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

VOLUME 9 | NUMBER 1 | 2025

HDIAC JOURNAL

Integrated Sensing and Communications for Small UAV Applications in CELLULAR NETWORKS

HDIAC JOURNAL

Volume 9 // Number 1 // 2025

Editor-in-Chief:
Aaron Hodges

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.

Copyright © 2025 by the SURVICE Engineering Company. This journal was developed by SURVICE under HDIAC contract FA8075-21-D-0001. The Government has unlimited free use of and access to this publication and its contents, in both print and electronic versions. Subject to the rights of the Government, this document (print and electronic versions) and the contents contained within it are protected by U.S. copyright law and may not be copied, automated, resold, or redistributed to multiple users without the written permission of HDIAC. If automation of the technical content for other than personal use, or for multiple simultaneous user access to the journal, is desired, please contact HDIAC at 443.360.4600 for written approval.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or HDIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or HDIAC and shall not be used for advertising or product endorsement purposes.

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: 123RF.com)*.

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 26

INTEGRATED SENSING AND COMMUNICATIONS FOR SMALL UAV APPLICATIONS IN CELLULAR NETWORKS

By Amjad Soomro and Mark Norton

This article explores the potential integrated sensing and communication (ISAC) protocols for detecting small unmanned aerial vehicles (UAVs). The convergence of communication and sensing technologies presents a unique opportunity to enhance UAV detection capabilities, leveraging existing communication infrastructure and spectrum resources.

IN THIS ISSUE

WEB EXCLUSIVE

Financing of Terrorism Through Cryptocurrencies

By Keven Hendricks | Photo Source: Canva

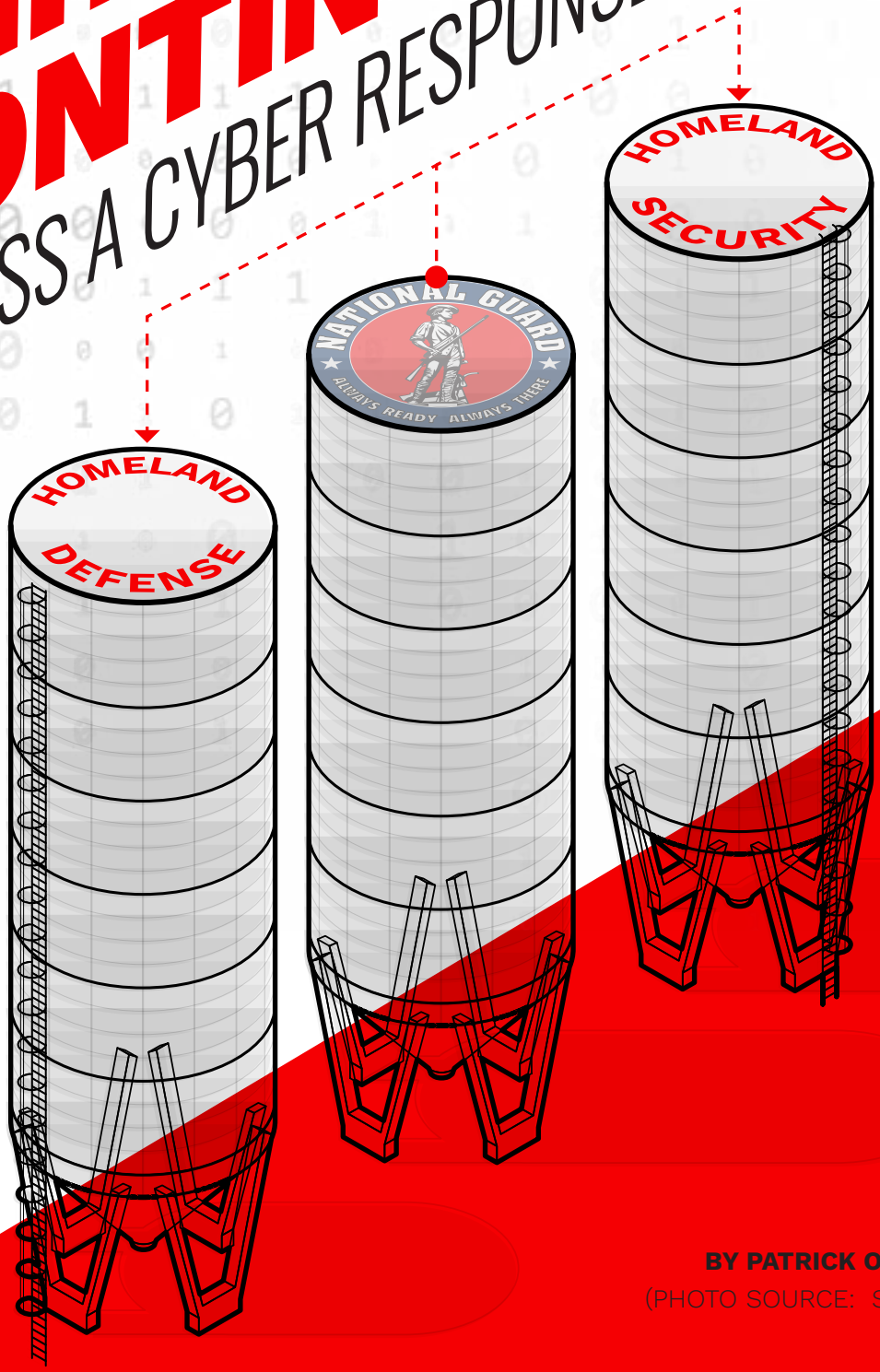
This article examines how terrorist organizations began to incorporate cryptocurrencies as part of their financing networks in tandem with the rise of dark web drugs. Cryptocurrencies remain a persistent medium for the fiduciary networks that enable terrorism around the world.

AVAILABLE ONLY ONLINE

https://hdiac.dtic.mil/articles/financing-terrorism-through-cryptocurrencies

ENHANCING CONTINUITY

ACROSS A CYBER RESPONSE



BY PATRICK O'BRIEN BOLING

(PHOTO SOURCE: SHUTTERSTOCK)

SUMMARY

The increasing sophistication and frequency of cyber incidents targeting U.S. infrastructure highlight an urgent need for a unified cyber response that bridges Homeland Security (HS) and Homeland Defense (HD). The National Guard's (NG's) Cyber Protection Teams (CPTs) are uniquely positioned to enhance continuity across this spectrum by operating flexibly under both HS and HD authorities and collaborating through Civil Support (CS) and Defense Support of Civil Authorities (DSCA).

This article examines key definitions—Homeland, HS, HD, CS, and DSCA—and introduces the "Response Spectrum" model, illustrating the progression from HS-led incident response to HD-led threat response. Additionally, it outlines the U.S. Department of Defense's (DoD's) cyberspace operations structure, including Defensive Cyberspace Operations–Internal Defensive Measures (DCO-IDM), Defensive Cyberspace Operations–Response Actions (DCO-RA), and Offensive Cyberspace Operations (OCO), to propose a cohesive cybersecurity strategy. By reinforcing coordination among civilian and military entities, the United States can build a resilient cybersecurity posture prepared to respond to various threats, ensuring comprehensive protection and national resilience in the evolving cyber domain.

ENHANCING CONTINUITY ACROSS HS AND HD

Cyber resilience has become a critical component of national security in today's complex and interconnected threat landscape. The increasing frequency and sophistication of cyber incidents targeting U.S. infrastructure highlight the need for a coordinated response across federal, state, and local levels. This response must involve HS and HD, which have traditionally operated under separate mandates yet now face converging challenges in the cyber domain. The NG's CPTs present a unique opportunity to strengthen continuity and effectiveness across a spectrum of cyber responses due to their flexibility to operate under both HS and HD authorities and their capacity to integrate with public-private partnerships. These capabilities enable the NG to bridge the gap between civilian and military responses and support resilience through DSCA.

> ***Cyber resilience has become a critical component of national security in today's complex and interconnected threat landscape.***

This article first clarifies the definitions of critical terms essential to understanding the distinct but overlapping roles in cyber operations: Homeland, HS, HD, CS, and DSCA. It then explores the concept of a "Spectrum of Response" that illustrates the progressive transition from incident response (HS-led) to threat response (HD-led) and how CS and DSCA serve as critical links in this continuum. Examining these roles and responsibilities can gain a better understanding of how the NG, under its unique state active duty (SAD) and U.S. Code Title 32 authorities [1], can operate effectively within civilian and military frameworks.

Furthermore, this article delves into the U.S. Joint Doctrine's definitions of security, defense, and offense, offering insights into the structured approach to cyberspace operations. The DoD categorizes these operations into DCO-IDM, DCO-RA, and OCO, which together form a comprehensive strategy for cyberspace resilience. These elements are crucial to building a cybersecurity posture adaptable to various threats while maintaining interagency cooperation, robust communication channels, and rapid-response capabilities.

Through this detailed examination of roles, responsibilities, and strategies, the article underscores the importance of DSCA and CS in fostering a unified approach to cybersecurity. By enhancing coordination between civilian agencies and military assets, prioritizing continuous training and intelligence sharing, and leveraging NG capabilities under SAD and Title 32, the United States can significantly

improve its readiness to confront cyberthreats, ensuring the nation's security and resilience across a spectrum of potential crises.

DEFINITIONS

To truly understand the complexity of cybersecurity, it is necessary to review definitions of key concepts and explain their meanings, beginning with Homeland, HS, and HD.

The **Homeland** is "the physical region that includes the continental United States, Alaska, Hawaii, United States territories, and surrounding territorial waters and airspace" [2].

HS is "a concerted national effort to prevent terrorist attacks within the United States and to reduce our vulnerability to terrorism, major disasters, and other emergencies" [3].

HD refers to "the military protection of U.S. sovereignty and territory against external threats and aggression or, as directed by the President, other threats" [3].

However, this article introduces the following HS vs. HD simplified definitions, as proposed by the author:

- **HS primarily focuses on preventing and mitigating incidents within the United States' borders**, encompassing various measures from counterterrorism to disaster response.
- **HD emphasizes protecting the nation against external threats before or once they reach U.S. soil**, often involving military capabilities and international partnerships.

