–62, 1999.

[13] DiEuliis, D., and J. Giordano. "Why Gene Editors Like CRISPR/CAS May Be a Game-Changer for Neuroweapons." *Health Security*, vol. 15, no. 3, pp. 296–302, 2017.

[14] Chen, C., J. Andriola, and J. Giordano. "Biotechnology, Commercial Veiling, and Implications for Strategic Latency: The Exemplar of Neuroscience and Neurotechnology Research and Development in China." In *Strategic Latency*: *Red, White, and Blue*: *Managing the National and International Security Consequences of Disruptive Technology*, Livermore CA: Lawrence Livermore Press, pp. 12–32, edited by Z. S. Davis and M. Nacht, 2018.

[15] Giordano, J. "The Neuroweapons Threat." *Bull. Atomic Sci.*, vol. 72, no. 3, pp. 1–4, 2016.

[16] Giordano, J. "Battlescape Brain: Engaging Neuroscience in Defense Operations." *HDIAC Currents*, vol. 3, no. 4, pp. 13–16, 2017.

[17] De Franco, J. P., and J. Giordano. "Mapping the Past, Present, and Future of Brain Research to Navigate the Directions, Dangers, and Discourses of Dual-Use." *EC Neurol.*, vol. 12, no. 1, pp. 1–6, 2020.

[18] Etzkowitz, H. *The Triple Helix*: *University-Industry-Government Innovation in Action*. NY: Routledge, 2008.

[19] Wurzman, R. "Inter-Disciplinarity and Constructs for STEM Education: At the Edge of the Rabbit Hole." *Synesis*: *Journal of Science Technology Ethics and Policy*, vol. 1, pp. 32–35, 2010.

[20] Venkatram, V., D. DiEuliis, and J. Giordano. "The COVID Crisis: Implications and Lessons for United States'—and Global—Biosecurity." In *COVID-19*: *Analysing the Threat*, New Delhi: Pentagon Press, pp. 397–405, edited by A. Lele and K. Roy, 2020.

[21] DiEuliis, D., N. B. Kohls, and J. Giordano. "Of Nemesis and Narcissus: Lessons COVID May Provide for Enterprises—and Ethics—of Global Health Promotions and Biosecurity." In *Medicine and Ethics in Times of Corona*, Zürich: LIT Verlag, pp. 323–329, edited by M. Woesler and H. M. Sass, 2020.

[22] DiEuliis, D., and J. Giordano. "COVID-19: Lessons to Be Learned for Biosecurity and Future Operational Environments." *J. Def. Res. Engineer.*, vol. 8, no. 3, 2020.

[23] DiEuliis, D., and J. Giordano. "The Need for Modernization of Biosecurity in the Post-COVID World." *mSphere*, vol. 12, pp. 8–14, 2022.

[24] DiEuliis, D., and J. Giordano. "Regarding and Reducing Risks of the Biotechnology Revolution." *NCT J.*, vol. 6, pp. 2–6, June 2022.

[25] DiEuliis, D, and J. Giordano. "Neurotechnological Convergence and 'Big Data:' A Force-Multiplier Toward Advancing Neuroscience." In *Ethical Reasoning in Big Data*, pp. 71–80, April 2016.

[26] Collmann, J. *Ethical Reasoning in Big Data*: An Exploratory Analysis. NY: Springer, edited by S. A. Matei, 2016.

[27] Giordano, J. "Integrative Convergence in Neuroscience: Trajectories, Problems and the Need for a Progressive Neurobioethics." In *Technological Innovation in Sensing and Detecting Chemical, Biological, Radiological, Nuclear Threats and Ecological Terrorism*, (NATO Science for Peace and Security Series), NY: Springer, edited by A. Vaseashta, E. Braman, and P. Sussman, 2012.

[28] Shook, J. R., T. Solymosi, and J. Giordano. "Ethical Constraints and Contexts of Artificial Intelligence in Biomedical Applications for Public Health and Safety, National Security, and Defense Operations." In *Artificial Intelligence and Global Security*. *Future Trends, Threats and Considerations*, London: Emerald, pp. 137–152, edited by Y. Masakowski, 2020.

[29] DiEuliis, D., and J. Giordano. "Precision Medicine and National Security: Implications, Issues and Imperatives." *Mil. Med.*, vol. 17, no. 12, pp. 35–39, 2021.

[30] National Research Council of the National Academy of Sciences (NAS). *Emerging Cognitive Neuroscience and Related Technologies*. Washington D.C.: National Academies Press, 2008.

[31] National Academies of Sciences, Engineering, and Medicine (NASSEM). *Biodefense in the Age of Synthetic Biology*. Washington, D.C.: National Academies Press, 2018.

[32] Giordano, J. (editor). "Topics in the Neurobiology of Aggression: Implications for Deterrence." U.S. DoD; Strategic Multilayer Assessment Group – Joint Staff/J-3, 2013.

[33] Giordano, J. "Intersections of "Big Data," Neuroscience and National Security: Technical Issues and Derivative Concerns." In *A New Information Paradigm? From Genes to "Big Data," and Instagrams to Persistent Surveillance: Implications for National Security*, pp. 46–48, U.S. DoD, Strategic Multilayer Assessment Group – Joint Staff/J-3/Pentagon Strategic Studies Group, edited by H. Cabayan et al., 2014.

[34] Giordano, J. (editor). "Leveraging Neuroscience and Neurotechnological (NeuroS/T) Development With Focus on Influence and Deterrence in a Networked World." U.S. DoD, Strategic Multilayer Assessment Group – Joint Staff/J-3, 2014.

[35] Giordano, J., J. P. DeFranco, and L. R. Bremseth. "Radical Leveling and Emerging Technologies as Tools of non-Kinetic Disruption." U.S. DoD, Strategic Multilayer Assessment Group – Joint Staff/J-3/ Pentagon Strategic Studies Group, 2021.

[36] Giordano, J., and R. Wurzman. "Neurotechnology as Weapons in National Intelligence and Defense." *Synesis J. Sci. Technol. Ethics Policy*, vol. 2, pp. 138–151, 2011.

[37] Bremseth, L. R., and J. Giordano. "What COVID-19 and China's Grand Strategy May Teach About a History of the Future." In *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order*, Livermore CA: Lawrence Livermore Press, pp. 109–120, edited by Z. S. Davis, F. Gac, C. Rager, P. Reiner, and J. Snow, 2021.

[38] Tennison, M., J. Giordano, and J. Moreno. "Security Threat Versus Aggregated Truths: Ethical Issues in the Use of Neuroscience and Neurotechnology for National Security." In *Neuroethics: Anticipating the Future*, Oxford: Oxford University Press, pp. 531–553, edited by J. Illes and S. Hossein, 2017.

[39] Giordano, J., C. Forsythe, and J. Olds. "Neuroscience, Neurotechnology and National Security: The Need for Preparedness and an Ethics of Responsible Action." *AJOB-Neurosci.*, vol. 1, no. 2, pp. 1–3, 2010.

[40] DeFranco, J. P., D. DiEuliis, L. R. Bremseth, J. J. Snow, and J. Giordano. "Emerging Technologies for Disruptive Effects in Non-Kinetic Engagements." *HDIAC Currents*, vol. 6, no. 2, pp. 49–54, 2019.

[41] Tractenberg, R. E., K. T. FitzGerald, and J. Giordano. "Engaging Neuroethical Issues Generated by the Use of Neurotechnology in National Security and Defense: Toward Process, Methods, and Paradigm." In *Neurotechnology and National Security and Defense: Practical Considerations, Neuroethical Concerns*. Boca Raton: CRC Press, pp. 259–278, edited by J. Giordano, 2015.

[42] Giordano, J. "Neurotechnology, Global Relations, and National Security: Shifting Contexts and Neuroethical Demands." In *Neurotechnology and National Security and Defense: Practical Considerations, Neuroethical Concerns*. Boca Raton: CRC Press, pp. 1–10, edited by J. Giordano, 2015.

[43] Casebeer, W. D. "A Neuroscience and National Security Normative Framework for the Twenty-First Century." In *Neurotechnology and National Security and Defense: Practical Considerations, Neuroethical Concerns*, Boca Raton: CRC Press, edited by J. Giordano, pp. 279–284, 2015.

[44] Johnson, J. T. *Morality and Contemporary Warfare*. New Haven: Yale University Press, 1999.

[45] Bower, R., and J. Giordano. "Use of Neuroscience and Neurotechnology in Interrogations: Practical Considerations and Neuroethical Concepts." *AJOB Neurosci. Suppl.*, vol. 3, p. 3, 2012.

BIOGRAPHY

JAMES GIORDANO is a Pellegrino Center professor of neurology and biochemistry, chief of the Neuroethics Studies Program, and director of the Program in Biosciences, Biosecurity and Ethics of the Cyber SMART Center at Georgetown University Medical Center; senior bioethicist of the Defense Medical Ethics Center; and Stockdale distinguished fellow of science, technology, and ethics at the U.S. Naval Academy. He currently serves as a nonresident senior fellow of the Simon Center for the Professional Military Ethic, U.S. Military Academy at West Point, NY. Dr. Giordano holds a BSc in physiological psychology from St. Peter's College; an M.S. in neuropsychology from Norwich University; an MPhil in philosophy of science and Ph.D. in biopsychology, both from the City University of New York; and has completed post-doctoral fellowship training in neurotoxicology and pathology at the Johns Hopkins University Schools of Medicine and Public Health.

PROTECTION OF CRITICAL INFRASTRUCTURE

in Support of the Deployment of U.S. Forces During Multidomain Operations

BY MARK O'BRIEN (PHOTO SOURCE: GETMILITARYPHOTOS [CANVA])

INTRODUCTION

The United States is facing an unprecedented set of challenges to our national interests. In the coming years, threat nations will have weaponized all instruments of national power (economic, diplomatic, informational, and military) to undermine the ability of the United States, its allies, and partners to project power to protect their vital interests during all phases of the conflict continuum (competition, crisis, armed conflict, and return to competition), as shown in Figure 1.

Threat capabilities will lead to an unstructured international environment where the lines between conflict and peace are blurred. Threat nations will leverage technological advances that have enabled the integration of space, cyber, information, and electronic warfare (EW) capabilities to shape the conflict continuum environment to attempt to thwart American power projection capabilities during transition from competition to armed conflict.

There is an urgent need for transformational change in how the United States exercises its national power capabilities and counters those of threat nations to meet these emerging challenges, particularly how they support the military instrument of national power during transition to armed conflict. The protection of critical infrastructure (CI) is now and will become even more important to ensure projection of military power capabilities.

> ***Threat capabilities will lead to an unstructured international environment where the lines between conflict and peace are blurred.***

CI

Protection of CI is an essential function of the Department of Homeland Security. CI includes

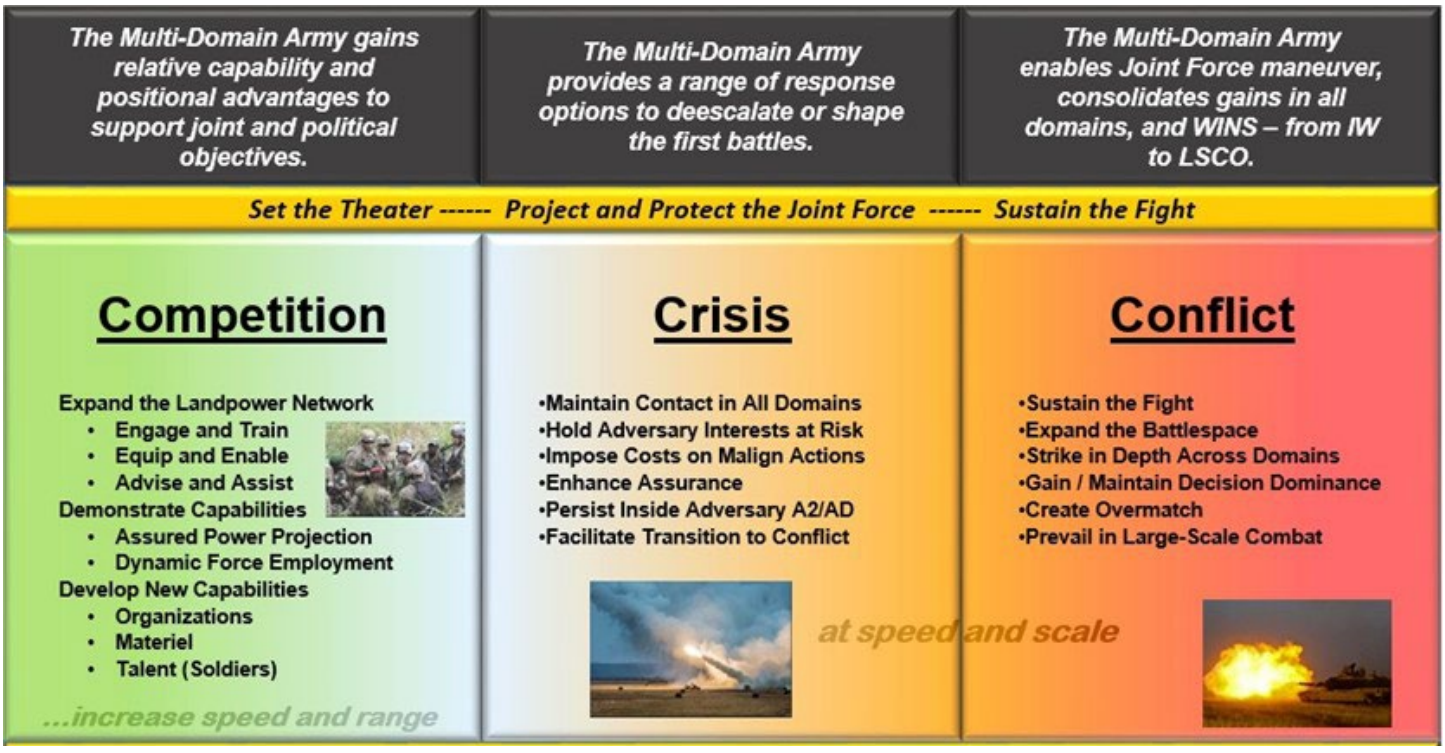


Figure 1. Conflict Continuum *(Source: U.S. Army Training and Doctrine Command [TRADOC] [1])*.