CS encompasses the NG's (Title 32) and State Guards' (SAD) support to state to local civil authorities for domestic incidents like natural or artificial disasters, terrorism, and other emergencies.

DSCA provides a formal structure allowing federal military assets under U.S. Code Title 10 [4] to support civilian agencies in emergencies, including cyber incidents. Under DSCA, federal military forces can be deployed at the request of civil authorities to address domestic threats [2]. While DSCA focuses on immediate response needs, CS includes ongoing collaboration and supports long-term civilian resilience through capacity-building, training, and infrastructure security [5].

Imagine two overlapping circles. Label one circle "Homeland Security (HS)" and the other "Homeland Defense (HD)." In the area where the circles overlap, write "Civil Support (CS)" and "Defense Support of Civil Authorities (DSCA)" to illustrate how CS and DSCA exist where HS and HD intersect. This visual demonstrates how HS and HD contribute to the nation's security and defense. CS and DSCA are critical components bridging these domains during domestic emergencies and crises. Though there is an overlap between "All Hazard Response" and "Persistent Attack on Homeland (Homeland Defense)" there is a point of transition for the decision (see the dashed line in Figure 1).

SPECTRUM OF RESPONSE

The introduction of a concept referred to as the "Spectrum of Response" illustrates the progressive transition from incident response to threat response. The Spectrum of Response considers that a hostile act may not initially start as an apparent threat, and, therefore, the initial reaction might be an incident response. Threats conducting grey zone activities may successfully disguise an attack and delay the response necessary to neutralize the threat. Beginning with the broader U.S. Joint Doctrine, outside of the specific context of cyberspace, the terms security, defense, and offense are defined with broader military applications in mind.

In military doctrine, **security** refers to measures a military force takes to protect itself against threats like espionage, sabotage, attack, and surprise. Security includes safeguarding troops, installations, activities, and information from hostile actions and influences. This concept is central to military operations, ensuring that forces can operate effectively without undue interference from adversarial actions [6].

In military terms, **defense** employs all available means and methods to

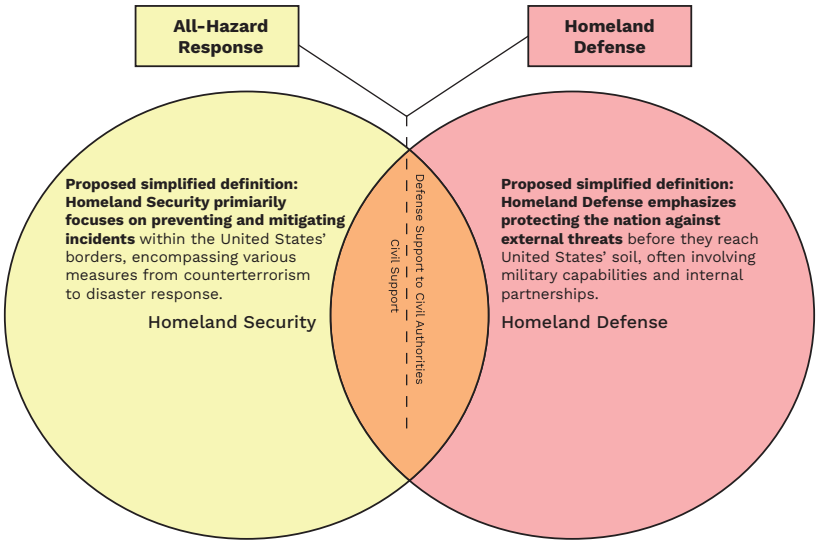


Figure 1. HS and HD Interactions *(Source: P. Boling)*.

> ***Security includes safeguarding troops, installations, activities, and information from hostile actions and influences.***

avoid or minimize damage from enemy actions and counter or defeat hostile forces. Defensive operations are undertaken to protect personnel, equipment, and designated areas from threats, thus enabling freedom of maneuver and resilience against attacks [7]. Active and passive defensive operations are conducted to repel or neutralize enemy attacks, buy time, conserve resources, or create conditions favorable for future offensive actions.

Offensive operations are actions taken to impact an enemy's operational capability or influence other strategic aspects of the conflict, aiming to achieve national or coalition objectives. Offense focuses on direct engagement to disrupt or neutralize enemy forces, seizing control, and asserting dominance in contested areas [8]. Offensive operations are designed to seize, retain, and exploit the initiative, defeating or destroying enemy forces, gaining territory, and imposing the commander's will upon the enemy.

Considering these definitions and how the U.S. military conceptualizes its operations in traditional warfare settings, these operations focus on physical engagements, territorial control, and direct application of force. They are foundational to military strategy, guiding how forces are organized, trained, and employed in various combat scenarios. The Spectrum of Response provides a framework for moving along a road to war and accounting for how ambiguity delays the focus transition across security, defense, and offense. While the offense waits for the threat to be identified and based on what a potential adversary may seek to exploit in the grey zone (see Figure 2), the defense can start early.

INTEGRATING HS, HD, DSCA, AND CS FOR CYBERSECURITY RESILIENCE

The complex and rapidly evolving cyberthreat landscape requires a coordinated response involving civilian and military capabilities. HS and HD are two distinct but interconnected frameworks for addressing national security needs, with DSCA and CS doctrines providing critical support during cyber emergencies. This article examines the roles of HS, HD, DSCA, and CS within cybersecurity, proposing a unified approach to bolster national resilience.

Understanding cybersecurity's role within national security requires clarifying the distinctions between HS, HD, DSCA, and CS. Led by the Department of Homeland Security (DHS), HS is the primary federal agency responsible for protecting the United States from various threats, including cyberattacks. It focuses on mitigating and responding to threats within U.S. borders, including counterterrorism and disaster response. Led by the DoD, HD protects U.S. sovereignty and territory from external threats, including cyber adversaries.

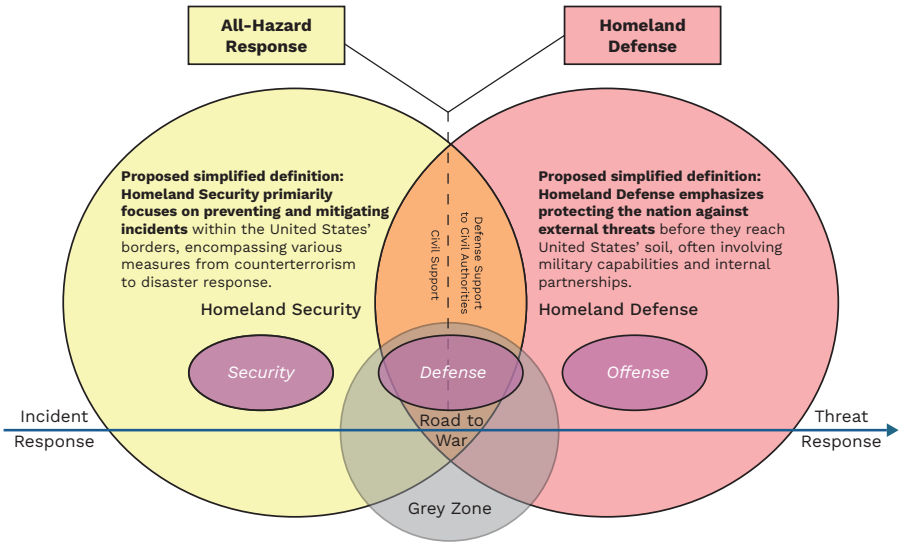


Figure 2. HS and HD Interactions With Security, Defense, and Offense *(Source: P. Boling)*.

> ***Understanding cybersecurity's role within national security requires clarifying the distinctions between HS, HD, DSCA, and CS.***

INTERPLAYING HS, HD, DSCA, AND CS IN CYBERSECURITY

In the cyber domain, HS and HD face overlapping challenges that demand coordinated efforts to defend critical infrastructure from internal and external cyberthreats. Cyberspace is a "global domain within the information environment consisting of interdependent information technology networks" [9], making it susceptible to foreign and domestic actors.

Cyberthreats targeting critical infrastructure blur the boundaries between HS and HD, requiring the integration of DSCA and CS to support immediate response and long-term cybersecurity resilience. The DoD's National Defense Strategy [10] highlights HD as a top priority, emphasizing the need to synchronize with HS to address complex cyberthreats. Including CS within this framework adds depth by focusing on sustained support and capacity building for civilian agencies. This includes providing ongoing training, sharing best practices, and assisting in developing robust cybersecurity policies—all reinforcing the resilience of HS-led efforts over time.

TRANSLATING DOCTRINAL LANGUAGE TO CYBERSPACE OPERATIONS

According to Joint Publication (JP) 3-12 [9], the correct doctrinal terms for cyberspace security, defense, and offense operations within the DoD are defined in Figure 3.

These terms reflect the structured approach to both defensive and offensive cyber operations as delineated in JP 3-12, with each term specifically addressing different aspects of cyberspace operations. This doctrinal language provides a clear framework for categorizing and conducting cyber operations within the DoD, helping integrate them effectively with HS, HD, CS, and DSCA efforts.

This triad of DCO-IDM, DCO-RA, and OCO enables a comprehensive approach to achieving and maintaining security in various domains, particularly in the increasingly contested cyber domain (see Figure 4).

STRATEGIES FOR INTEGRATED CYBERSECURITY USING DSCA AND CS

Strengthening CS and DSCA for Cybersecurity Resilience

CS and DSCA must work together to bolster immediate response capabilities and long-term defense strategies to achieve robust cybersecurity. CS provides a foundation for sustained collaboration, where DoD assets and expertise support civilian agencies

CYBERSPACE SECURITY (DCO-IDM)

Operations involving actions taken within the "DoD Information Networks (DODIN)" to protect, monitor, analyze, and respond to unauthorized activities. They focus on proactively securing the DOD's systems, including implementing security measures to prevent unauthorized access, exploitation, or damage.

CYBERSPACE DEFENSE (DCO-RAO)

Operations aimed to defend DoD cyberspace by detecting, analyzing, countering, and mitigating threats. They encompass actions to detect and respond to threats that have breached or threaten to breach the DoDIN, including identifying, countering, and mitigating malware and unauthorized activity. DCO-RA are specific to actions taken outside DoDIN in response to cyber threats impacting U.S. interests.

CYBERSPACE OFFENSE (OCO)

Operations intended to project power by applying force in and through cyberspace. Their actions create noticeable denial effects, such as degradation, disruption, or destruction of information systems or networks or manipulation, leading to denial effects in the physical domain. Essentially, OCO aims to achieve national objectives by targeting adversary systems.

Figure 3. Cyberspace Security, Defense, and Offense Operations *(Source: JP 3-12 [9] and Canva).*

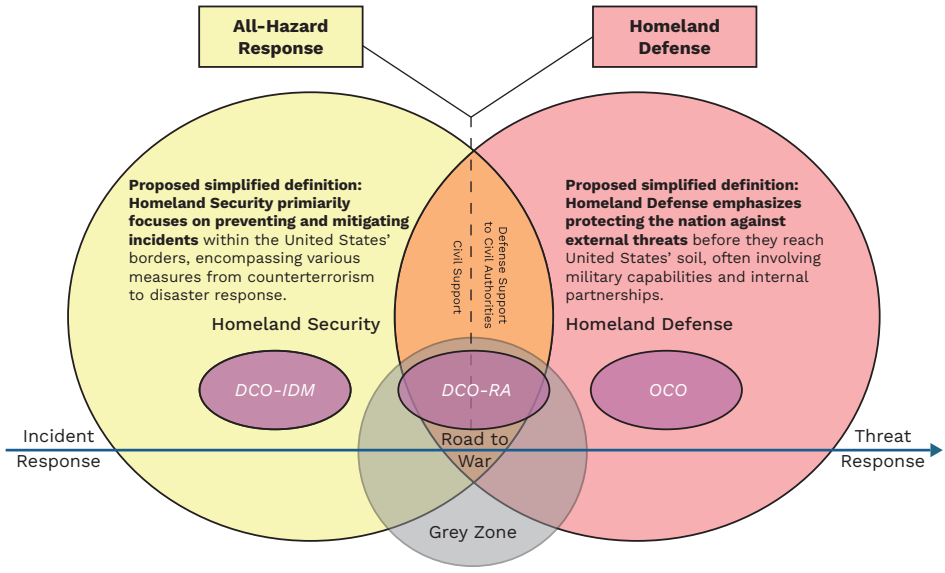


Figure 4. HS and HD Interactions With Defensive and Offensive Cyber Operations *(Source: P. Boling).*

beyond emergencies. States can enhance interagency coordination with DHS and federal agencies through CS, integrating defense capabilities into cybersecurity preparedness frameworks.

Conversely, DSCA enables immediate deployment of military resources during cyber crises. For example, NG CPTs activated during the 2020 elections exemplified DSCA in action, supporting state and local authorities in safeguarding election systems. By establishing robust DSCA and CS frameworks, the DoD can respond effectively to cyber emergencies while enhancing civilian agencies' preparedness through continuous training and resource allocation.

Integrating CS With NG Cyber Capabilities

Under SAD and Title 32, NG personnel operate under the authority of the state governor. They are mobilized for state missions, such as natural disaster response or civil support, and are funded by the state.

The SAD status allows the NG to directly support local government agencies, including cybersecurity assistance, while aligning with state laws. In SAD status, personnel are not restricted by the Posse Comitatus Act [11] because personnel are not federalized; in their Title 32 status, they are under the authority of the State and thus allowed to support law enforcement.

Title 32 allows NG units to operate under state authority with federal funding, making them critical players in CS and DSCA efforts. This authority enables NG units to conduct cyberspace defense activities for crucial infrastructure while remaining under state control and complying with federal and state laws. The NG's unique status allows for rapid deployment during crises (DSCA) while supporting ongoing cybersecurity training and preparedness (CS) through coordinated efforts with civilian agencies. Unlike SAD and Title 32, Title 10 status restricts Guard members from direct law enforcement activities due to Posse Comitatus limitations.

Under Title 10, NG members are federalized, operating under the authority of the President and the DoD. In this status, personnel are fully integrated with active-duty forces, allowing them to participate in national defense missions, including offensive and defensive cybersecurity operations. U.S. Code Title 50 [12] authority is generally exercised in a federalized (Title 10) context and in close collaboration with intelligence agencies.

This article does not discuss Title 50 in detail, but a potential consideration is using NG CPTs under Title 50. Title 50 provides a legal framework for the NG's involvement in national security-related cyber missions, typically when intersecting with intelligence gathering, covert activities, or classified defense strategies. While not traditionally associated with the NG's operational statutes, Title 50 does provide a legal framework for the Guard's involvement in national security-related cyber missions.

OPERATIONALIZING NG CPTs WITH HS, HD, DSCA, AND CS

Under the CS and DSCA frameworks, NG cyber units can participate in joint training exercises with DHS, the Federal Bureau of Investigation (FBI), and private sector partners, bolstering interagency cooperation and cybersecurity readiness relationships that can be critical in future cyber incidents. These exercises improve real-time communication, develop shared protocols, and build capability.

The NG CPT's ability to work across SAD, Title 32, and Title 10 statuses positions it as a versatile asset for cybersecurity within the CS and DSCA frameworks. NG units can contribute significantly by conducting infrastructure assessments, facilitating information-sharing initiatives, and providing cybersecurity education to communities. NG CPTs can sign Non-Disclosure Agreements (NDAs) with civil, private, and industry partners and maintain continuity and confidentiality across the incident and threat response spectrum. These activities bolster the cybersecurity posture of both HS and HD, effectively reducing the nation's vulnerability to cyber incidents and enhancing overall resilience [13].

Lt. Col. McKinney recommends using outlines of the pressing need for clear authority and structure within the U.S. Air National Guard to address cyberattacks on U.S. critical infrastructure [14]. Current legislation limits the NG's capability to prepare for and respond to cyberthreats in Title 32 (state-level) status, even though it is involved in other domestic operations and military alert programs. Policymakers should create legislation that would empower the NG to operate in cyberspace effectively, paralleling its active support roles in different areas like the U.S. Coast Guard's Maritime Operational Threat Response and NG's counter-drug support, wildfire suppression, and air defense.

Multiple stakeholders, including the President, the DoD, DHS, and Congress, underscore the urgency of strengthening cybersecurity

efforts. They seek to protect digital infrastructure, recognizing cyberthreats as one of the most significant challenges to national security. Recommendations emphasize legal changes to integrate NG cyber forces in domestic cybersecurity and collaborate with DHS, United States Cyber Command (USCYBERCOM), FBI, and state agencies. Implementing these measures would ensure NG cyber forces can defend critical public and private infrastructure nationally.

> ***Multiple stakeholders, including the President, the DoD, DHS, and Congress, underscore the urgency of strengthening cybersecurity efforts.***

INTEGRATING OFFENSIVE AND DEFENSIVE CYBER MEASURES

Offensive and defensive cyberspace operations are integral to HD and HS. USCYBERCOM coordinates these efforts with the DoD, DHS, and other federal agencies to enhance the nation's cyber resilience. These agencies ensure operational readiness by conducting joint training and exercises, enabling swift responses to cyber incidents. Through coordinated DCO-RA, DCO-IDM, and OCO, HS, HD, DSCA, and CS can build a comprehensive defense posture.

Laws governing military actions within the United States also apply to cyberspace, limiting DoD operations to gray and red cyberspace (neutral and adversarial networks) unless DSCA permits otherwise. These regulations ensure that DoD involvement respects civil liberties while providing critical support to civilian agencies when necessary.

RECOMMENDATIONS FOR STRENGTHENING CYBERSECURITY THROUGH DSCA AND CS

The shift from HS to HD marks a critical transition from a primarily civilian-led approach to a more integrated framework involving civilian and military assets. This shift requires states to adapt by enhancing coordination between civilian agencies and the military, fostering interoperability, and establishing clear lines of communication and command to ensure effectiveness during crises. Such strategies are feasible and essential for strengthening the country's collective security and defense. By investing in joint training exercises, sharing intelligence, and conducting collaborative risk assessments, states can significantly enhance their ability to respond effectively to a wide range of threats, creating a more resilient defense posture across the spectrum of security and defense challenges.

To effectively enhance cybersecurity resilience through CS, states must develop comprehensive plans that clearly outline procedures for integrating DoD support into routine cybersecurity activities. These CS plans should prioritize continuous training, regular risk assessments, and robust intelligence-sharing mechanisms between civilian agencies and the DoD. By doing so, states can create well-prepared, unified, proactive response frameworks to address evolving cyberthreats [15].

Adequate DSCA and CS rely on robust communication networks to facilitate real-time threat intelligence sharing across federal, state, and local agencies. Establishing liaison officers and interagency planning cells and conducting regular tabletop exercises under the CS framework are essential to strengthening these networks. These practices ensure critical information flows seamlessly between agencies, enhancing coordination and response capabilities during routine operations and crises [16].

The NG CPTs are uniquely positioned to support cybersecurity across SAD, Title 32, and Title 10 statuses, making them a versatile asset within CS and DSCA. NG CPTs play a vital role by

conducting infrastructure assessments, sharing critical information, and educating communities about cybersecurity. They can engage with private industry through NDAs, ensuring confidentiality and continuity in response efforts and thereby strengthening both HS and HD. Current legislation limits NG's ability to respond to cyberthreats in Title 32 status. However, policymakers are urged to empower the NG to operate effectively in cyberspace, similar to support roles like counter-drug operations and wildfire suppression. Strengthened collaboration with DHS, USCYBERCOM, and the FBI is recommended to enhance NG's capability to defend critical national infrastructure from cyberthreats.

CONCLUSIONS

The evolving cyberthreat landscape necessitates an integrated and adaptable approach to national cybersecurity resilience. By leveraging the NG CPTs within the framework of both HS and HD, the United States can create a coordinated cyber response that can operate effectively across federal, state, and local levels. This capability is further enhanced by the flexibility of the NG to operate under Title 32 and Title 10 authorities, bridging the civilian-military divide and facilitating essential public-private partnerships that reinforce cyber resilience.