"assets, systems, and networks, whether physical or virtual, that are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" [2]. The Cybersecurity and Infrastructure Security Agency (CISA) indicates that there are 16 CI sectors, identified as the following [2]:

1. Agriculture and Food
2. Chemical and Hazardous Materials Industry
3. Defense Industrial Base
4. Government Facilities
5. Nuclear Reactors, Materials, and Waste
6. Communications
7. Financial
8. Critical Manufacturing
9. Emergency Services
10. Information Technology
11. Transportation
12. Commercial Facilities
13. Dams
14. Energy
15. Healthcare and Public Health
16. Water and Water Treatment Systems

Protection of CI has become increasingly relevant for the U.S. Department of Defense (DoD) in its ability to project power across the competition continuum, including competition, crisis, conflict, and return to competition, as the homeland is no longer viewed as a sanctuary [3].

MULTIDOMAIN OPERATIONS (MDOs)

Historically, the United States has engaged in military conflict outside the continental United States. In the past, the advantage of geography has provided a sanctuary from which the country has had the ability to project power from with little opposition. Because of emerging threat capabilities, the U.S. military can no longer view the continental United States as a sanctuary because the likelihood of a threat nation, as well as nonstate actors, disrupting and/or delaying our power projection capabilities through direct and asymmetric means is becoming more assured. Power projection, as defined by different versions of Joint Publication (JP) 3-35, is "the ability of a nation to apply all or some of its elements of national power - political, economic, informational, or military - to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability" [4].

In the Joint Operating Environment 2035: "The Joint Force in a Contested and Disordered World," dated 14 July 2016, it states, "For the foreseeable future, U.S. national interests will face challenges from both persistent disorder and states contesting international norms…" [5]. As the Joint Force responds to adversaries contesting international norms in either competition or armed conflict, it will conduct operations in an emerging operational environment shaped by the following four interrelated characteristics:

1. Adversaries are contesting all domains, the electromagnetic spectrum (EMS), and the information environment. U.S. dominance is not assured.
2. Smaller armies fight on an expanded battlefield that is increasingly lethal and hyperactive.
3. Nation states have more difficulty in imposing their will within a politically, culturally, technologically, and strategically complex environment.
4. Near-peer states more readily compete below armed conflict, making deterrence more challenging.

Protection of CI has become increasingly relevant for the U.S. Department of Defense (DoD) in its ability to project power across the competition continuum.

These characteristics allow adversaries, particularly near-peer threats like China and Russia, to expand the battlefield in time (a blurred distinction between peace and war), in domains (space and cyberspace), and in geography (now extended into the homeland) to create tactical, operational, and strategic standoff.

The MDO concept, depicted in Figure 2, considers operations in seven domains (space, cyber, air, land, maritime, information, and EMS) across seven MDO framework spaces (Strategic Support Area [SSA], Operational Support Area, Tactical Support Area, Close Area, Deep Maneuver Area, Operational Deep Fires Area, and Strategic Deep Fires Area). The homeland is part of the SSA. Each of the spaces contributes to the ability of military forces to successfully complete operations.

SUPPORT AREAS

Collectively, these areas represent that space in which the Joint Force seeks to retain maximum freedom of action, speed, and agility and counter the enemy's multidomain efforts to attack friendly forces, infrastructure, and populations. The nature of these threats varies with the adversary; although with current technology, virtually all adversaries will have reached into the homeland (e.g., through cyberspace, information warfare [IW], agents, sympathizers, and space), even if only by using social media to undermine public support and encourage "lone-wolf attacks." The reach of regional powers is also growing, and the most potent adversaries already possess multiple advanced cyberspace, space, and physical capabilities (air, naval, special operations, and/or missile forces) that can always contest the friendly rear areas. Though enemy capabilities will vary with the situation, a common requirement will be the need to ensure

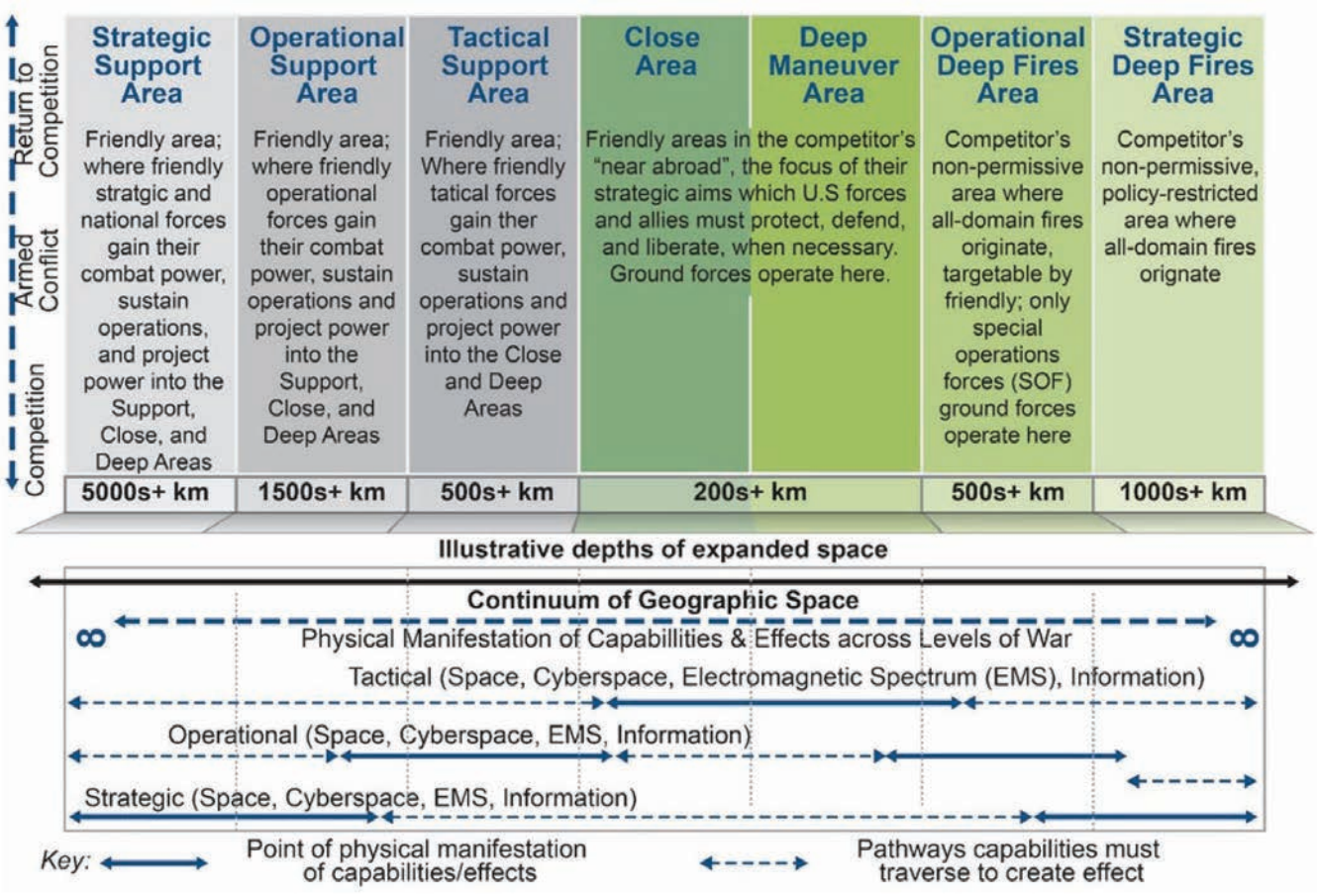


Figure 2. MDOs Areas and Domains *(Source: TRADOC [6])*.

that responsibilities, resources, and authorities are properly aligned among echelons, functions, and political organizations.

Support areas are divided according to friendly and enemy capabilities typically operating in each area.

The SSA

This is the area of cross-combatant command coordination, strategic sea and air lines of communications, and the homeland. Most friendly nuclear, space, and cyberspace capabilities and important network infrastructure are controlled and located here. Joint logistics and sustainment functions required to support MDO campaigning throughout competition and armed conflict emanate from the SSA. The enemy will attack the SSA to disrupt and degrade deployments and reinforcements attempting to gain access to the Operational Support Area and move to the Close Area, taking advantage of the reach of strategic lethal and nonlethal weapons, as well as special operations reconnaissance and strikes. Enemy engagements in this area will drive a rapid tempo of friendly operations in other areas to seek decision and limit enemy options for escalation.

The Operational Support Area

This is the area where many key Joint Force mission command, sustainment, and fire/strike capabilities are located; these can be land or sea based. This area normally encompasses many entire nations, thus making it an important space for friendly political-military integration. Due to the political and military importance here, the enemy targets this area with substantial reconnaissance, IW, and operational fires capabilities.

The Tactical Support Area

This area directly enables operations in the Close, Deep Maneuver, and Deep Fires Areas. Many friendly sustainment, fires, maneuver support, and mission command capabilities are here. The enemy directs IW, unconventional warfare, tactical fires, maneuver forces, and even operational fires at friendly forces, populations, and civil authorities.

Operational and Strategic Deep Fires Areas

These areas are defined as those beyond the feasible range of movement for conventional forces but where Joint fires, Special Operations Forces, information, and virtual capabilities can be employed.

Deep Maneuver Area

This is the highly contested area where conventional maneuver (ground or maritime) is possible but requires significant support from multidomain capabilities; commanders must make a concerted effort to "break into" this area. Because more friendly capabilities possess the range and survivability to influence or operate within this space than in the Deep Fires Area and commanders can take advantage of fire and movement, there are many more options for Joint Force employment here than in the Deep Fires Area.

Close Area

This area is where friendly and enemy formations, forces, and systems are in imminent physical contact and will contest for control of physical space in support of campaign objectives. This area includes land, maritime littorals, and airspace.

PROTECTION OF CI

Direct adversarial action against homeland infrastructures, assets, and personnel in the SSA poses the greatest risk to power projection capabilities. The TRADOC assessment of the future operational environment identifies eight homeland sectors particularly vulnerable to such disruption [1]:

1. Agriculture and food supply – Those areas affecting acquisition, processing, and availability of foodstuff.
2. Finance, banking, and commerce – Disruption of financial networks,

availability of funds, confidence in markets, and access to retail.

3. Rule of law/government institutions – Degrade confidence in the government's ability to provide functioning, stable, and legitimate law and order, services, and governance.
4. Transportation – Prolonged interruption of air, cargo, and public sectors.
5. Medical – Loss of services, corruption of supply chain, and inability to react to pandemics.
6. Water – Contamination of public supply, disruption of distribution, and loss of access to water.
7. Power – Disruption to the electromagnetic spectrum over wide areas and interdiction of power generation.
8. Entertainment and information – Attacks against arenas and public gathering places, prolonged internet denial, and loss of confidence in journalism.

By targeting CI in the homeland, adversaries will attempt to delay U.S. forces' capacity to respond to events, tying up critical military homeland assets with Defense Support of Civil Authorities (DSCA) responsibilities and eroding the nation's support for military operations. In addition, adversaries may also time their CI attacks to take advantage of an ongoing natural disaster or DSCA activity in the homeland to amplify their effects.

CI supporting deployment activities critical to power projection capabilities and installation/command deployment plans that would likely be targeted for disruption include the following eight sectors:

1. Power
2. Ports
3. Rail
4. Road networks
5. Airports
6. Fuel
7. Water
8. Communication networks

Attacks on the homeland and installation/command deployment plans, which rely heavily on these eight CI sectors, are likely to come from multidomain formations that seek to disrupt power projection capabilities from the other side of the globe. Where possible, adversaries will use multidomain effects to encourage or compel attacks by irregular or asymmetric domestic groups (e.g., narco-terrorists). Adversaries are likely to conduct multiple attacks simultaneously across all domains. Threat courses of action (COAs) will also include the application of new and emerging technologies, especially innovative artificial intelligence/machine-learning (AI/ML) tools.

Threat action categories considered most likely to target CI include the following:

- Cyber-based Effects – Attacks on the homeland will target industrial control systems and supervisory control and data acquisition architectures to degrade or disable systems that control power and water utilities, industrial processes, transportation infrastructures, and other critical networks (e.g., communications). Attacks will also use traditional denial of service and ransomware cyber-based tools.
- IW – Adversaries will deploy online spam, disinformation, and media manipulation tactics to influence public perception and citizen actions, including via social media (e.g., Facebook and Twitter). IW efforts will also seek to translate online sentiments into real-world protests or other hostile demonstrations.
- Unmanned aerial systems (UASs) – Attacks on the homeland will exploit the proliferation of low-cost and expendable UASs (including drone

Where possible, adversaries will use multidomain effects to encourage or compel attacks by irregular or asymmetric domestic groups.

swarms and other autonomous, robotic systems) to deliver payloads to degrade or destroy physical targets; conduct intelligence, surveillance, and reconnaissance missions; disseminate powders or other chemical/biological payloads above populations; and directly disrupt airport operations.

- Sabotage – Adversaries will combine information warfare, cyber-based effects, and other means to encourage or compel irregular forces—including suicide bombers, lone-wolf actors, narco-terrorists, and preplaced special forces—to sabotage assets central to the nation's defense-critical infrastructure (e.g., major highways, utility stations, rail depots, and internet nodes).
- Unconventional attacks – Adversary COAs may use chemical, biological, radiological, nuclear in a manner outside the confines of traditional warfare, namely the targeting of noncombatant populations. Adversaries may also employ electromagnetic pulse weapons, seek to disable the Global Positioning System and conduct widespread jamming of the cellular system and other networks, and exploit as-of-yet unknown vulnerabilities in Smart City/Internet of Things technologies.