> ***By leveraging the NG CPTs within the framework of both HS and HD, the United States can create a coordinated cyber response that can operate effectively across federal, state, and local levels.***

The comprehensive examination of key concepts like Homeland, HS, HD, CS, and DSCA illustrates the critical overlap between HS and HD and the importance of clear, unified definitions within doctrine.

This article's Spectrum of Response model, which spans from HS-led incident response to HD-focused threat response, emphasizes the progressive shift required to address increasingly ambiguous and sophisticated cyberthreats. Utilizing established definitions of security, defense, and offense, as well as cyberspace-specific doctrines like DCO-IDM, DCO-RA, and OCO, provides a structured approach for preventative and responsive measures.

Ultimately, by strengthening the synergy between DSCA and CS, prioritizing interagency coordination and communication, and harnessing the unique capabilities of the NG under SAD, Title 32, and Title 10, the United States can significantly enhance its cybersecurity posture. A robust, unified response framework improves immediate crisis response capabilities and fosters a long-term commitment to building resilient civilian infrastructures. As the cyber domain continues to evolve, such a proactive and coordinated strategy will be essential to protecting national security interests and ensuring a resilient defense against an increasingly complex spectrum of cyberthreats. ■

REFERENCES

[1] U.S. House of Representatives. U.S. Code Title 32 – National Guard, 10 August 1956.

[2] Joint Chiefs of Staff. "JP 3-28: Defense Support of Civil Authorities." Washington, DC, 17 April 2018.

[3] Joint Chiefs of Staff. "JP 3-27: Homeland Defense." Washington, DC, 29 November 2021.

[4] U.S. House of Representatives. U.S. Code Title 10 – Armed Forces, July 2011.

[5] Jackson, B. A. "The Role of the U.S. Department of Defense in Domestic Disaster Response: Legislative Evolution and Issues for Congress." Santa Monica, CA: RAND Corporation, 2018.

[6] Joint Chiefs of Staff. "JP 3-10: Joint Security Operations in Theater." Washington, DC, 13 November 2014.

[7] Joint Chiefs of Staff. "JP 3-0: Joint Operations." Washington, DC, 17 January 2017.

[8] Joint Chiefs of Staff. "JP 3-09: Joint Fire Support." Washington, DC, 10 December 2019.

[9] Joint Chiefs of Staff. "JP 3-12: Cyberspace Operations." Washington, DC, 8 June 2018.

[10] U.S. DoD. "2022 National Defense Strategy of the United States of America." Washington, DC, 2022.

[11] U.S. Congress. Posse Comitatus Act, 15 June 1878.

[12] U.S. House of Representatives. U.S. Code Title 50 – War and National Defense, 2011.

[13] Jensen, E. T. "Cyber Sovereignty: The U.S. Perspective and the Implications for National Guard Cyber Operations." Washington, DC: Georgetown University Press, 2020.

[14] McKinney, Lt. Col. M. M. "A National Solution: Rethinking the Employment of Air National Guard Title 32 Status Citizen-Airmen to Defend the Nation's Cyberspace Infrastructure." Unpublished research paper, Air War College, Maxwell Air Force Base, AL, 2013.

[15] Brenner, S. W. "Cyberthreats: The Emerging Fault Lines of the Nation State." New York, NY: Oxford University Press, 2019.

[16] Lin, H. S., and A. B. Zegart, eds. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington, DC: Brookings Institution Press, 2019.

BIBLIOGRAPHY

Ferguson, A. T. "Closing the Gaps: Cybersecurity for U.S. Forces and Commands." Ph.D. dissertation, Joint Forces Staff College, Joint Advanced Warfighting School, 2017.

OpenAI. ChatGPT [Large language model], https://chatgpt.com, 2024.

xAI. Grok. AI Chatbot, https://x.com/i/grok, 2024.

BIOGRAPHY

PATRICK O'BRIEN BOLING, a recent graduate of the Joint Combined Warfighting School, serves as Deputy for the J7 Plans, Exercises, and State Partnership Program Division in the Louisiana National Guard. He has served in a variety of joint, strategic, operational, and tactical assignments in the U.S. Army and National Guard as a field artillery officer and infantry officer. LTC Boling holds an M.S. in management of engineering from Louisiana Tech University, an M.S. in administration of justice and security from the University of Phoenix, and a Ph.D. in organizational management from Capella University.

HDIAC WEBINAR SERIES

HDIAC hosts live online technical presentations featuring a DoD research and engineering topic within our technical focus areas. Visit our website to view our upcoming webinars.

(Photo Source: Canva)

BREAKING THROUGH INTELLIGENCE SILOS FOR

DOMESTIC EMERGENCY MANAGEMENT

BY MICHAEL PRASAD (PHOTO SOURCE: CANVA AND U.S. COAST GUARD)

INTRODUCTION

While there are gaps in the United States between law enforcement and emergency management on intelligence and information sharing, those gaps also extend to other members of the intelligence community (IC). This includes U.S. Department of Defense (DoD) groupings and non-DoD military groups such as the U.S. Coast Guard (USCG)—especially as they relate to the DoD's support to civilian authorities.

Past headlines have shown the adverse impacts from the disconnects on intelligence sharing between solo—and siloed—law enforcement entities and other groups, including federal law enforcement entities. Per U.S. Presidential Policy Directive (PPD)-8 [1], intelligence and investigation roles [2] at the U.S. Department of Homeland Security (DHS)/ Federal Emergency Management Agency (FEMA) are limited to law enforcement-driven interdiction and investigation and do not flow across all five mission areas (see Figure 1) in all threats/hazards [3]. Because of this, those roles are only defined in the prevention and protection mission areas in the figure.

Even internally within divergent law enforcement entities on a law enforcement-centric incident response, these "failures to share intelligence" can have adverse impacts on life safety, such as the tragedy at the Robb Elementary School in Uvalde, TX [4]. Compounding this intelligence-siloing problem, when U.S. military elements (whether federalized or state/territory controlled) are introduced for civilian support, there is not a clear set of processes and procedures in the United States to utilize and share actionable intelligence to benefit emergency management in support of that response.

The solution is to shift the roles for and concept of intelligence from a law-enforcement/terrorism view to one applicable to a broader set of needs for overall emergency management while still preserving and protecting the civil liberties and privacy rights of U.S. citizens [5]. Thus, the introduction of a concept of the overarching collection of curated emergency management intelligence (EMINT) elements applies to civilian-led incident operations. Through a comprehensive review of the plans, organizations (and staff roles), equipment and systems, training, and joint exercises between military and civilian emergency management groupings, EMINT can be applied. It is through emergency management principles and actions that the unified command and control—the unity of effort—can be achieved through coordination, collaboration, cooperation, and communication. This was lacking on 9/11 [6] (and most likely before that) and continues even now.

This article focuses on the domestic emergency management adverse impacts of the silos for intelligence curation and distribution within the United States at the federal level. It covers the various federalized DoD military groupings to include the USCG and the National Guard units and other members of our national IC like the Federal Bureau of Investigation (FBI) and DHS.

On an all-hazard/all-threat basis, the tactical gaps between our nation's collective IC and the local emergency management professionals and practitioners can limit the missions for successful emergency management and may even cause harm or death to U.S. persons. Such threats and hazards can include, but are not limited to, those that generate domestic incidents where the traditional tradecraft of the IC may come into play, such as acts of terrorism or materialized, onshore national security concerns.

It is also worth noting that these same IC groups have access to intelligence generated or adversely impacted by other threats and hazards like natural ones. This also includes cascading adverse impacts like the Key Bridge collapse in 2024 [7] or complex aspects of human-made accidents like the massive train derailment in East Palestine, OH, in 2023 [8].

In many countries, including the United States, the thought of intelligence sharing external to homeland security and law

PREVENTION	PROTECTION	MITIGATION	RESPONSE	RECOVERY
Planning				
Public Information and Warning				
Operational Coordination				
Intelligence and Information Sharing		Community Resilience	Infrastructure Systems	
Interdiction and Disruption		Long-Term Vulnerability Reduction	Critical Transportation	Economic Recovery
Screening, Search, and Detection		Risk and Disaster Resilience Assessment	Environmental Response/Health and Safety	Health and Social Services
Forensics and Attribution	Access Control and Identity Verification	Threats and Hazards Identification	Fatality Management Services	Housing
	Cybersecurity		Fire Management and Suppression	National and Cultural Resources
	Physical Protective Measures		Logistics and Supply Chain Management	
	Risk Management for Protection Programs and Activities		Mass Care Services	
	Supply Chain Integrity and Security		Mass Search Rescue Operations	
			On-scene Security, Protection, and Law Enforcement	
			Operational Communications	
			Public Health, Healthcare, and Emergency Medical Services	
			Situational Assessment	

Figure 1. Core Capabilities by Mission Areas *(Source: FEMA/DHS [3]/Canva).*

> ***In many countries, the thought of intelligence sharing external to homeland security and law enforcement may be a new concept.***

enforcement may be a new concept. It is quite unusual for there to be curation (collection, analysis, and distribution) of actionable intelligence *beyond* the traditional silos of the IC. In other countries (e.g., New Zealand [9]), that curation of actionable EMINT is already integrated into their overall emergency management doctrine, policies, practices, and procedures, regardless of the type of threat or hazard. And such an emergency management viewpoint is much broader than the vantage point of homeland security and law enforcement by themselves.

As shown in Figure 2, EMINT is actionable intelligence necessary for life safety, incident stabilization, property/asset protection, economic/environmental stability, and recovery from the adverse impacts of hazards generated by any threat [10].

EMINT needs to be curated and disseminated on a "need-to-know" basis before, during, and after incidents occur. It can be curated from open-source intelligence (OSINT), human intelligence, geospatial intelligence (GEOINT), economic intelligence, weather intelligence (WEATHINT), communications intelligence, and other intelligence sources.