The nature of these threats varies with the adversary; although with current technology, virtually all adversaries could reach into the homeland (e.g., through cyberspace, IW, saboteurs, sympathizers, and space), even if only by using social media to undermine public support and encourage "lone-wolf attacks." The reach of regional powers is also growing, and the most potent adversaries already possess multiple advanced cyberspace, space, and physical capabilities (air, naval, special operations, and/or missile forces) that can always contest the friendly rear areas. Figure 3 provides a visual representation of an attack on the homeland during military deployment.

For instance, Russia and its proxies have excelled in using cyberattacks to gather intelligence on U.S. military and commercial assets and spread misinformation, while the Chinese People's Liberation Army has reoriented much of its force to focus on space, cyberspace, and EW operations. Many of these capabilities can originate from anywhere on the globe and project directly into the homeland, threatening to erode Army freedom of action.

MILITARY INSTALLATION RELIANCE ON CI

DoD Directive (DoDD) 3020.40, *Mission Assurance* [7], and DoD Instruction (DoDI) 3020.45, *Mission Assurance Construct* [8], provide risk-based assessment processes to identify, assess, manage, and monitor the risks to strategic missions. These processes identify defense critical infrastructure

Russia and its proxies have excelled in using cyberattacks to gather intelligence on U.S. military and commercial assets and spread misinformation.

vulnerabilities in federal, state, and allied/partner nations assets and infrastructure. Areas of consideration are threats and vulnerabilities, including terrorism; cyberthreats; chemical, biological, radiological, nuclear, and high-yield explosives; emergency management; extreme weather events such as hurricanes; and loss of utilities. Installation mission assurance must consider CI impacts of unconventional, sequential, or multiple threats such as civil unrest, UASs (to include drone swarms), robotic autonomous systems, IW, cyber, or threats to externally provided support like public utilities or commercial services. Installation protection plans must consider the threats posed by cascading system failures that an adversary is likely to effect via multidomain attack, including disabling a critical system via degradation of a supporting network (e.g., disruption of water purification systems due to debilitation of a base microgrid power controller). It is likely that an incomplete situational awareness of installation vulnerabilities

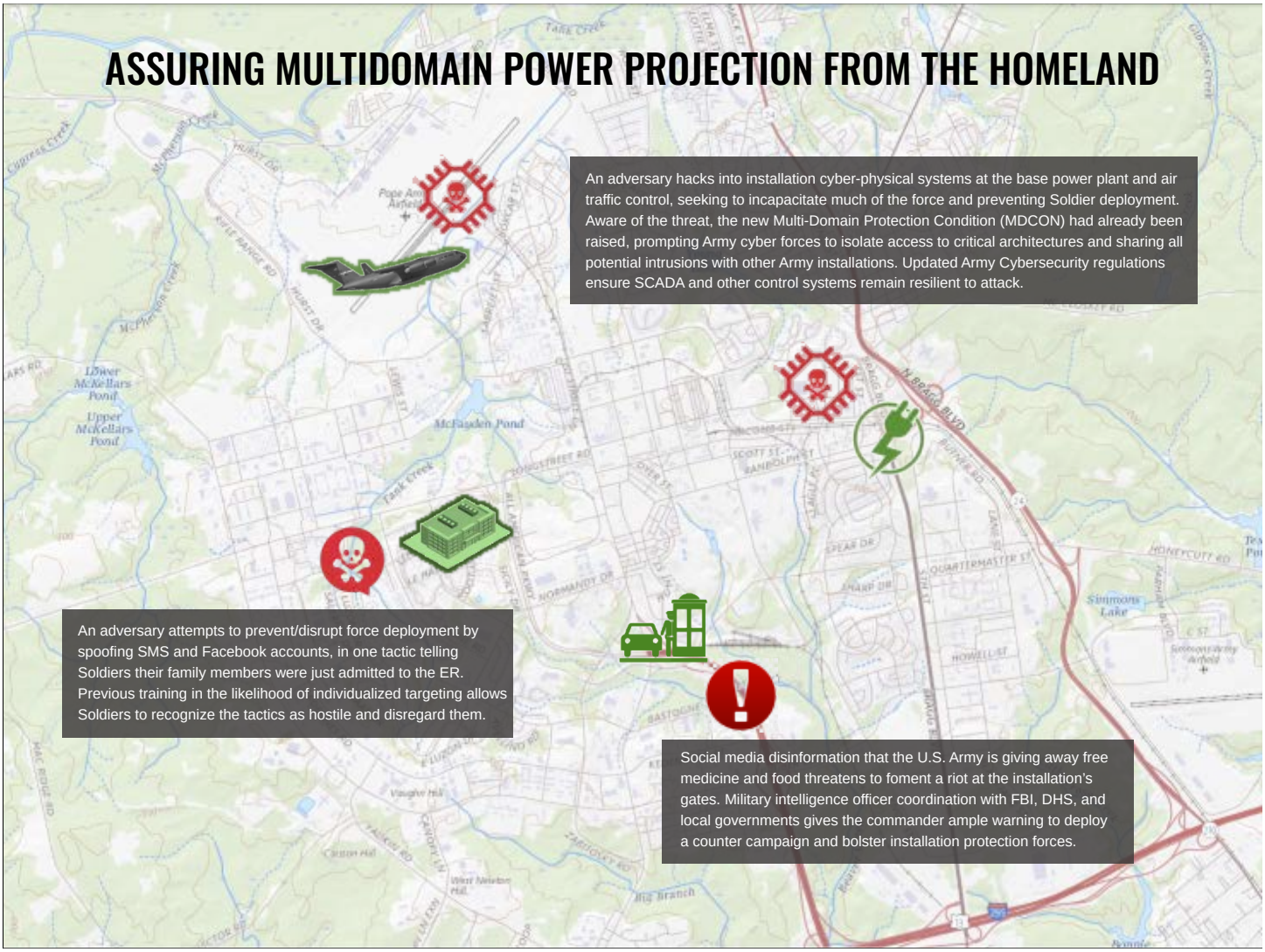


Figure 3. Example Threat Attack on Deployment *(Source: J. Hewett)*.

will result in the misallocation of protective measures required in the threat environment.

Commercial companies, suppliers, and distributors play a key role in the homeland by providing electrical, water, telecommunications, trucking, food services, and other critical infrastructure and business services essential to installation and force sustainment and support. Threat nations and nonstate actors operating on their behalf will have sophisticated and diverse capabilities designed to prevent the United States from projecting military power from the homeland. Many of these capabilities can originate from anywhere on the globe and project directly into the homeland, threatening to erode our freedom of action. Threat nations and their proxies have excelled in using cyberattacks to gather intelligence on key CI and military assets and spread misinformation. There are several recent examples reported by multiple news organizations where attacks, accidents, and weather impacted the functioning of infrastructure assets, such as the cyber/ransomware attacks on 7 May 2021 to Colonial Pipeline, an American oil pipeline system, which shut down and delayed fuel distribution for several weeks, and another cyberattack on 30 May 2021, which impacted the world's largest meat processor, JBS Foods, who had to close its nine beef plants

> ***Threat nations and their proxies have excelled in using cyberattacks to gather intelligence on key CI and military assets and spread misinformation.***

in the United States. The February 2021 winter storm in Texas caused a massive electricity generation failure, leading to shortages of food, water, and heat. Even more recent events, such as the notorious Chinese spy balloon and the train derailment in East Palestine, OH, demonstrate aspects of CI vulnerabilities.

COUNTERING THREATS TO MILITARILY SIGNIFICANT CI

Countering the ability of threat nations and nonstate actors' abilities to successfully employ direct and asymmetric attacks to disrupt and delay the deployment of forces from U.S. installations will require rethinking and synchronizing homeland and defense coordination, planning, and action.

Key CI-related considerations to counter contested deployment of forces from installations include the following:

- Enhance the sustainability and resilience of military installations against enemy action and natural disasters. CI that contributes to this capability would include agriculture and food supply, rule of law/government institutions, transportation, medical, water, and power.
- Increase coordination with partners, particularly in the U.S. domestic private and public sectors, to increase capacity and develop redundancy to protect critical homeland commercial and governmental sectors against disruption.
- Ensure that intelligence generation, collection, and analysis are sufficient to provide installations with all-domain coverage of potential threat courses of action, likelihood of targeting, and risk mitigation of expected outcomes.
- Focus policies and guidance for installation protection on multidomain threats and the risks to cyber-physical systems.
- Develop comprehensive and coordinated analytical methodologies to assess vulnerabilities in homeland installations that are central to deployment.
- Advance the use of AI technologies to enhance commander command, control, and convergence of protection effects. As an emerging capability, AI can provide the ability to generate, ingest, process, format, and analyze large volumes of sustainment and protection data produced at a high velocity/variety, contributing extensively to command-and-control efforts.
- Develop capabilities to detect, target, deny, and conduct post-incident intelligence collection on adversary small UASs or other drone types.
- Establish civil-military relations guidance that is robust for directing how military forces should consult and coordinate with local governments and organizations to defend homeland CI before and during contested conditions.

CONCLUSIONS

It is no longer business as usual when it comes to power projection during times of competition, crisis, and transition to armed conflict.

The ability of our nation to deploy forces from the homeland in a time of conflict—supported by political, diplomatic, economic, and informational means—in and across all domains, the electromagnetic spectrum, and the information environment to prevail in competition and armed conflict and then return to competition is an existential requirement.

Protection of CI will facilitate our forces to retain maximum freedom of action, speed, and agility to counter the

threat's multidomain efforts to attack friendly forces, infrastructure, and populations, resulting in a timelier end to crises and return to competition. ■

REFERENCES

[1] TRADOC. *The Operational Environment and the Changing Character of Warfare*. PAM 525-92, October 2019.

[2] CISA. U.S. Department of Homeland Security. "Critical Infrastructure Sectors." https://www.cisa.gov/critical-infrastructure-sectors, accessed 19 March 2024.

[3] U.S. DoD. "National Defense Strategy," 2018.

[4] Joint Chiefs of Staff. *Deployment and Redeployment Operations*. Joint Publication (JP) 3-35, 10 January 2018.

[5] Joint Chiefs of Staff. "The Joint Force in a Contested and Disordered World." *Joint Operating Environment 2035*, 14 July 2016.

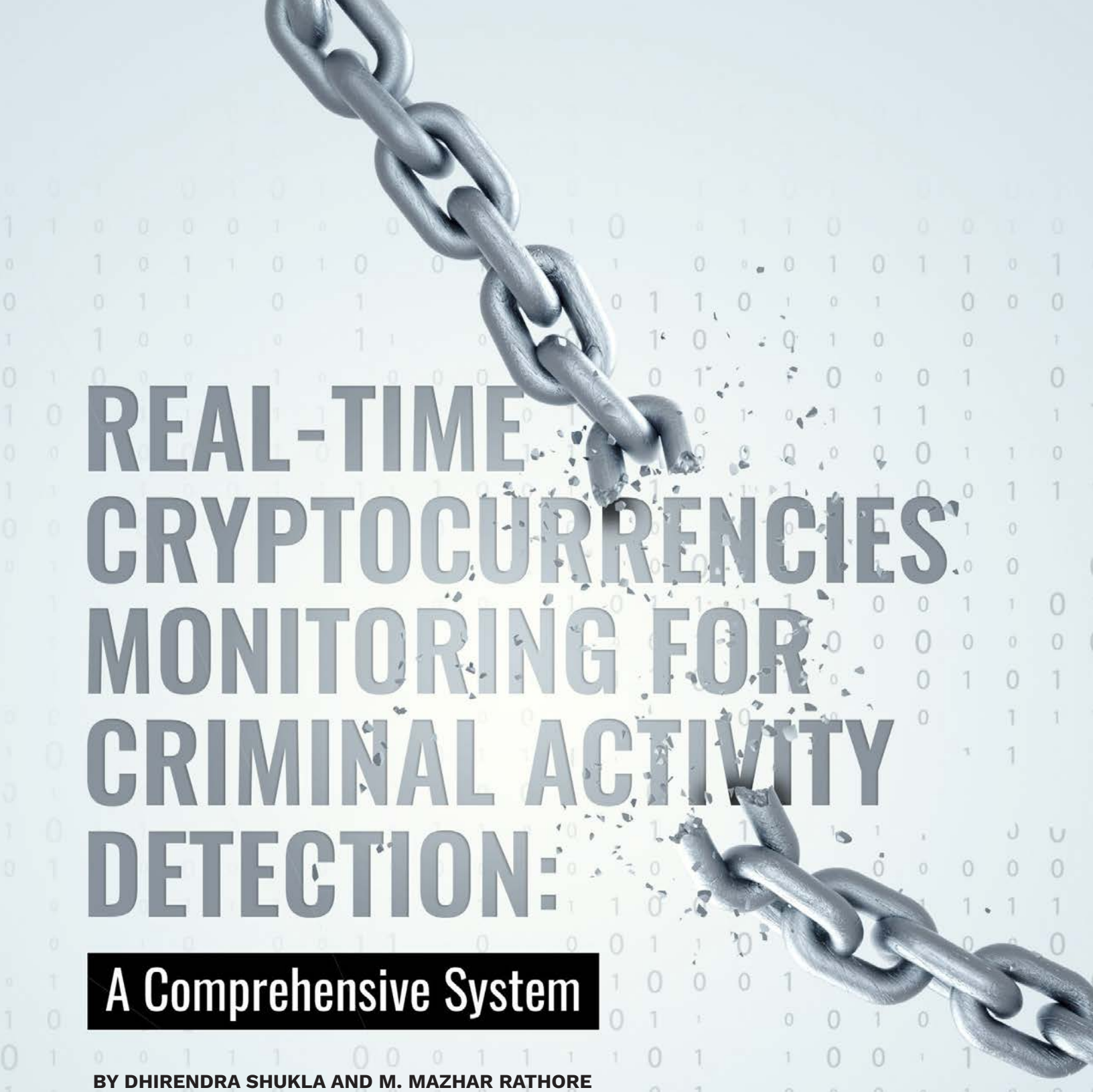
[6] TRADOC. *The U.S. Army in Multi-Domain Operations* 2028. TRADOC Pamphlet 525-3-1, 6 December 2018.