EMINT is novel and agile in its definition [11]. For many U.S. civilian-led incidents, there is the current model of *situational awareness* which can represent "what is happening now" and what *might* happen "next." This tends to be self-limiting for those incident management teams (IMTs) who do not have strong connections to law enforcement or their own connection to intelligence and homeland security built into their current steady-state structure. Those emergency management groups can be siloed away from the intelligence available. On the other hand, there are jurisdictions who have recognized and corrected this. For example, New Jersey's Office of Emergency Management is operated by their state police, and their Fusion Center [12] with standing members of their state-level Office of Homeland Security and Preparedness residing in the same building as their state emergency operations center.

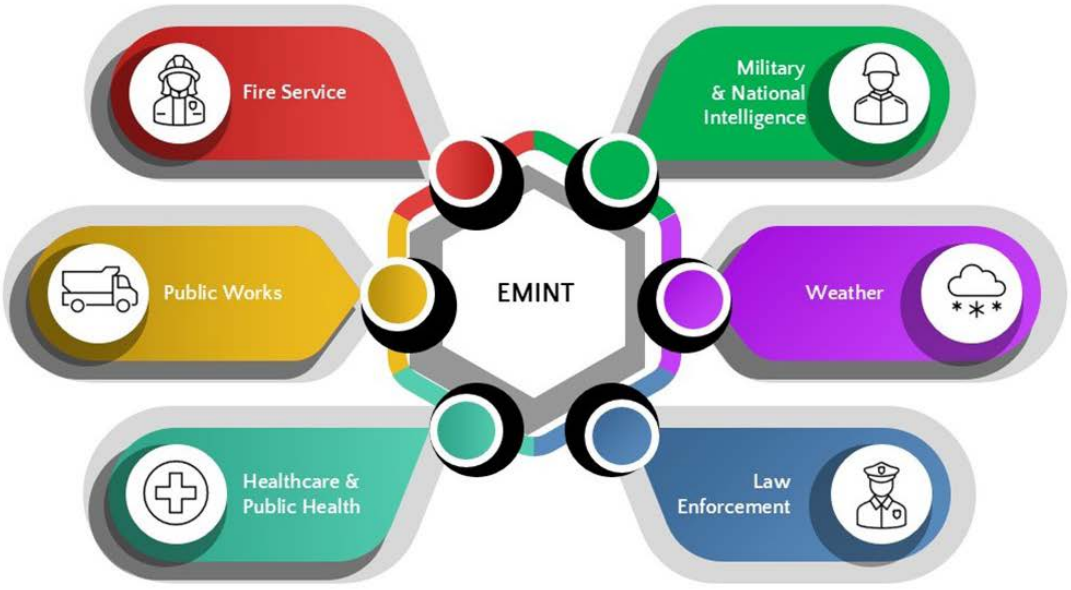


Figure 2. Examples of the Nexus to EMINT *(Source: Center for Emergency Management Intelligence Research [CEMIR] [10])*.

When considering the overall concept of intelligence gathering, analysis, and distribution only applying to criminal activities or terrorism, the activities of EMINT are generally not performed. This severely limits command and control (C2) of any incident.

There are many cases where intelligence was needed when information was only provided or limited to law enforcement organizations. For example, there are major differences between what is defined as weather information, weather forecasting, and WEATHINT. Weather information can include historical data and trend analysis and represent what is happening now, as well as what has happened in the past. Weather forecasting (e.g., meteorology and climatology) can represent what might happen next. WEATHINT is achieved when cross-walked with population centers, socially vulnerable population areas, critical infrastructure sites, and more. It represents the **how we will be adversely impacted**, as well as many of the **what ifs** needed by C2 for successful consequence management.

A straight line can be drawn for many threats—terrorism and domestic violent extremism included—to local hazards with adverse impacts to populations. This can occur where emergency management (not just law enforcement) has jurisdictional responsibilities for life safety during response operations, as well as overall protection and prevention aspects on a whole-community basis. In addition, there is a typology of disasters originating as natural threats and becoming technological hazards or Natech incidents [13]. The *probability* of a bad actor capitalizing on the adverse impacts from a disaster created by a natural threat and then cascading it into a greater disaster is very real.

There are many cases where intelligence was needed when information was only provided or limited to law enforcement organizations.

This article will introduce EMINT to a military audience to enhance and amplify the U.S. Department of Defense's Support to Civilian Authorities [14], encouraging the exploration of the tactical view for shared intelligence support via Joint Publication (JP) 2-0: "Joint Intelligence" [15]; JP 3-28: "Defense Support to Civil Authorities" [16]; the recently updated DoD Directive 5240.01 [17]; and other DoD doctrine from a local civilian emergency management perspective (and not a law enforcement one). The deliberative planning needed to create/refine emergency operations plans, organize staffing, allow for access to equipment/systems, and conduct joint training and exercises must be established for steady-state and disaster-state operations on incidents of scale. This is distinctly critical for civilian-led and DoD-supported operations.

PROBLEM STATEMENT

The current tactical model is too focused on terrorism/counterterrorism and needs improvement. Not enough is systemically being performed for the nation's "Duty to Warn" [18] to extend through a local jurisdiction's emergency management besides its law enforcement entities. Because of this, the following needs addressed:

- There is the U.S. Department of Justice's (DOJ's) Anti-Terrorism Advisory Council [19]. Does this group operate at the tactical level? Is the sharing of information, in fact, the sharing of intelligence? Does it flow in both directions? How can the private sector receive timely tactical outputs/warnings with actionable EMINT? A global CrowdStrike software error occurred in 2024, with almost all the economic sectors and large private businesses becoming adversely impacted for days and longer. There was a well-communicated and collaborative aspect for solutioning among governmental resources and the private sector. Would this all be the same for a cyberattack from a foreign adversary?
- Will the DOJ continue to limit its intelligence sharing to only law enforcement, as shown in Figure 3?

Or will it expand the bidirectional networking the nation needs for protecting the critical infrastructure possibly through its InfraGard program and with members of the private sector? Can the DoD support to the Defense Industrial Base services be expanded beyond the scope of National Security Memorandum 22 [20]?

- DHS now has a "National Threat Evaluation and Reporting Master Trainer Program" [22] to build national capacity in Behavioral Threat Assessment and Management (BTAM) techniques and best practices. BTAM teams follow several IC tradecraft methods (and are also championed by the U.S. Secret Service); local BTAM teams may not have direct access to law enforcement intelligence. There are BTAM teams in the private sector, including nonpublic K12 schools and higher educational institutions. This DHS program is limited to public sector employees of federal or state, local, tribal, and territorial agencies.

There are current challenges with declassifying or reclassifying intelligence to generate actionable and timely EMINT. This includes the desire for a formalized construct to potentially move EMINT from classified to controlled unclassified information (CUI) for EM use and not just be limited to law enforcement officials.

This should include the need for vetting, training, and credentialling *potential* team members from other agencies and jurisdictions and supporting the use of classified EMINT on civilian-led, domestic disaster operations.

- This will benefit a unified command. The prime example of this is the *potential* concept of operations from the USCG, which includes an intelligence/investigations branch in its Incident Command System [23] and roles for intelligence officers in steady-state operations [24].
- States and territories now utilize the Emergency Management Assistance Compact (EMAC) to coordinate resources during disasters with each other. EMAC sharing can and

U.S. Department of JUSTICE

USDOJ Strategic Plan (FYs 2022–2026)

Goal 2, Objective 2.2 Strategy 2: Strengthen Federal, State, Local, Tribal, and International Counterterrorism Partnerships

The Justice Department will protect national security by maintaining strong partnerships with law enforcement and intelligence community partners. In addition, the Department will focus on innovative intelligence analysis that supports:

- disrupting terrorist actors who threaten the United States government, its interests, or civilian populations;
- understanding the spread of violent extremist ideology;
- anticipating new and evolving terrorist threats; and
- building adaptive capabilities to counter terrorism globally.

The Department will also continue to exploit, analyze, and share intelligence with the intelligence community; state, local, and Tribal law enforcement community partners; and partner nations. And the Department will support foreign government efforts to investigate and prosecute, in their own courts, terrorists who threaten U.S. national security, through information sharing with foreign law enforcement, capacity building, and, where consistent with foreign law, the optional participation of U.S. victims of overseas terrorism in foreign justice processes.

Figure 3. DOJ Strategic Plan (FYs 2022–2026) *(Source: U.S. DOJ [21]).*

has included National Guard units [25]. The operational and tactical questions of how existing military intelligence can be shared to/from these units assigned to civilian-supported missions remain open. Even interoperable communications systems between military units and the unified command group remain a challenge.

- IMTs and incident management assistance teams are civilians who come from the staff of various states and territories and can be requested by governors to support incidents in other jurisdictions. They are specialists in intelligence, some who already have various levels of security clearances, and leadership individuals who could be prequalified to work with classified material and within a sensitive compartmented information facility [26].

LITERATURE REVIEW

Separate solutions exist today which are sector specific or limited to a single jurisdiction as previously noted; however, the primary academic resources aligned to the novel concept of EMINT are still being developed (e.g., cyber threat intelligence impacts to/from EMINT [27]). These existing policies, procedures, directives, etc., are primarily designed to provide the "guardrails" for the use of military personnel in civilian-led incidents. The Posse Comitatus Act of 1878 [28] comes to the forefront for many

The primary academic resources aligned to the novel concept of EMINT are still being developed.

people, but the use of EMINT is beyond law enforcement. There is a scarcity of detail relating to emergency management coordination with civilian authorities and toward the U.S. military's operational continuity and local continuity of government (COOP/COG), as impacted from domestic threat hazards of any kind. The following publications show existing DoD publications connecting military intelligence to civilian support:

- JP 2-0: "Joint Intelligence" has as its focus the intelligence sharing within the military but does have a section to "enable civil authority" on pp. IV–24 of the 2013 OSINT version [15].
- JP 3-28: "Defense Support of Civil Authorities" has Chapter II "Supporting a Comprehensive All Hazards Response" but does not mention intelligence [16].
- MCWP 5-10: "Marine Corps Planning Process" has examples of intelligence types and uses but no specific references to civilian support or intelligence sharing/curation. As expected, the U.S. Marine Corps (USMC) organizational structure for its civilian support is like the civilian Incident Command System Model [29].
- The USCG Incident Management Handbook 2014 [30] has a section on intelligence/investigations (pp. 4–12); however, activating that section under a unified command is not always conducted. During the Key Bridge collapse incident in 2024, neither an intelligence nor an investigations branch was initially established by the USCG [31]. This may have been due to the quick assessment that it was an accident and not an act of terrorism. However, this precludes a unified command from using these same resources and intelligence curation to support C2 and other elements of EMINT.