[7] U.S. DoD. *Mission Assurance*. DoDD 3020.40, 29 November 2016.

[8] U.S. DoD. *Mission Assurance Construct*. DoDI 3020.45, 14 August 2018.

BIOGRAPHY

MARK O'BRIEN is a senior survivability analyst at the SURVICE Engineering Company, where he recently led a team of researchers on behalf of the Homeland Defense & Security Information Analysis Center to complete a capabilities-based assessment for the U.S. Army Maneuver Support Center of Excellence concerning the homeland in MDOs. He is a retired U.S. Army Field Artillery and Army Acquisition Corps Officer. Mr. O'Brien is a graduate of the Command and General Staff College, Fort Leavenworth, KS, and holds a bachelor's degree in economics from Eastern Connecticut State University and a master's degree in information systems management from Oklahoma City University.



REAL-TIME CRYPTOCURRENCIES MONITORING FOR CRIMINAL ACTIVITY DETECTION:

A Comprehensive System

BY DHIRENDRA SHUKLA AND M. MAZHAR RATHORE

(PHOTO SOURCE: MIKKYR [123RF.COM])

SUMMARY

Cryptocurrencies like Bitcoin and Ethereum are gaining popularity due to their decentralized nature and lack of central control. These digital currencies provide a high degree of user anonymity, making it difficult for attackers to identify the actual individuals behind addresses and trace funds transferred between users. However, these features of blockchain-based cryptocurrencies also pose challenges, as they can facilitate criminal activities and fraudulent transactions. Detecting such illicit actions or entities within cryptocurrencies proves to be a significant challenge for security agencies and financial authorities. As a response to this challenge, a comprehensive system for identifying fraudulent entities in cryptocurrency systems has been developed. This system comprises two primary modules: (1) off-chain monitoring and (2) on-chain monitoring. Off-chain monitoring involves artificial-intelligence (AI)-based real-time surveillance of the World Wide Web (WWW), dark web searches, and social media analytics to detect fraudulent entities. Subsequently, it issues alerts to prevent individuals from engaging in transactions with such entities. Through off-chain analysis, a significant set of fraudulent cryptocurrency addresses is extracted, which aids in on-chain monitoring. Contrary to off-chain analysis, which identifies fraudulent addresses before any cryptocurrency fraud occurs, the on-chain monitoring module detects fraudulent entities after the fraud has taken place in the blockchain. Using on-chain analysis, machine-learning (ML)-based models have been developed for detecting fraudulent addresses in Bitcoin and Ethereum. Additionally, a function to identify mixer and tumbler services has been created, facilitating the identification of money-laundering activities involving cryptocurrencies. These results demonstrate promising outcomes in terms of both correctness and real-time capability.

INTRODUCTION

Fraud has been a persistent issue in society since human creation; the only difference lies in the evolving methods of committing fraud. With the advancement of technology, fraudulent activities have become more modernized and sophisticated, making them increasingly challenging to identify. In recent decades, identifying fraud has garnered significant attention and discussion. Banks have made substantial financial investments to detect fraudulent transactions occurring within their networks. In the traditional fiat currency system, banks and government authorities manage and supervise fund movements. They have implemented a new generation of security measures to address these risks [1]. Since the fiat currency system is regulated and controlled, involves recognized customers, and is monitored, it is not easy for criminals to engage in financial fraud.

> ***With the advancement of technology, fraudulent activities have become more modernized and sophisticated, making them increasingly challenging to identify.***

Contrary to fiat currency, committing fraud using cryptocurrency is comparatively easier due to features provided by cryptocurrency systems, such as user anonymity and decentralization. All cryptocurrencies (e.g., Bitcoin and Ethereum) employ decentralized blockchain technology to execute transactions and record them in a public ledger. While everyone has access to the ledger, no one has control over it. User identities are anonymized and represented as a long random number called a public key or address. A user can generate multiple addresses to receive and transfer cryptocurrency coins. These features make cryptocurrencies a strong alternative to the fiat currency system, resulting in an increasing number of cryptocurrency users each day. However, they also contribute to a rise

in the overall fraud ratio. Although everyone has access to all transactions and authorities can trace them, the challenge lies in detecting fraud and uncovering the actual identity behind it due to the anonymity provided. Typically, fraudulent users generate a new address each time to receive and transmit coins, aiming for increased privacy and avoiding being identified.

Cryptocurrencies not only facilitate fraud but also various other criminal activities like money laundering, terrorism financing, drug trafficking, child trafficking, bribery, and ransom. According to a report by Chainalysis [2], illicit addresses received over $24 billion in 2023, constituting 0.42% of overall transactions. The report highlighted a significant increase in ransomware and dark net crimes. Additionally, Elliptic reported that illicit entities laundered $2.7 billion worth of coins in 2022 using cross-chain methods, with North Korea's hacking organization alone responsible for over $900 million [3]. The inherent features of cryptocurrencies, such as anonymity, the changing nature of user addresses, and the lack of central control, make it challenging to identify and track criminals and their transactions within the cryptocurrency system.

Government authorities, agencies, and various companies are actively engaged in detecting cryptocurrency fraud and criminal activities and identifying real entities associated with them through on-chain analysis. However, these agencies conduct manual analyses and transaction tracing with the assistance of human experts to ascertain the legitimacy of a given transaction or entity, aiming to identify the actual individuals or organizations behind illicit activities. Some of these organizations utilize computer algorithms for analysis and detection, although their monitoring processes are not always in real time. Additionally, contemporary criminals employ sophisticated third-party services, such as mixers and tumblers, to enhance privacy and obscure the traceability of their fund transfers. For instance, money launderers leverage mixers and tumblers that offer protection by mixing coins through multiple transactions involving several users. This mixing mechanism significantly complicates the task for authorities attempting to trace funds within the cryptocurrency system and identify their source.

Cryptocurrencies not only facilitate fraud but also various other criminal activities like money laundering, terrorism financing, drug trafficking, child trafficking, bribery, and ransom.

Furthermore, the majority of cryptocurrency monitoring bureaus overlook off-chain monitoring. Most frauds are perpetrated by scammers who encourage individuals to invest in cryptocurrency and purchase counterfeit products or services. To achieve this, scammers create deceptive websites or advertise on social media, providing cryptocurrency addresses to receive coins. The early detection of these off-chain platforms, advertisements, and crypto-addresses can help prevent fraud. While some monitoring organizations engage in manual detection, the process is slow and cannot keep up with the rapid creation of such deceptive content.

To address these challenges, an AI-based comprehensive system has been designed to identify scams, fraudulent entities, and services supporting money laundering, such as mixers. This system comprises two major modules: (1) off-chain monitoring and (2) on-chain monitoring. The objective of the off-chain module is to prevent cryptocurrency fraud before it occurs, while the on-chain module detects an illicit entity after the crime is committed. The off-chain module involves real-time monitoring of the WWW to identify cryptocurrency phishing websites and extract associated cryptocurrency wallet addresses. It also establishes connections between the extracted wallet addresses and the dark web, tracing them on social media platforms. Upon identifying

any suspicious website, social media content, or crypto-address, the system issues an alert to deter individuals from engaging in transactions with such entities. Through off-chain analysis, a significant set of fraudulent cryptocurrency addresses can be extracted, which aids on-chain monitoring.

On the other hand, the on-chain monitoring conducts real-time surveillance of cryptocurrency blockchains to detect fraud and money-laundering activities. To achieve this, ML-based models for detecting fraudulent addresses in Ethereum and Bitcoin have been developed. Additionally, a function to identify mixer and tumbler services has been created, facilitating the identification of money-laundering activities involving cryptocurrencies. The on-chain module also enables users to assess the risk level associated with a given address, providing insights into the potential risk of trading with that address. Furthermore, clustering on addresses has been performed to group all addresses associated with a single entity. Finally, the system's correctness and its ability to operate in a real-time environment has been evaluated. Results demonstrate promising outcomes in terms of both correctness and real-time efficiency.

The remainder of this article is organized as follows. The next section titled Preliminaries provides an understanding of basic concepts, including the workings of Bitcoin and Ethereum, the definition of mixers and tumblers, and an exploration of how fraud is committed by scammers. The Proposed System section follows, examining the technical details of the system, encompassing both on-chain and off-chain monitoring modules. The results of the system evaluation are presented in the section titled System Evaluation and Results, followed by Conclusions.

PRELIMINARIES

In this section, the preliminary concepts to understand the overall system are discussed. How Bitcoin, Ethereum, and Mixers execute their operations is then demonstrated. Furthermore, the overall scenario of fraud execution in cryptocurrency domain is reviewed.

Bitcoin

Bitcoin is a decentralized cryptocurrency system that facilitates peer-to-peer transfers of Bitcoins without involving any central party. In contrast to traditional banking systems, Bitcoin operates without central controlling or regulatory authority. Each Bitcoin user possesses a pair (or multiple pairs) of a public key and a corresponding private key, generated through secure mechanisms. The public key serves as the user's address for receiving Bitcoins, while the corresponding private key is utilized to transfer or withdraw those Bitcoins to other users by signing the transaction. The private key is kept confidential, known only to the user who employs it for withdrawing or transferring coins, particularly after receiving Bitcoins in the corresponding public key. This approach ensures user anonymity within the Bitcoin system, making it challenging to identify the real identities, such as persons or individuals, behind public keys or addresses. The combination of user anonymity and decentralized control has contributed to Bitcoin's popularity. However, these features also pose risks, as they can be exploited for criminal activities such as fraud, money laundering, child trafficking, and more.

> ***Bitcoin is a decentralized cryptocurrency system that facilitates peer-to-peer transfers of Bitcoins without involving any central party.***

Consider a simple Bitcoin transfer scenario, as shown in Figure 1, between users U_n, U_x, U_y, and U_z who have public and private key pairs (PU_n,PR_n), (PU_x,PR_x), (PU_y,PR_y), and (PU_z,PR_z), respectively. U_x has received 15 Bitcoins from U_n in two transactions, TD_{11} and TD_{111}. Now, U_x wants to transfer 15 Bitcoins to U_y and generates a transaction TD_{22}

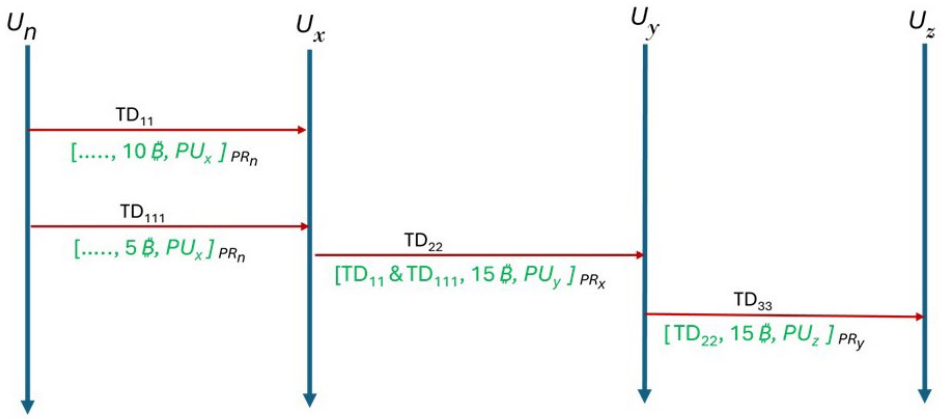


Figure 1. Bitcoin Transaction Scenario *(Source: D. Shukla and M. Rathore).*

by mentioning the receiver's address as PU_y and the input transactions' references (i.e., transactions from where those Bitcoins were received) as TD_{11} and TD_{111}. U_x signs TD_{22} using private key PR_x and broadcasts it to the Bitcoin network. When each Bitcoin miner receives TD_{22}, the signature that the TD_{11} and TD_{111} are never spent in any earlier transaction is verified and then added to a block, along with other transactions to mine it. Once any miner node successfully mines the block, the block is added to the blockchain, and the transaction is successfully committed. In the same way, U_y transfers Bitcoins to U_z in the transaction TD_{33}. In the throughout process, no one knows who is behind the PU_n, PU_x, PU_y, and PU_z addresses (i.e., U_n, U_x, U_y, and U_z are never revealed). Specific details of the mining process are not provided here; however, Al-Farsi et al. [4] explain the working of the Bitcoin system and whole mining process in a very comprehensive way.

Ethereum

Ethereum is the second-most popular cryptocurrency after Bitcoin, introduced in 2013 by Vitalik Buterin in his white paper [5]. Like Bitcoin, Ethereum operates on a decentralized network and prioritizes user anonymity. However, unlike Bitcoin, Ethereum employs proof-of-stake (PoS) [6] for block mining, transaction validation, and security, as opposed to proof-of-work (PoW). Notably, Ethereum recently transitioned from PoW to PoS for its mining protocol. Unlike PoW, PoS is quite efficient, as it does not keep all nodes busy in the mining process. PoS randomly selects a single node in the network to validate all the transactions in a block and add them to the Ethereum network. Moreover, Ethereum's transfer message only supports one sender and one receiver address in a single transaction. In contrast, a Bitcoin transaction can involve multiple senders and receivers in a single transaction.

Mixers and Tumblers

Mixers, also known as tumblers, are cryptocurrency services provided by third parties to enhance the privacy of transactions for cryptocurrency users. The Bitcoin blockchain, being public, allows anyone to view all transactions, enabling tracking of fund sources. Through sophisticated transaction analysis, monitoring, and tracking, the real person behind an address can be identified. To make it more challenging to trace funds to a specific address, mixers combine coins from various sources by repeatedly sending and receiving funds using multiple addresses in a single transaction. They obfuscate coins by receiving them from a user; gathering and mixing them using multiple source and destination addresses in one or more transactions, as illustrated in Figure 2; and then sending them to the user-provided address. This method makes it difficult for attackers to backtrack the funds received in a transaction by an address. From the perspective of cryptocurrency users, mixers offer privacy. However, it is essential to note that mixing can be exploited by criminals for money laundering and concealing their sources. Consequently, many national security authorities aim to identify transactions involving mixing services.

Fraud Scenarios

Most cryptocurrency frauds are perpetrated by scammers who

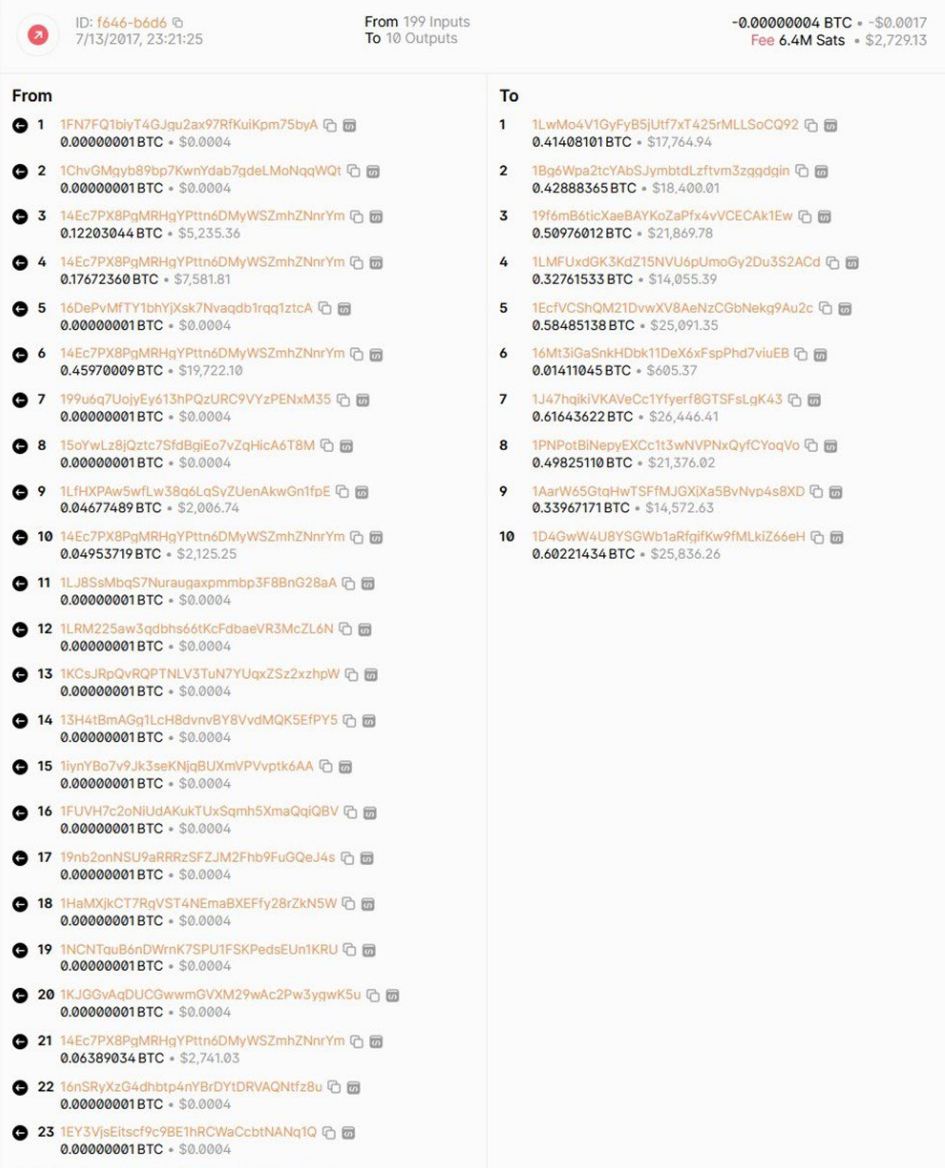


Figure 2. Bitcoin Transaction Involving a Mixer *(Source: D. Shukla and M. Rathore).*

employ various tactics to deceive users. These individuals convince users to send them Bitcoins in exchange for promised services, products, or financial gains. However, once the coins are received, no such offerings are provided. The anonymity feature inherent in Bitcoin makes it challenging to trace and apprehend these fraudulent actors. Most scams occur through phishing attacks, wherein scammers create deceptive websites (referred to as phishing websites), send fraudulent emails, utilize social media and other platforms for misleading advertisements, and encourage individuals to invest in their platform or acquire services/products by transferring Bitcoins to a provided Bitcoin address. Early detection of such phishing attacks can aid in identifying potential sources of fraud, allowing for proactive measures to be taken to prevent cryptocurrency-related scams.

PROPOSED SYSTEM

To monitor fraudulent activities in cryptocurrencies and prevent them through an early-detection mechanism, a comprehensive system that performs both real-time, off-chain monitoring and on-chain monitoring has been developed. Figure 3 illustrates the overall layered architecture of the system. At the current stage, the focus is on monitoring two major cryptocurrencies, including Bitcoin and Ethereum. Off-chain monitoring primarily focuses on early fraud detection by identifying cryptocurrency-related scamming/phishing websites and monitoring social media and the dark web. On the other hand, real time, on-chain monitoring is designed to identify fraudulent transactions as they occur in the cryptocurrency blockchain. This system identifies mixers to help control money laundering, detects fraudulent transactions, and clusters addresses to group those belonging to the same entity. Additionally, risk analysis is performed on addresses to assign a risk level, indicating whether an address belongs to a legitimate user or a scammer. Intercomponent analysis between each of the off-chain and on-chain submodules has been conducted. Both NoSQL database

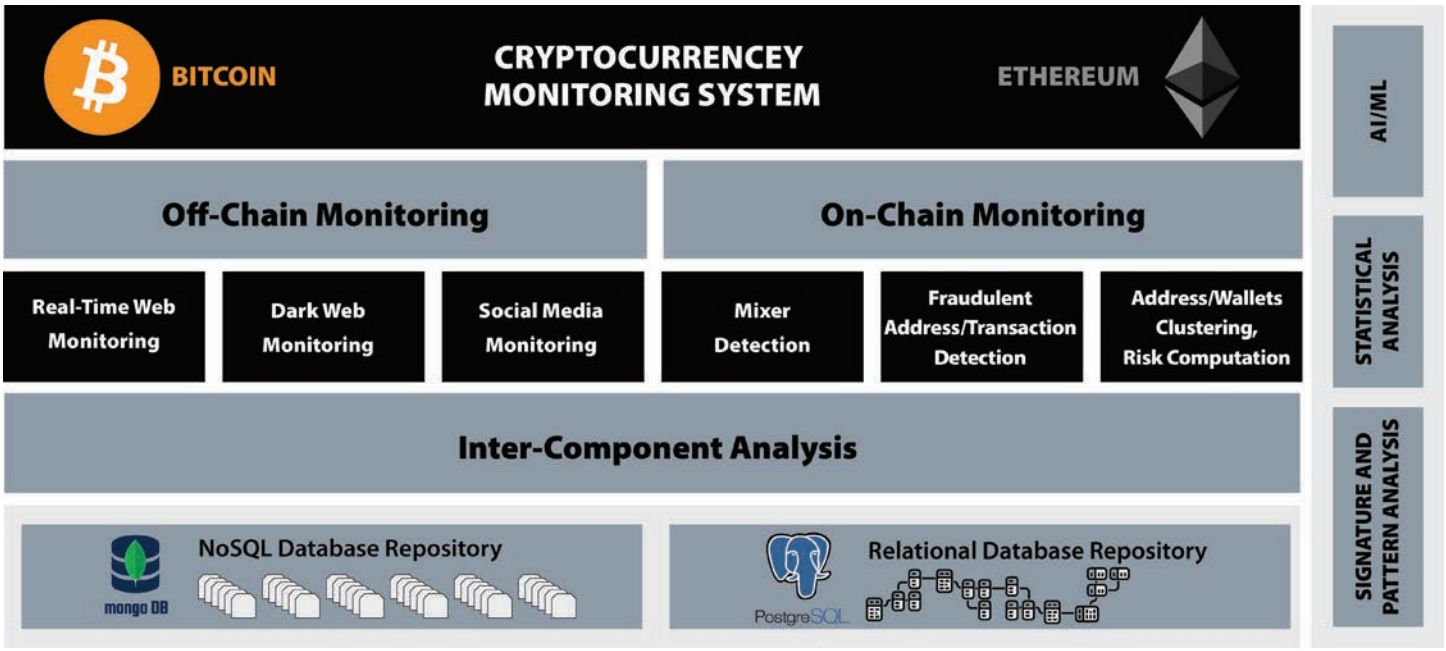


Figure 3. System Architecture *(Source: D. Shukla and M. Rathore).*

management systems (DBMS), such as MongoDB, and relational DBMS, such as PostgreSQL, are utilized to store data, features, intermediate findings, and results. For data analysis at both on-chain and off-chain levels, signature-based pattern detection algorithms, statistical methods, and ML are employed. This section delves into the technical details of each individual module of off-chain and on-chain monitoring.

Data Collection, Preprocessing, and Features Engineering

The detection models are data driven, requiring an extensive amount of data for initial analysis and model development. These data were collected from various public sources and Telegram groups. Some of the datasets were built in-house. Data on cryptocurrency scamming websites for off-chain analysis were sourced from industry experts who conducted manual analyses to identify cryptocurrency scams. Initially, a dataset comprising 500 deceptive websites and 200 nondeceptive websites (resembling scams but not fraudulent) was compiled. Using this dataset as a foundation, AI-based clustering techniques were employed to expand a list of deceptive websites to 10,000. For on-chain analysis, the data generated by Toyoda et al. [7] containing addresses of 3,199 mixers and 23,114 nonmixers (26,313 total) were obtained. The labels were primarily assigned through heuristics and clustering techniques. Nonmixer samples include addresses from services that may resemble mixers, such as exchanges, faucets, high-yield investment program, pools, markets, and gambling platforms. For fraudulent transaction analysis, a list of 12,146 fraudulent and legitimate Ethereum addresses was obtained from *Kaggle* [8].

After removing 246 duplicated entries, 5,054 fraudulent addresses and 6,846 nonfraudulent addresses were left. Additionally, a set of fraudulent addresses from off-chain sources was gathered and included Telegram chats, scamming websites, the dark web, and social media.

Usually, the data are not refined; they may contain null or missing values, unnormalized values, repeated data, and unbalanced samples. Consequently, data preprocessing was conducted to refine the data and prepare it for analysis. Both the

Bitcoin mixers dataset and Ethereum dataset were imbalanced, indicating an unequal distribution of samples across categories. Therefore, when training an AI-based model for mixer detection, only 3,601 random nonmixer addresses from the mixer dataset were selected to achieve a somewhat balanced dataset.

In contrast, for the Fraudulent dataset, the SMOTE [9] resampling mechanism was employed to equalize the number of both fraudulent and nonfraudulent addresses to 6,846 each. Additionally, zero-variance attributes, abnormal outside samples, and outliers were eliminated from all datasets using box-plot analysis. To address missing and null values, the data were partitioned, based on class labels, and k-means clustering (with k = 10) was applied to each partition to identify subgroups. Subsequently, the mean value of all attributes in each subgroup was calculated, and the missing values were replaced with the mean value of the corresponding attribute. Furthermore, to prevent poor performance due to nonstandardized attribute values, Gaussian normalization was applied, ensuring zero mean and unit variance. Values were transformed using the Yeo-Johnson power transformer method [10] with in-place computation [11].

On-chain datasets comprise many parameters. Mixer and nonmixer addresses are characterized by 36 features, while Ethereum addresses have 32 parameters (excluding "address" and the "class" parameter). Utilizing all these parameters for on-chain, real-time monitoring may result in significant overhead. Therefore, to reduce the number of parameters in the Ethereum dataset, correlation and feature importance scores were employed. Certain attribute pairs with strong interlinear relationships, such as ratioRecSent and receivedTransactions, maxValReceived and avgValReceived, and ratioSentTotal and ratioRecTotal, were identified. One attribute from each pair was removed by choosing the one with a stronger correlation to the class attribute. Subsequently, the Gini index [12] (a method for determining feature importance) was applied to the remaining 29 attributes to select the top 16 attributes. The feature importance scores for these attributes are depicted in Figure 4.

To eliminate unimportant features from the Bitcoin mixer dataset, basic signature and pattern, statistical, correlation, and information gain analysis was conducted [13]. The information gain of an attribute A represents the amount of information gained about a class variable from the observing attribute A. In simple terms, it is the measure used in a decision tree to identify the best parameter.