CASE EXAMPLES

The most prominent case of a failed "Duty to Warn" from IC elements and/or intelligence sources directly to provide EMINT to a civilian individual is related to the murder of Mr. Jamal Khashoggi [32]. There have been publicly identified successes recently, including warning Ms. Taylor Swift of a terror plot toward her in Austria in 2024 [33]. European Union countries appear to blend their national intelligence models more effectively, and there are even plans in the United Kingdom to consolidate nonmilitary intelligence capabilities and remove organizational boundaries [34].

In the healthcare and public health sectors, the CrowdStrike example with work through the DHS's Cybersecurity

and Infrastructure Security Agency (CISA) provided and sought swift and comprehensive EMINT to and from the private sector [35]. For contagions and novel vaccines, the 2024 example of the Marburg virus in Rwanda [36] and an experimental vaccine from Sabin [37] will have both current U.S. military implications/impacts, potential impacts to the U.S. Department of Health and Human Services/Administration for Strategic Preparedness and Response's Strategic National Stockpile, and subsequent distribution through military units. The reverse of this EMINT application could be from a potential civilian access to freeze-dried plasma, cryopreserved platelets, etc., from the U.S. Army Medical Materiel Development Activity (USAMMDA) [38].

For individual active assailant attacks, including the mis/disinformation campaigns of K-12 school swatting examples tracked and monitored by the FBI, there are several nexus points for cross-border threats becoming actualized hazards in the United States [39]. The alerts for these threats do not always make it past law enforcement officials to their intended targets. Unfortunately, there are also connections between the U.S. military and active assailant attacks, including the 2013 Washington Navy Yard shooting by a military contractor [40] and the 2023 Lewiston Maine shooting by an Army Reservist [41]. These attacks can also have long-term risk management and financial adverse impacts to the military [42].

Emergency management has learned and applied some lessons from the attack on the U.S. Capitol on January 6, 2021 [43]. However, there are still many open issues, including possible alternative pathways for civilian support by the various National Guard units in and around the District of Columbia [44]. CISA and other groups have bolstered EMINT distribution to the public regarding election interference from other nation states. Per U.S. Government Accountability Office (GAO) guidance for the Electoral College count event in 2025 [45], the U.S. Capitol Complex has implemented National Special Security Event protections.

Emergency management has learned and applied some lessons from the attack on the U.S. Capitol on January 6, 2021.

For GEOINT and the U.S. military's National Geospatial-Intelligence Agency (NGA) [46], there are already current inroads for EMINT sharing through the use of Homeland Infrastructure Foundation-Level Data from the Geospatial Management Office of the DHS. Could this be a conduit for more CUI GEOINT from the U.S. military? There is humanitarian assistance and disaster relief from an international/outside-the-continental-United States perspective [47]. As noted in DoD Directive 5240.01 [17], the military's ordering of NGA products and services does have detailed exceptions for humanitarian missions and support to civilian authorities during disasters.

DISCUSSION

There are two goals for this article: (1) an increased awareness of the needs and potential capabilities for actionable EMINT sharing between DoD groups and local emergency management officials to break through and bridge those silos as far and wide as needed and (2) the initiation of further discussions and debate on the changes to legacy protocols and procedures needed to implement these changes while remaining within existing U.S. laws and preserving the constitutional rights of U.S. citizens. EMINT is primarily in support of life safety. "Life, liberty, and pursuit of happiness" [48] does start with life.

Applying any of the emergency management principles without including intelligence curation to benefit emergency management missions is a formula for disaster. This must also include the **applicable** intelligence flow from the IC through domestic agencies down to the local emergency management groups who need it. Imagine if a credible threat to a specific target in the United

> ***Applying any of the emergency management principles without including intelligence curation to benefit emergency management missions is a formula for disaster.***

States were curated by the Five Eyes Intelligence Oversight and Review Council [49] and only stopped at the Office of the Director of National Intelligence. Should some EMINT elements be shared through the FBI or DHS to then move downward to the local emergency management entities who support the target?

Military Intelligence is much broader than just warfare and espionage and needed to protect members of the military within the United States. Protecting and preventing adverse life safety impacts from all threats and hazards is what EMINT supports, including protecting civilian and military responders themselves [50]. Just as the military is **not** the only curator or recipient for elements of national security intelligence, law enforcement cannot be the same for EMINT.

CONCLUSIONS

The connections between the civilian members of the IC (FBI and DHS) should be strengthened in support of CUI modalities for the curation of EMINT. The U.S. Fire Administration's Emergency Management and Response Information Sharing and Analysis Center (EMR-ISAC) and other ISACs can bridge OSINT to and from CUI through the DHS's Homeland Security Information Network (HSIN). Could HSIN be a conduit for the Homeland Defense & Security Information Analysis Center (HDIAC) and other information analysis center material now being supported through the U.S. Air Force server?

There is national value in understanding the "state of the union" when it comes to the coordination and collaboration between military and civilian units, especially as it relates to information and intelligence sharing surrounding a disaster or incident of scale. This includes active-duty federal military units who support the local jurisdictions they are physically located within and Reserve and National Guard units or groups in all the states and territories. U.S. military intelligence analysts may find historical references for EMINT usage in the Joint Lessons Learned Info System from the Defense Logistics Agency. Learning the specifics as to which military grouping does what they do now—specifically how EMINT is curated or even compartmentalized—may be a worthwhile technical inquiry (TI) for a qualified submitter to request. Examples of prior EMINT-related TIs include "Emergency Planning and Community Right-to-Know Act (EPCRA) Sections 301-303" [51] as well as the "Agricultural Security Risks" TI [52].

DoD groups like the Center for Excellence in Disaster Management and Humanitarian Assistance (CFE-DM) [53] may benefit from such a TI. While theirs is a global mandate—and typically involved DoD resources utilized by inviting other countries for humanitarian purposes, the conduits and pathways for EMINT to move from DoD to U.S.-based local emergency management can be aligned. Another candidate for a TI might be the Office of the Undersecretary of Defense for Intelligence and Security (OUSD[I&S]) [54].

In many cases, it is the preincident knowledge and networking among partners that is more beneficial than the force multipliers of staff and equipment for response and recovery missions. (The U.S. Army Corp of Engineers' "Emergency Operations" work [55] is one strong exception to this postulate.) Incorporating whole-of-government/whole-community partners into the planning, training, and exercising needed for EMINT will bridge those silos and benefit the overall DoD missions in support of civilian authorities.

As highlighted in Figure 4, there are other federal entities, as well as

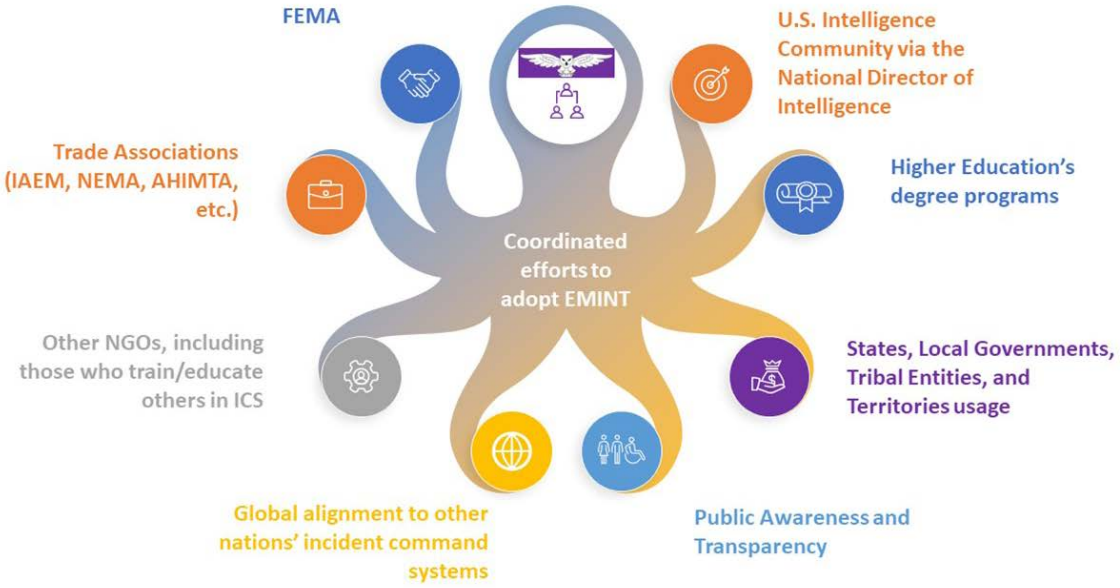


Figure 4. Other Whole Community Partners for EMINT *(Source: CEMIR [58])*.

academic, trade associations, nonprofit, and private groups, who can help craft the policies and protocols for curating EMINT beyond the various DoD groups. Examples include the EMR-ISAC group [56] from the U.S. Fire Administration, the Rand Corporation [57], the Strategic Consortium of Intelligence Professionals [58], and CEMIR [59]. ■

REFERENCES

[1] U.S. DHS. "Presidential Policy Directive/PPD-8: National Preparedness." https://www.dhs.gov/presidential-policy-directive-8-national-preparedness, 2011.

[2] U.S. DHS. "National Incident Management System - Intelligence/Investigations Function Guidance and Field Operations Guide." https://www.fema.gov/sites/default/files/2020-07/fema_nims_intelligence-investigations-function-guidance-oct-2013.pdf, October 2013.