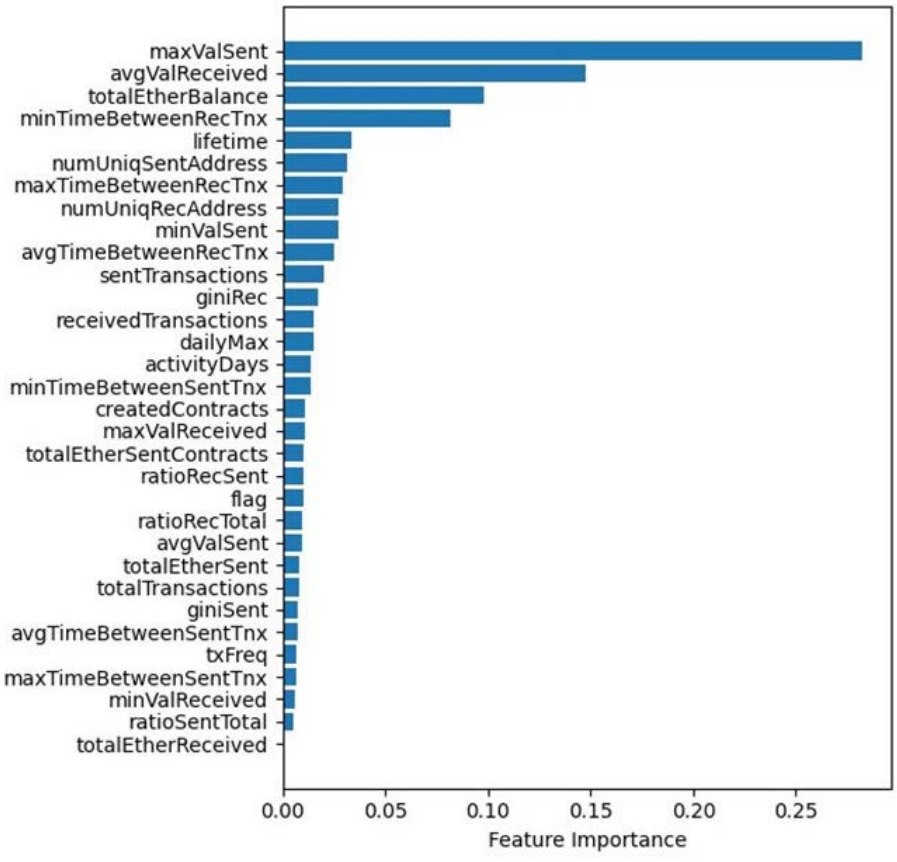


Figure 4. Gini Feature Importance Scores for the Ethereum Fraud Dataset *(Source: D. Shukla and M. Rathore)*.

Through information gain analysis, each feature was categorized as either important or nonimportant. The top eight most important features that can effectively distinguish mixer and nonmixer addresses were then selected. Table 1 shows the selected features and their corresponding information gain values. Later, patterns and flow analysis of Bitcoin transactions was performed by constructing a big graph using Neo4j [14]. Specifically, the focus was on transactions containing a mixer's address in the sender list (inputs) or receiving list (outputs).

Findings revealed that most of the mixer's transactions exhibited "fan-in," "fan out," or "scatter-gathered patterns." In a fan-in pattern, the transaction involves multiple senders and one receiver, while the fan-out pattern features one sender and many receivers. In a scatter gathered (or gathered-scatter) scenario, there are too many relationships between the number of inputs and outputs of the transaction. Graphs depicting the analysis of transactions involving the mixer address "1PzuVHgrSH7rRJNttzgknuomMLohX54dCB" are illustrated in Figures 5 and 6. Figure 5 shows all the Bitcoin exchanges (represented by blue nodes) by the mixer (represented by the orange node). Each blue node contains the information about transactions where Bitcoins were received and subsequently sent to other addresses. To further analyze inputs and outputs, a blue node can be expanded, as demonstrated in Figure 6.

Table 1. Parameters Selected by Information Gain for Mixers Detection

INFORMATION GAIN	SELECTED PARAMETER	DETAILS
0.73	*frequency per day*	Number of transactions/day
0.431	*mean spent input*	Average Bitcoins spent per spent transaction
0.404	*ratio AllPatterns*	Ratio of fan-in, fan-out, and scatter-gathered transactions to total transactions
0.39	*ratio InPattern*	Ratio of fan-in transactions to total transactions
0.346	*ratio received* 2_0	Ratio of number of times the digit *i* in U.S. dollars appeared in received transactions, where I (10^3,10^2,...,10^6), over number of received transactions
0.303	*ratio spent*	Ratio of number of spent transactions over total transactions
0.303	*ratio received*	Ratio of number of received transactions over total transactions
0.293	*ratio spent* 2_0	Ratio of number of spent 2_0 over number of spent transactions

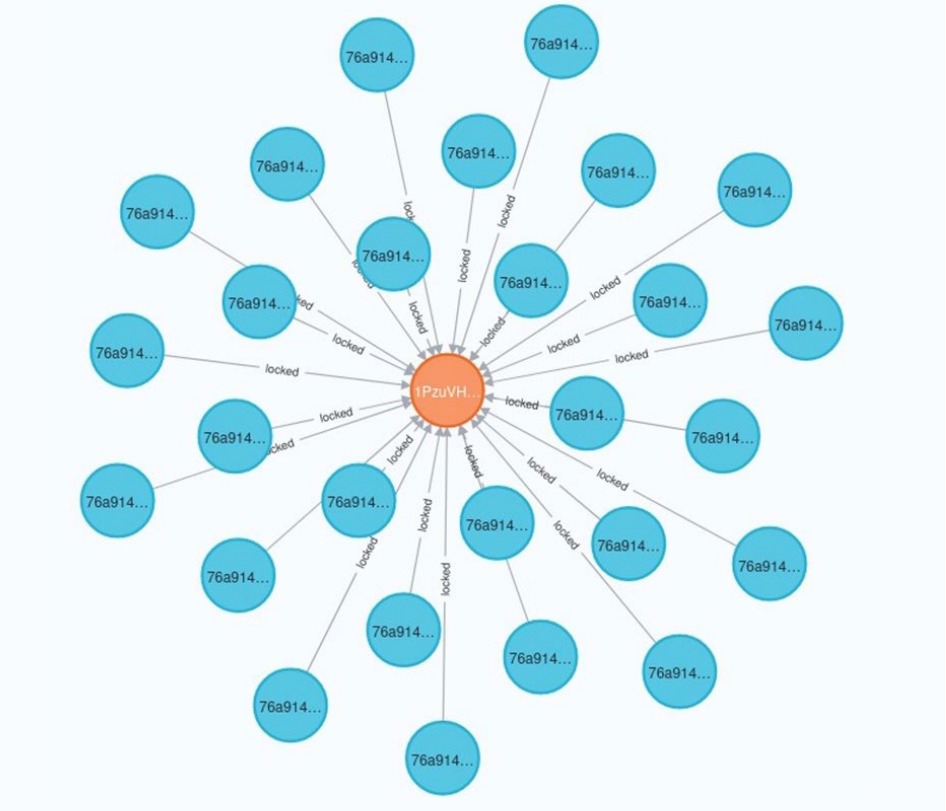


Figure 5. Transactions of the Mixer 1PzuVHgrSH7rRJNttzgknuomMLohX54dCB *(Source: D. Shukla and M. Rathore).*

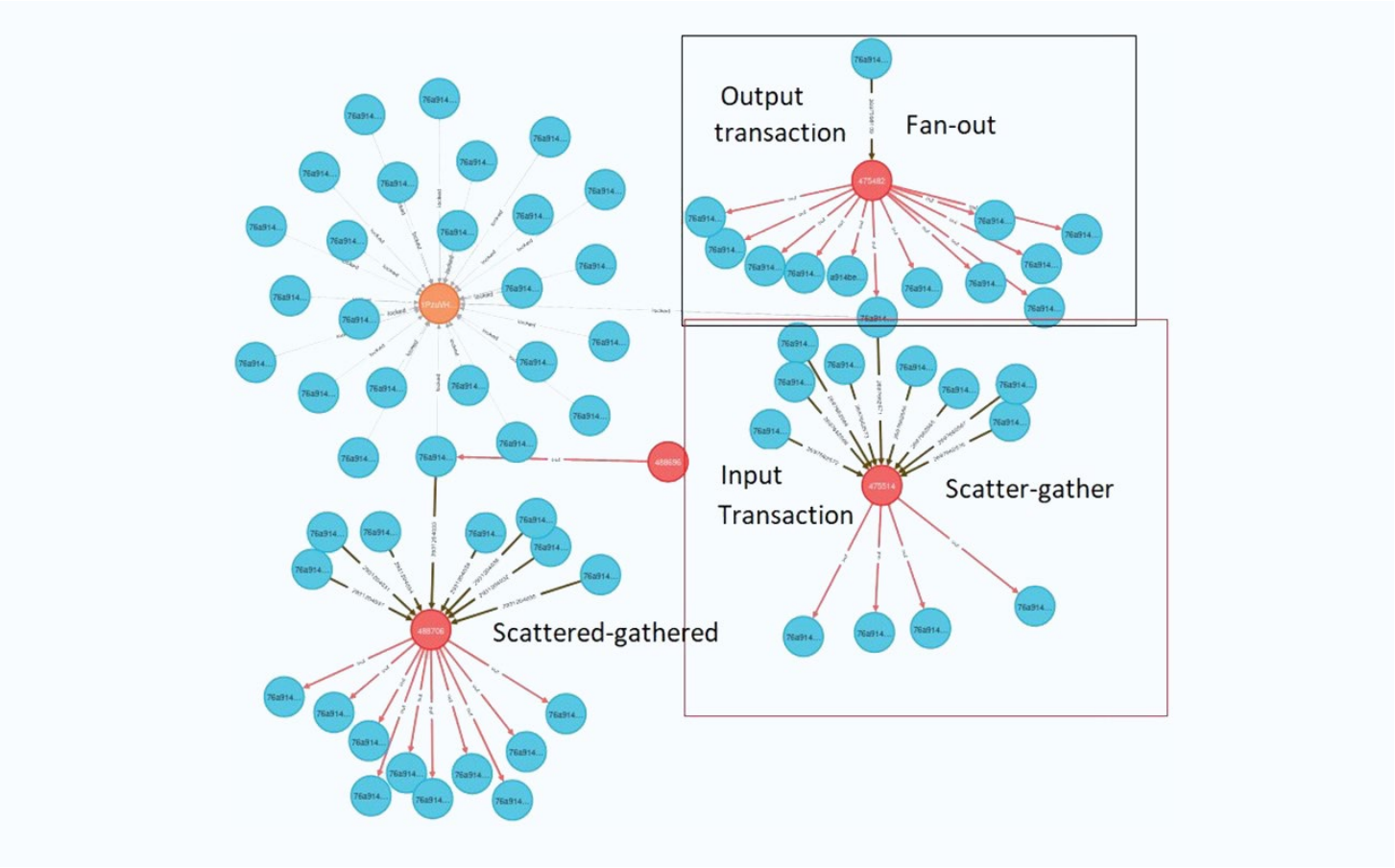


Figure 6. Fan-out and Scatter-Gathered Transactions of the Mixer 1PzuVHgrSH7rRJNttzgknuomMLohX54dCB *(Source: D. Shukla and M. Rathore)*.

Based on this transaction pattern and flow analysis, three additional features were added to the list of important features, including "number of fan-in patterns," "number of fan-out patterns," and "number of scattered-gather patterns," making a total of 11 features.

Real-Time, Off-Chain Monitoring

The motivation for real-time, off-chain monitoring is to prevent fraud before it occurs. Through the surveillance of the web, dark web, and social media, cryptocurrency wallet addresses associated with scams and fraudulent activities are identified. These efforts aim to thwart attempts to collect coins through deceptive means. The overall flow of the off-chain monitoring system is illustrated in Figure 7.

Web Monitoring

This system provides real-time monitoring of the web to detect any fake websites that attempt to persuade users to invest in cryptocurrency or purchase products/services at a lower price. Scammers often provide cryptocurrency wallet addresses for users to make payments. This system extracts newly created websites daily and assesses which ones are scams. To achieve this, the system initially filters all cryptocurrency-related websites by applying a signature- and pattern-matching algorithm to the website's content and basic features. Subsequently, complex features are extracted from the filtered websites, such as the age of the website, region, daily visitor count, and more, and the term frequency inverse document frequency vector is computed. This vector, along with the feature set, is then provided to the AI-based deceptive website detection module to determine whether the website is deceptive or nondeceptive. Also, the

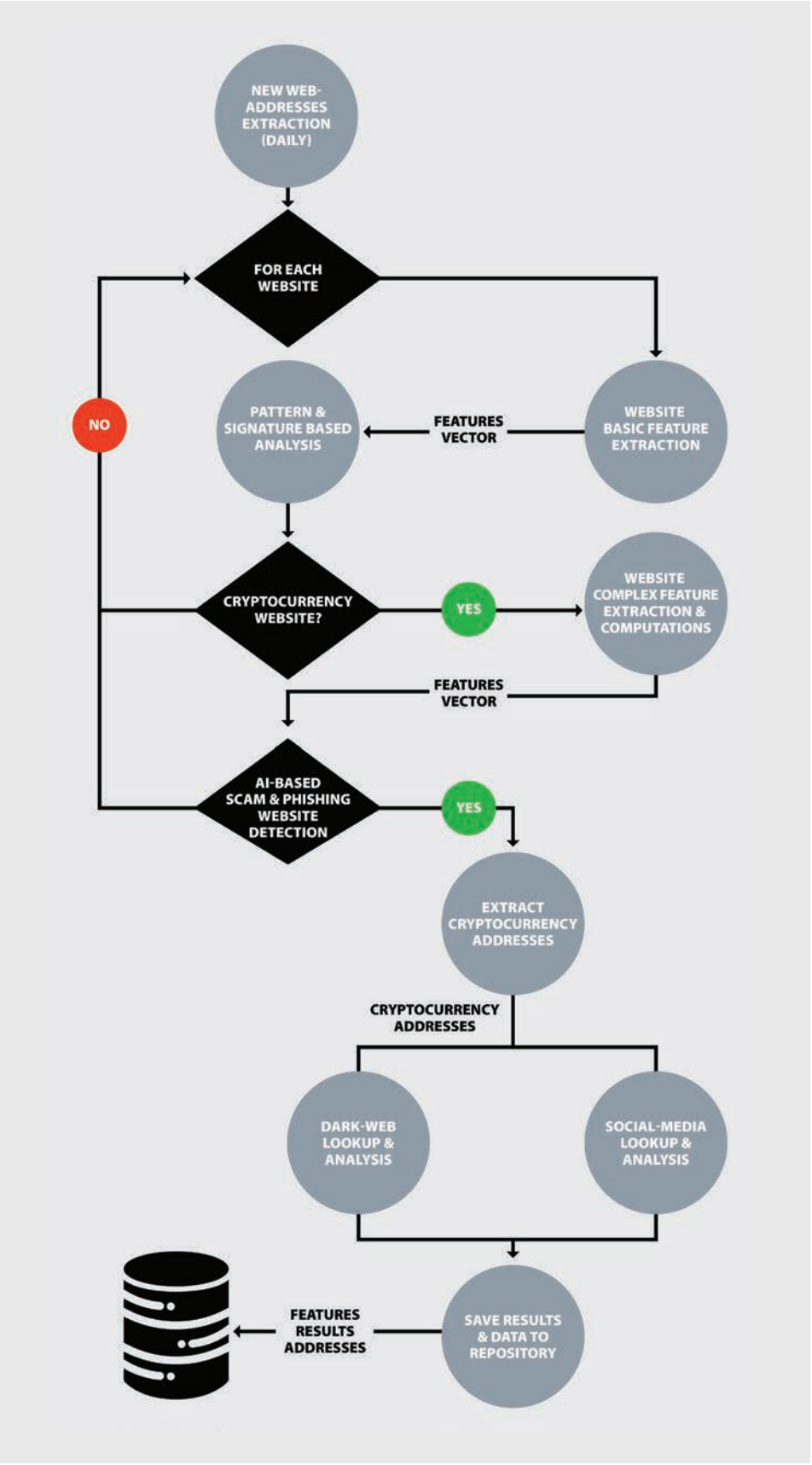


Figure 7. Flow Chart of the Off-chain Monitoring System *(Source: D. Shukla and M. Rathore).*

> ***The motivation for real-time, off-chain monitoring is to prevent fraud before it occurs.***

system thoroughly scans each website flagged as a scam to extract the Bitcoin addresses provided by the scammer. The system generates alerts whenever it identifies a scam website on the web and stores the website details, along with the corresponding extracted wallet address in a blacklist.

The deceptive website detection module employs a random forest ML model, trained and extensively tested on an in-house labeled dataset, as previously discussed in the Data Collection, Preprocessing, and Features Engineering section of this article. Occasionally, scammers may create multiple similar websites to launch an effective phishing campaign. There is also the possibility that a group of scammers works together to launch phishing attacks using a combination of scamming websites. Thus, this system identifies such groups of similar websites that are identical to a given scamming website by employing a k-means clustering approach. The system also identifies similar websites that share the same wallet address. To date, this system has scanned more than 250 million websites created since 2014 [15], at a daily rate of 250,000 per day. Overall, more than

67,000 websites have been detected as deceptive, with a daily detection rate exceeding 500 per day.

Dark Web Monitoring

This system also monitors the dark web to identify cryptocurrency addresses. It searches for traces of wallet addresses blacklisted by the scamming website detector within the dark web, thereby enhancing the confidence level of the system. SOS Intelligence Limited's application programming interface (API) [16] is employed to extract all the active dark web uniform resource locators (commonly known as URLs) daily and monitor them regularly. Whenever the system finds the cryptocurrency address on the dark web, it retrieves the contents of the corresponding dark web page for further investigation.

Social Media Monitoring

As with dark web monitoring, social media contents like X are also monitored to compile all the wallet addresses discussed on social media. To raise the confidence level for the scammers wallet address list (blacklist addresses), the system checks to see if any of these addresses are reported on social media. This module is at the initial stage of development.

Real-Time, On-Chain Monitoring

Bitcoin and Ethereum do not have a central authority to control their operations and monitor them. Therefore, a real-time monitoring system is required for these cryptocurrencies to generate alerts if a new transaction involves any suspicious entity in either the receiving side or sending side. Specifically, the aim of the real-time monitoring system is to identify fraudulent entities and mixer services.

The overall flow of the on-chain fraudulent entities and mixer detection is illustrated in Figure 8. The system is connected with the Ethereum and Bitcoin blockchain nodes, which always have the latest version of the blockchains and updates whenever a new block is created in the chain. This system processes each newly created block and prepares a list of all input and output addresses in each transaction. Each address is looked up in the database to determine whether the address exists in the record (i.e., finding whether the address had already been analyzed in the past). If the address does not exist in the database, the system extracts and computes all the address features, as previously mentioned in the Data Collection, Preprocessing, and Features

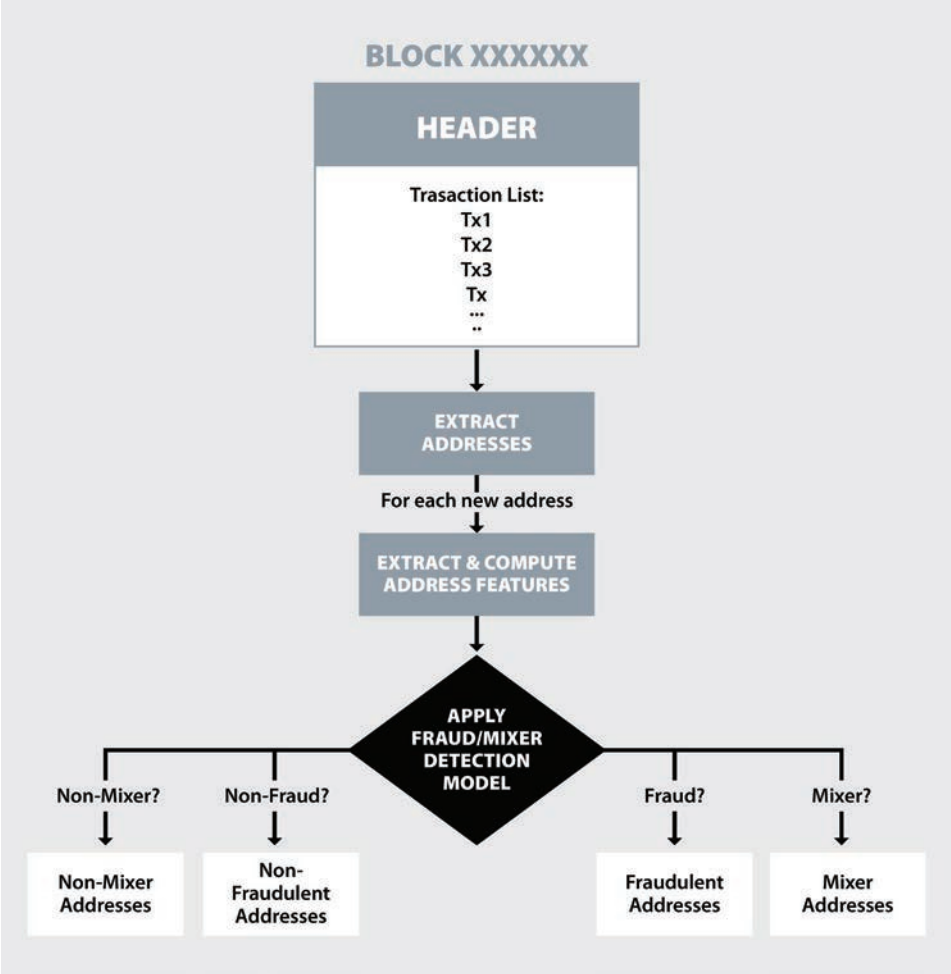


Figure 8. AI-Based Mixer and Fraud Detection *(Source: D. Shukla and M. Rathore).*

Engineering section of this article. These features are then provided to the AI-based classification models to determine whether the address is legitimate or fraudulent or if it is a mixer. The system generates alerts to users if there is a mixer or a fraudulent entity involved in any transaction. Also, by utilizing graph-based clustering and address connection analysis, the system determines the group of addresses that may belong to a single specific entity. In the same way, the system also provides risk scoring to each entity to guide the user to avoid any trade with high-risk addresses.

Mixers and Tumblers Detection

Mixers assist money launderers not only in concealing the origin of their illicit funds, which may be obtained through fraud, ransom, scams, or other unlawful activities, but also in obscuring the recipients of these funds in the form of cryptocurrency coins. Consequently, identifying mixing services is crucial for unveiling money-laundering activities within the realm of cryptocurrencies. Current approaches in the literature either lack high accuracy due to the dynamic nature of mixing methods or are insufficiently efficient for real-time monitoring. This system achieved high accuracy by building ML-based distributed gradient-boosted decision trees (GBDT) using the extreme gradient boosting (XGBoost) library [17, 18]. The mixer detection model [19] consists of multiple small decision trees that operate in parallel to perform decision-making. Furthermore, after an extensive analysis of mixers, only 11 important features were found, which are quite fewer in number. A smaller number of attribute computations and a parallel decision-making approach through multiple distributed trees ensure real-time processing capabilities.

Fraud Detection

Off-chain monitoring is employed to prevent fraud before it happens. The other way to deal with the fraudulent entities is to detect them and their transactions in the on-chain by monitoring the cryptocurrency blockchain in real time. This system performs fraudulent entity detection [20] by employing an AI-trained model.

To select the best ML model, four tree-based learners, such as classification regression trees (CART), random forest, light gradient-boosting machine (LGBM), and GBDT, were tested using XGBoost. These models were assessed using a 10-fold cross-validation on a refined version of an Ethereum dataset, which consisted of both fraudulent and nonfraudulent entities (wallet addresses) based on 16 features. The correctness results for each of these models are presented in Table 2. Ultimately, the distributed GBDT learner was chosen, as it demonstrated exceptional performance. The model was retained on the entire dataset, and validation was conducted using various hyperparameter configurations. The optimal hyperparameters were determined to be [colsample_bytree = 0.7, learning rate = 0.5, max depth = 4, n estimators = 200, and subsample = 0.9]. Eventually, the model was deployed in a real-time environment, where the GBDT-based, fraud-detection model exhibited significantly higher accuracy with these hyperparameters.

Wallets and Address Clustering

In cryptocurrencies, an address is essentially a public key. A user can have multiple addresses and generate as many pairs of public and private key as desired. Once an address

Table 2. Accuracy of Machine Learning Model on Ethereum Fraud Dataset Using k-Fold Cross-Validation

TREE-BASED LEARNERS	ACCURACY	PRECISION	RECALL
CART	0.911	0.92	0.90
Random forest	0.93	0.94	0.92
LGBM	0.94	0.96	0.93
GBDT	0.95	0.96	0.94

(i.e., a public key) receives coins in a transaction, the corresponding private key can be employed to access the received coins, either for transfer or withdrawal. This feature in cryptocurrency enables criminals to generate and utilize multiple addresses for sending and receiving coins, thus avoiding identification. Therefore, a graph-based algorithm has been developed to identify the set of addresses that may pertain to a single entity, particularly a fraudulent one. The algorithm accomplishes this grouping by tracking and tracing all the transactions associated with a given address, both upward and downward. A heuristic approach has been utilized, and rules for addresses to be part of the same group have been established. For instance, a straightforward rule is as follows: if two addresses are used as inputs in a single transaction, they belong to the same entity. Similarly, there are more complex rules utilized by the algorithm.

Address Risk Factor Computation

In addition to detecting fraudulent entities, a risk model that assigns risk scores to addresses has also been developed, providing cryptocurrency users with information about the level of risk when trading with a particular address. Once again, a graph-based approach is utilized to analyze addresses, focusing on the transaction network of each address and its interactions with known fraudulent or high risk addresses. The risk scores are determined by the distance of an address from identified fraudulent or high-risk entities within the network.

SYSTEM EVALUATION AND RESULTS

Overall, the system comprises six modules. However, in this evaluation, the focus is on three major modules of the comprehensive system: (1) real-time web monitoring, (2) mixers detection, and (3) fraudulent entity detection. These modules are assessed in terms of correctness and efficiency.

Implementation Environment

Currently, the back-end, real-time monitoring modules operate on multiple local machines. The results, report, and alerts are generated through a cloud portal [15]. Three local machines are utilized, with two of them equipped with 16-GB random access memory (RAM) and 20 central processing unit (known as CPU) cores at 2.10-GHz speed, whereas the third one is more powerful—a Dell Precision 7920 machine with 128-GB RAM and 52 2.10-GHz Intel Xeon(R) Gold 6230R processors. All systems are running an Ubuntu 22.04.3 long-term support operating system.

For real-time, on-chain monitoring, transactions data are extracted from two platforms—Bitquery [21] and Blockchain Explorer [22]. For off-chain monitoring, the website list is obtained from the WHOIS database [23], the dark net data are extracted using SOS Intelligence APIs [16], and the social media data are collected using Twitter API [24]. The ML-based detection models are trained, tested, evaluated, and implemented in Python using the XGBoost library [25].

Correctness

The correctness of the AI-based detection models is evaluated with k-fold cross-validation, where $k = 10$. With this validation approach, the entire dataset is divided into k mutually exclusive equal portions. The model is trained and tested k times, with each trial involving training the model on one of the $k-1$ data portions and then testing it on the remaining part, in a repetitive manner. Finally, the results from all trials are aggregated.