[3] FEMA/U.S. DHS. *National Preparedness Goal*. Second edition, https://www.fema.gov/sites/default/files/2020-06/national_preparedness_goal_2nd_edition.pdf, September 2015.

[4] U.S. DOJ. "Critical Incident Review: Active Shooter at Robb Elementary School." Office of Community Oriented Policing Services, Washington, DC, https://portal.cops.usdoj.gov/resourcecenter/content.ashx/cops-r1141-pub.pdf, 2024.

[5] U.S. DoD. "DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities." DoD Directive 5240.01, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/524001p.pdf, p. 5, 2024.

[6] National Commission on Terrorist Attacks Upon the United States. "The 9/11 Commission Report." https://dpcld.defense.gov/Portals/49/Documents/Civil/911Report.pdf, 2004.

[7] Prasad, M. "Key Bridge Collapse: Unity of Effort." *Domestic Preparedness Journal*, vol. 20, no. 5, pp. 31–35, May 2024.

[8] Vincent, J., and D. Schultz. "East Palestine: Transforming Crisis Communication into Information Architecture." *CBNW Magazine*, https://nct-cbnw.com/east-palestine-transforming-crisis-communication-into-information-architecture/, 1 September 2024.

[9] National Emergency Management Agency (New Zealand). *Coordinated Incident Management System (CIMS)*. Third edition, https://www.civildefence.govt.nz/resources/coordinated-incident-management-system-cims-third-edition.

[10] CEMIR. "Examples of the Nexus to EMINT Source." https://cemir.org/, accessed on 4 November 2024.

[11] Nawaz, A. I., and I. A. Zualkernan. "The Role of Agile Practices in Disaster Management and Recovery: A Case Study." CASCON '09: Proceedings of the 2009 Conference of the Center for Advanced Studies on Collaborative Research, https://doi.org/10.1145/1723028.1723048, 2 November 2009.

[12] U.S. DHS. "Fusions Centers." https://www.dhs.gov/fusion-centers, 17 October 2022.

[13] Cruz, A. M., and M. C. Suarez-Paba. "Advances in Natech Research: An Overview." *Progress in Disaster Science*, vol. 1, p. 100013, Advances in Natech research: An overview - ScienceDirect, May 2019.

[14] Garamone, J. "Pentagon Condemns Political Violence, Details National Guard Aid to Convention." U.S. DoD, https://www.defense.gov/News/News-Stories/Article/Article/3838931/pentagon-condemns-political-violence-details-national-guard-aid-to-convention/, 15 July 2024.

[15] Joint Chiefs of Staff. JP 2-0: "Joint Intelligence." https://irp.fas.org/doddir/dod/jp2_0.pdf, Washington, DC, 22 October 2013.

[16] Joint Chiefs of Staff. JP 3-28: "Defense Support of Civil Authorities." Washington, DC, 29 October 2018.

[17] U.S. DoD. DoD Directive 5240.01: "DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities." https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/524001p.pdf, p. 11, 2024.

[18] Office of the Director of National Intelligence. Intelligence Community Directive 191: "Duty to Warn." https://www.dni.gov/files/documents/ICD/ICD-191.pdf, 21 July 2015.

[19] U.S. DOJ. "Anti-Terrorism Advisory Council." https://www.justice.gov/usao-edwi/anti-terrorism-advisory-council, accessed 5 November 2024.

[20] U.S. DoD. "DOD Support to National Security Memorandum 22." https://www.defense.gov/News/Release/Article/3766979/dod-support-to-national-security-memorandum-22/, accessed on 5 November 2024.

[21] U.S. DOJ. "FYs 2022–2026 Strategic Plan." https://www.justice.gov/file/1225821/, 11 July 2022.

[22] U.S. DHS. "National Threat Evaluation and Reporting Master Trainer Program." https://www.dhs.gov/mtp, accessed on 4 November 2024.

[23] USCG. "Incident Command System (ICS) Training Job Aid." https://homeport.uscg.mil/Lists/Content/Attachments/2922/ICS%20Training%20Job%20Aid_JAN23.pdf, January 2023.

[24] USCG. "Intelligence (CG-2)." https://www.dco.uscg.mil/Our-Organization/Intelligence-CG-2/, accessed on 5 November 2024.

[25] EMAC. "The National Guard and EMAC." https://www.emacweb.org/index.php/learn/learn-about-emac-your-discipline/national-guard, accessed on 5 November 2024.

[26] U.S. General Services Administration. "Sensitive Compartmented Information Facility Use (SCIF) Policy." https://www.gsa.gov/directives-library/sensitive-compartmented-information-facility-use-scif-policy, accessed on 5 November 2024.

[27] Prasad, M. "Cyber Threat Intelligence: A Component of Emergency Management Intelligence." *Journal of Information Warfare*, vol. 22, no. 3, https://www.jinfowar.com/journal/volume-22-issue-3/cyber-threat-intelligence-component-emergency-management-intelligence, 2023.

[28] Moore, R. H. "Posse Comitatus Revisited: The Use of the Military in Civil Law Enforcement." https://www.ojp.gov/ncjrs/virtual-library/abstracts/posse-comitatus-revisited-use-military-civil-law-enforcement, accessed on 5 November 2024.

[29] USMC. MCWP 5-10: "Marine Corps Planning Process." https://www.usmcu.edu/Portals/218/CDET/content/other/MCWP%205-10.pdf, 10 August 2020.

[30] USCG. "Incident Management Handbook." https://homeport.uscg.mil/Lists/Content/Attachments/2923/2014%20USCG%20Incident%20Management%20Handbook%20in%20English.pdf, May 2014.

[31] Prasad, M. "Key Bridge Collapse: Unity of Effort." *Domestic Preparedness Journal*, vol. 20, no. 5, pp. 31–35, May 2024.

[32] BBC. "Jamal Khashoggi: All You Need to Know About Saudi Journalist's Death." https://www.bbc.com/news/world-europe-45812399, accessed on 5 November 2024.

[33] Winter, T., A. Eckhardt, M. Burke, and R. Cohen. "Taylor Swift Concerts in Vienna Canceled After Austrian Police Say Foiled Terrorist Plot Targeted Shows." *NBC News*, https://www.nbcnews.com/news/world/taylor-swift-concert-terror-plot-austria-foiled-2-men-arrested-shows-w-rcna165591, 7 August 2024.

[34] Parker-Vincent, C., and M. S. Goodman. "Moving Towards a Secret Intelligence Joint Capability? Challenges and Opportunities of Removing Organisational Boundaries." *The RUSI Journal*, pp. 1–6, https://doi.org/10.1080/03071847.2024.2406617, 2024.

[35] U.S. DHS/CISA. "Widespread IT Outage Due to CrowdStrike Update." https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update, accessed on 5 November 2024.

[36] International Society for Infectious Diseases. "Marburg Virus Disease – Rwanda (07): Update." https://promedmail.org/promed-post/?id=20241019.8719472, accessed on 5 November 2024.

[37] Sabin Vaccine Institute. "Sabin Vaccine Institute Delivers Marburg Vaccines to Combat Outbreak in Rwanda." https://www.sabin.org/resources/sabin-vaccine-institute-delivers-marburg-vaccines-to-combat-outbreak-in-rwanda/, accessed on 5 November 2024.

[38] USAMMDA. "Blood Products and Components for our Warfighters and Military Working Dogs." https://usammda.health.mil/index.cfm/project_management/pharm/blood_products, accessed on 5 November 2024.

[39] Prasad, M. "Swatting: A Fictitious Threat Generating Real-World Hazards." *Global Network on Extremism and Technology*, https://gnet-research.org/2024/06/12/swatting-a-fictitious-threat-generating-real-world-hazards/, accessed on 5 November 2024.

[40] District of Columbia, Metropolitan Police. "MPD Navy Yard After Action Report." https://mpdc.dc.gov/publication/mpd-navy-yard-after-action-report, 11 July 2014.

[41] Neiberg, P. "Maine Mass Shooter Showed Red Flags, Army Investigation Finds." *Task and Purpose*, https://taskandpurpose.com/news/army-releases-investigation-reservist-maines-deadliest-mass-shooting/, accessed on 5 November 2024.

[42] Pezenik, S. "Maine Mass Shooting Survivors, Families of Victims File Intent to Sue Military." *ABC News*, https://abc7.com/post/survivors-families-victims-maine-mass-shooting-file-intent-sue-military/15432097/, accessed on 5 November 2024.

[43] Barton Dunant. "J6: An Independent Report on the Need for Multi-Jurisdictional Unified Command at the U.S. Capitol for National Security Special Events and Other Incidents." https://cemir.org/, 2021.

[44] Barton Dunant. "Commander-in-Chief – With One Big Asterisk." *Medium*, https://medium.com/policy-panorama/commander-in-chief-with-one-big-asterisk-242b9689b383, accessed on 5 November 2024.

[45] U.S. Government Accountability Office. "Capitol Attack: Special Event Designations Could Have Been Requested for January 6, 2021, but Not All DHS Guidance is Clear." https://www.gao.gov/products/gao-21-105255, accessed on 5 November 2024.

[46] NGA. Home page, https://www.nga.mil/, accessed on 5 November 2024.

[47] Defense Security Cooperation Agency. "Humanitarian Assistance and Disaster Relief." https://www.dsca.mil/50th-anniversary/humanitarian-assistance-and-disaster-relief, accessed on 5 November 2024.

[48] National Archives. "Declaration of Independence: A Transcription." https://www.archives.gov/founding-docs/declaration-transcript, accessed on 5 November 2024.

[49] Office of the Director of National Intelligence. "Five Eyes Intelligence Oversight and Review Council (FIORC)." https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc, accessed on 5 November 2024.

[50] Sganga, N., and K. Hoffman. "Arrest Made After Threat to FEMA in North Carolina as Hurricane Relief Operations Continue." *CBS News*, https://www.cbsnews.com/news/fema-crews-relocate-reported-threats-armed-militia-hurricane-helene-relief/, accessed on 5 November 2024.