To assess the system correctness from all perspectives, the accuracy, precision, and recall parameters were utilized—computed by equations 1, 2, and 3, respectively—along with true positives (*TP*), true negatives (*TN*), false positives (*FP*), and false negatives (*FN*). *TP* represents the number of correctly identified positive instances (frauds/mixers/scams), *TN* denotes the number of correctly identified negative instances (nonfrauds/nonmixers/nonscams), *FP* indicates the number

of incorrectly recognized positive instances, and *FN* is the number of incorrectly recognized negative instances.

$$Accuracy = (TP + TN)/(TP + TN + FP + FN). \quad (1)$$

$$Precision = (TP)/(TP + FP). \quad (2)$$

$$Recall = TP/(TP + FN). \quad (3)$$

The AI-based detection models demonstrate high accuracy. The offline monitoring module successfully identifies cryptocurrency scams and phishing websites with an accuracy exceeding 90%, whereas the on-chain modules exhibit even greater accuracy, surpassing 96% in detecting mixers and fraudulent entities across both Bitcoin and Ethereum (as detailed in Table 3). Notably, this study indicates that the reduction in feature sets (11 features for mixer detection in Bitcoin and 16 features for fraud detection in Ethereum) has no adverse impact on accuracy levels. This is corroborated by the consistent accuracy observed in both full and reduced feature sets.

Efficiency

This designed system is capable of operating in a real-time environment.

> ***The offline monitoring module successfully identifies cryptocurrency scams and phishing websites with an accuracy exceeding 90%.***

One of the local machines is dedicated to processing all the newly uploaded websites on the web each day. On average, the machine processes more than 250,000 websites daily and determines which ones are scams in just 4–6 hours.

In terms of on-chain monitoring, real-time cryptocurrency transaction data are collected from external blockchain nodes that hold the current state of the cryptocurrency blockchains. The bottleneck in the mixer and fraudulent entity detection is extracting data from these nodes, as the time depends on the current network speed, bandwidth, delay, server computation power, and other network factors at the client and server ends. In most cases, it takes fewer than 200 ms per address to retrieve basic parameters. However, at the local machine, it takes less than 1 ms to compute the selected 24 features from the basic ones. Once the features are computed, the detection time is negligible (i.e., less than 0.5 ms); it took around 20 ms to detect fraudulent entities from 2,739 instances.

With these results and having an in-house blockchain node running at the local machine, it is possible to detect mixer services and fraudulent entities, even if the cryptocurrency transactions are being generated at a very high speed.

CONCLUSIONS

This article presents a novel AI-based cryptocurrency monitoring system designed to identify scams, fraudulent entities, and mixers. The system aids in criminal investigations related to activities like money laundering, child trafficking and abuse, gambling, ransom, Ponzi schemes, and others. The system comprises two major

Table 3. Accuracy of the Mixers' Detection Model on Bitcoin Data

DETECTION TYPE	*TP*	*TN*	*FP*	*FN*	ACCURACY	PRECISION	RECALL
Mixers' detection (full dataset)	3,098	3,528	72	101	0.974	0.977	0.968
Mixers' detection (reduced dataset)	3,089	3,521	80	110	0.972	0.974	0.966
Fraudulent entities detection	1,306	1,334	48	51	0.96	0.96	0.96

modules: (1) off-chain monitoring and (2) on-chain monitoring. Off-chain monitoring involves real-time surveillance of the WWW to identify cryptocurrency phishing websites and extract associated cryptocurrency wallet addresses. Furthermore, it establishes the connection between the extracted wallet addresses and the dark web and traces them on social media.

On the other end, on-chain monitoring does the real-time surveillance of cryptocurrency blockchains to detect frauds and money-laundering activities (through detecting mixer service involvement in a transaction). This module also enables users to assess the risk level associated with a given address, providing insight into the potential risks of trading with that address. Furthermore, clustering is applied to group all addresses associated with a single entity. In summary, off-chain monitoring helps prevent cryptocurrency fraud before it occurs, while on-chain monitoring detects fraud after it has been committed within the cryptocurrency blockchain. ■

ACKNOWLEDGMENTS

The current work is supported by Atlantic Innovation Fund and Mitacs (funding no. IT24468).

NOTE

This article is exclusively written by the authors. AI-based tools like ChatGPT and Grammarly are employed solely for the purpose of detecting and correcting typos and grammar errors.

REFERENCES

[1] Lévesque, F. L., S. Chiasson, A. Somayaji, and J. Fernandez. "Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach." *ACM Transactions on Privacy and Security*, vol. 21, no. 4, 2018.

[2] Chainalysis Team. "2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, but Ransomware and Darknet Markets See Growth." https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/, accessed February 2024.

[3] Elliptic Enterprises Limited. "The State of Cross-Chain Crime 2023." https://www.elliptic.co/resources/state-of-cross-chain-crime-2023, accessed February 2024.

[4] Al-Farsi, S., M. M. Rathore, and S. Bakiras. "Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities." *Applied Sciences*, vol. 11, no. 12, p. 5585, 2021.

[5] Buterin, V. "Ethereum Whitepaper." *Ethereum*, https://ethereum. org, 2014.

[6] King, S., and S. Nadal. "PPCoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake." Self-published paper, 19 August 2012.

[7] Toyoda, K., T. Ohtsuki, and P. T. Mathiopoulos. "Multi-Class Bitcoin-Enabled Service Identification Based on Transaction History Summarization." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1153–1160, Halifax, NS, Canada, 2018.

[8] Escobero, G. "Ethereum-Fraud-Dataset." *Kaggle*, https://www.kaggle.com/datasets/gescobero/ethereum-fraud-dataset?resource=download, accessed February 2024.

[9] Camacho, L., G. Douzas, and F. Bação. "Geometric SMOTE for Regression." *Expert Systems With Applications*, vol. 193, no. 2, p. 116387, January 2022.

[10] Yeo, I.-K., and R. A. Johnson. "A New Family of Power Transformations to Improve Normality or Symmetry." *Biometrika*, vol. 87, no. 4, pp. 954–959, December 2000.

[11] Rein, S., and M. Reisslein. "Low-Memory Wavelet Transforms for Wireless Sensor Networks: A Tutorial. *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 291–307, 2011.

[12] Hasell, J. "Measuring Inequality: What Is the Gini Coefficient?" *Our World in Data*, https://ourworldindata.org/what-is-the-gini-coefficient, 30 June 2023.

[13] Azhagusundari, B., and A. S. Thanamani. "Feature Selection Based on Information Gain." *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), vol. 2, issue 2, pp. 18–21, January 2013.

[14] Neo4j, Inc. "GenAI Apps, Grounded in Your Data." https://neo4j.com/, accessed February 2024.

[15] Gray Wolf Analytics. "StaySafeCrypto: Analyze and Discover Deceptive Activities in Cryptocurrency." https://staysafecrypto.com/, accessed February 2024.

[16] SOS Intelligence Limited. "Business Risk Insight Using Cyber Threat Intelligence." https://sosintel.co.uk/, accessed February 2024.

[17] Chen, T., and C. Guestrin. "XGBoost: A Scalable Tree Boosting System." Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 785–794, August 2016.

[18] Brownlee, J. *XGBoost With Python*: *Gradient Boosted Trees With XGBoost and scikit-learn*. Machine Learning Mastery, 2016.

[19] Rathore, M. M., S. Chaurasia, and D. Shukla. "Mixers Detection in Bitcoin Network: A Step Towards Detecting Money Laundering in Crypto-Currencies." 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, pp. 5775–5782, 2022.

[20] Rathore, M. M., S. Chaurasia, D. Shukla, and P. Anand. "Detection of Fraudulent Entities in Ethereum Cryptocurrency: A Boosting-Based Machine Learning Approach." 2023 Global Communications Conference, Kuala Lumpur, Malaysia, 2023.

[21] Bitquery Inc. "Bitquery: Blockchain API and Crypto Data Products." https://bitquery.io/, accessed February 2024.

[22] Blockchain.com, Inc. "Blockchain Explorer APIs." https://www.blockchain.com/, accessed February 2024.

[23] WHOIS API, Inc. "WHOIS API Offers Unified & Consistent Data." https://whois.whoisxmlapi.com/, accessed February 2024.

[24] X Corp. "Twitter API." *X Developer Platform*, https://developer.twitter.com/en/docs/twitter-api, accessed February 2024.

[25] XGBoost Developers. "XGBoost Documentation." dmlc XGBoost, https://xgboost.readthedocs.io/en/stable/, accessed February 2024.

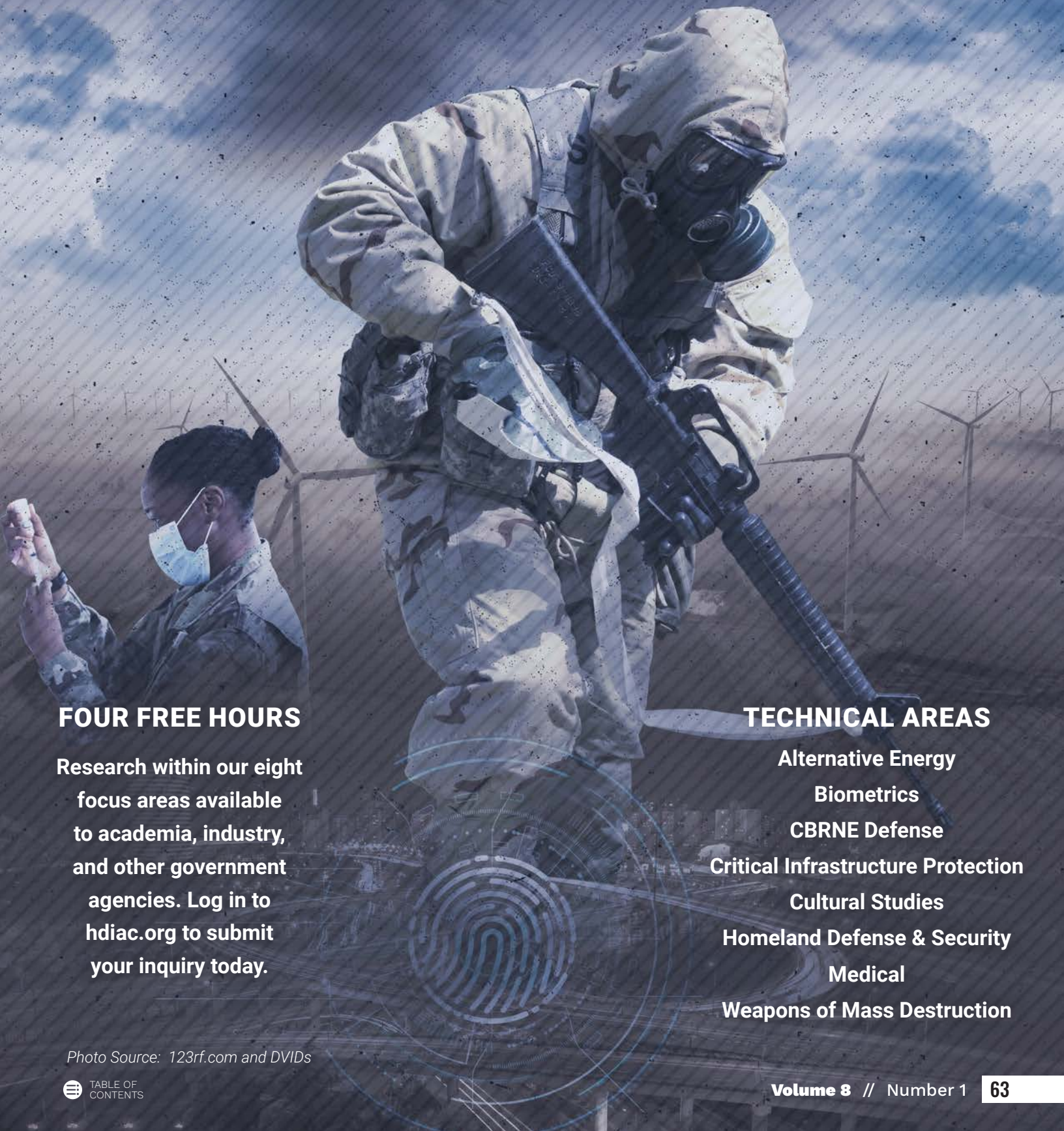
BIOGRAPHIES

DHIRENDRA SHUKLA is a professor and Dr. J. Herbert Smith Atlantic Canada Opportunities Agency chair in technology management and entrepreneurship at the University of New Brunswick (UNB), Canada, where he uses his telecom industry expertise and academic background to promote a bright future for UNB. His nominations as a finalist for Industry Champion by KIRA and Progress Media's Innovation in Practice Award show his tireless efforts and vision. Dhirendra was a finalist for the RBC Top 25 Canadian Immigrant Award. He received the 2017 Entrepreneur Promotion Award by Startup Canada and 2018 Outstanding Educator Award by the Association of Professional Engineers and Geoscientists of New Brunswick. Dr. Shukla holds a Ph.D. from King's London College.

MUHAMMAD MAZHAR ULLAH RATHORE is a postdoctoral researcher at the University of New Brunswick, Canada, where he researches Big Data Analytics, the Internet of Things, Smart Systems, Network Traffic Analysis and Monitoring, Remote Sensing, Smart Cities, Urban Planning, Intrusion Detection, and Information Security and Privacy. He serves as guest editor for various journals and is a professional member of the Institute of Electrical and Electronics Engineers and the Association for Computing Machinery. Dr. Rathore holds a Ph.D. in computer science and engineering from Kyungpook National University, South Korea, and a master's degree in computer and communication security from the National University of Sciences and Technology, Pakistan.

HDIAC Homeland Defense & Security Information Analysis Center

TECHNICAL INQUIRY SERVICES



FOUR FREE HOURS

Research within our eight focus areas available to academia, industry, and other government agencies. Log in to hdiac.org to submit your inquiry today.

TECHNICAL AREAS

Alternative Energy

Biometrics

CBRNE Defense

Critical Infrastructure Protection

Cultural Studies

Homeland Defense & Security

Medical

Weapons of Mass Destruction

Photo Source: 123rf.com and DVIDs

HDIAC JOURNAL

The Homeland Defense & Security Information Analysis Center (HDIAC) 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.HDIAC.ORG
CONNECT WITH US ON SOCIAL MEDIA