[51] HDIAC. "Emergency Planning and Community Right-to-Know Act (EPCRA) Sections 301-303." https://hdiac.dtic.mil/technical-inquiries/notable/emergency-planning-and-community-right-to-know-act-epcra-sections-301-303/, accessed on 5 November 2024.

[52] HDIAC. "Agricultural Security Risks." https://hdiac.dtic.mil/technical-inquiries/notable/agricultural-security-risks/, accessed on 5 November 2024.

[53] CFE-DM. "About CFE-DM." https://www.cfe-dmha.org/About, accessed on 5 November 2024.

[54] OUSD(I&S). "Welcome." https://ousdi.defense.gov/, accessed on 5 November 2024.

[55] U.S. Army Corps of Engineers. "Emergency Operations." https://www.usace.army.mil/Missions/Emergency-Operations/, accessed on 4 November 2024.

[56] U.S. Fire Administration. "Critical Infrastructure Protection Emergency Management and Response – Information Sharing and Analysis Center." https://www.usfa.fema.gov/a-z/critical-infrastructure-protection.html, accessed on 4 November 2024.

[57] Rand Corporation. "Homeland Security and Public Safety." https://www.rand.org/topics/homeland-security-and-public-safety.html, accessed on 4 November 2024.

[58] Strategic Consortium of Intelligence Professionals. Home page, https://www.scip.org/, accessed on 4 November 2024.

[59] CEMIR. Home page, https://cemir.org/, accessed on 4 November 2024.

BIOGRAPHY

MICHAEL PRASAD is a certified emergency manager and president of the International Association of Emergency Managers-USA Region 2. He is the executive director of the Center for Emergency Management Intelligence Research and a national-level expert on mass care, which involves feeding and sheltering children in disasters. As a professional writer on emergency management policies and procedures, he authored the book titled "Emergency Management Threats and Hazards: Water." Mr. Prasad holds a BBA in management information systems from Ohio University and an M.A. in emergency and disaster management from American Public University.

GET PUBLISHED WITH HDIAC

If you would like to publish with HDIAC or have an idea for an article, we would love to hear from you. To learn more, visit https://hdiac.dtic.mil/publish

14,000 SUBSCRIBERS

800 ONLINE VIEWS

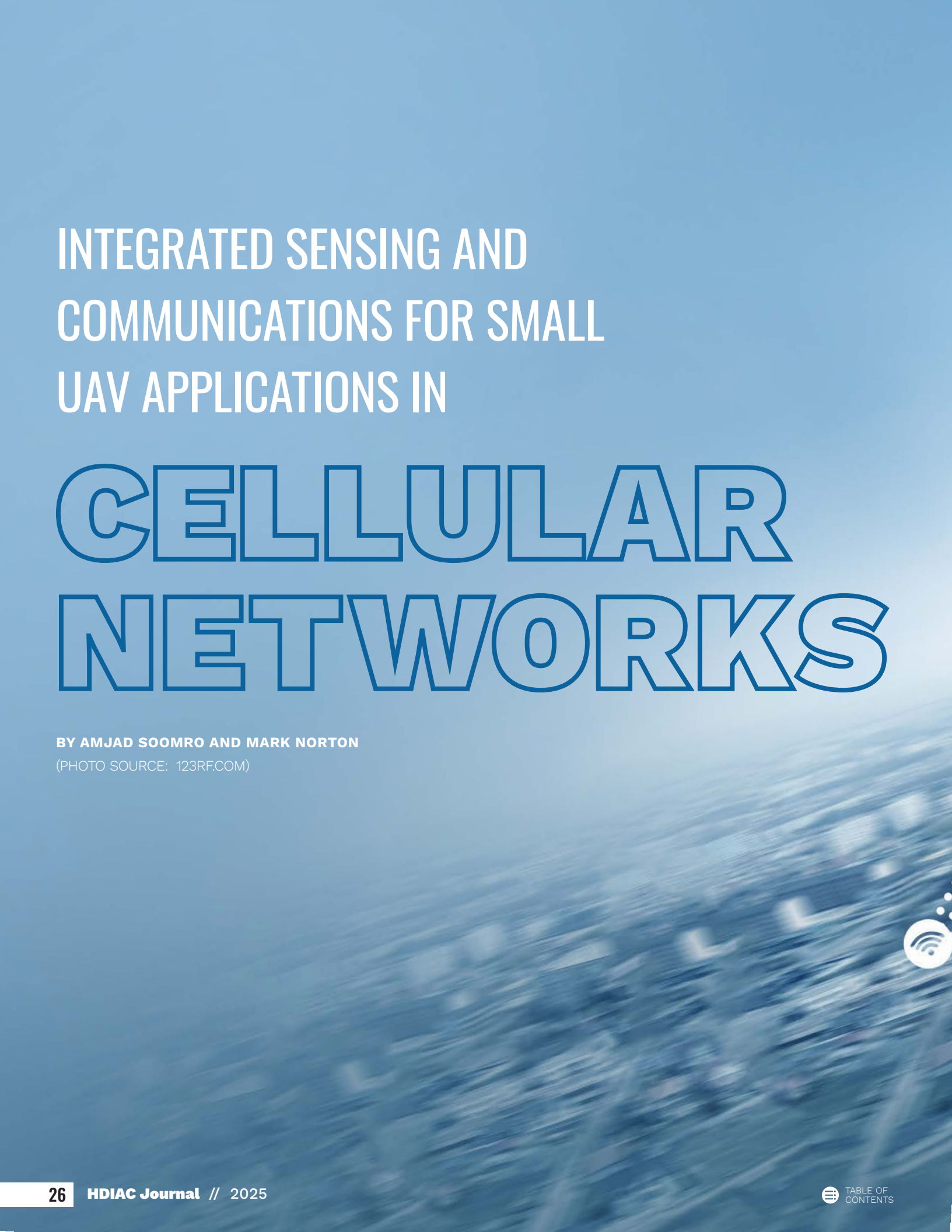
300 DOWNLOADS

The above are average statistics for each journal collected during the 2024 fiscal year. (Photo Pource: Canva)

INTEGRATED SENSING AND COMMUNICATIONS FOR SMALL UAV APPLICATIONS IN CELLULAR NETWORKS

BY AMJAD SOOMRO AND MARK NORTON

(PHOTO SOURCE: 123RF.COM)



SUMMARY

This article explores the potential integrated sensing and communication (ISAC) protocols for detecting small unmanned aerial vehicles (UAVs). The convergence of communication and sensing technologies presents a unique opportunity to enhance UAV detection capabilities, leveraging existing communication infrastructure and spectrum resources. By integrating radar sensing functionalities with communication systems, these protocols enable localization, tracking, and identification of small UAVs. The cellular communications standardization body Third Generation Partnership Project (3GPP) is considering adding these capabilities in its future standards specifications.

The underlying principles of joint sensing and communication, the specific modifications proposed in 3GPP standards, and implementation challenges are also discussed. The International Telecommunication Union (ITU) envisions ISAC use in various environments in the year 2030 and beyond. Its potential to improve security and situational awareness in homeland security and defense applications is highlighted. Adopting 3GPP integrated sensing and communication protocols is recommended to provide a cost-effective, scalable, and robust solution for small UAV detection and pave the way for future advancements in autonomous surveillance and airspace management.

INTRODUCTION

This article examines a promising area at the intersection of communication and sensing technologies, focusing on protocols designed to detect small UAVs. ISAC protocols use communication infrastructure to perform dual roles of communications and sensing based on radar principles. This approach capitalizes on existing spectrum and network resources to enhance the detection capabilities, including for small UAVs. Integrating radar sensing with communication infrastructure is expected to offer a more efficient way to localize, track, and identify small UAVs by leveraging existing communication networks, such as those outlined in cellular communication standards.

> ***Integrating radar sensing with communication infrastructure is expected to offer a more efficient way to localize, track, and identify small UAVs by leveraging existing communication networks.***

The 3GPP, a leading cellular communications standards body, is considering incorporating these protocols into future standards. These modifications would add functionalities for sensing and communication, enabling enhanced UAV detection through existing mobile networks. Some of the challenges to integrating ISAC into 3GPP standards include ensuring adequate spectrum allocation, addressing power and latency constraints, and developing modulation schemes and protocols that can handle the dual nature of communication and sensing. Also, security concerns and privacy issues, especially in civilian applications, would need consideration.

USE CASES

The broad range of use cases for ISAC technologies is introduced in this section, followed by the results of studies on their effectiveness. Then, ISAC benefits in a UAV monitoring use case are presented. Next, the relevance of an ISAC UAV monitoring use case to the U.S. Department of Defense (DoD) and Department of Homeland Security (DHS) scenarios is highlighted. Finally, select parameters of interest for generating the requirements in a homeland security use case are discussed.

Use Case Variety

ITU envisions that integrating sensing and communication into the next generation of infrastructure will enable new applications [1]. Several application scenarios have been considered, including high precision

range/velocity/angle estimation, assisted navigation, environmental monitoring for rain or pollution, human activity recognition, vehicle-to-everything communications, drone monitoring and management, smart manufacturing, and industrial Internet-of-Things (IoT) [2, 3].

The use case studies in real-world environments have been done to develop effective ISAC protocols [4, 5]. The studies show that ISAC improves situational awareness and security by utilizing communication networks to detect and track objects such as UAVs across different settings like urban and remote areas. The technology has significant potential for enhancing autonomous surveillance, airspace management, and defense operations, particularly in detecting small UAVs in restricted areas or critical infrastructures. The joint approach would provide a more scalable and robust solution compared to traditional standalone radar systems.

ISAC Benefits for UAV Monitoring

Whereas, UAV monitoring systems have traditionally used dedicated equipment and frequency bands, ISAC provides an attractive alternative. Figure 1 shows the key advantages of using ISAC in this application scenario.

DoD and DHS Specific Use Cases

Homeland security can be significantly enhanced by using upcoming ISAC technologies. Several UAV use cases have been proposed and studied that infer information from communication signals for drone detection and tracking and perform satellite-based imaging and broadcasting and drone swarm synthetic aperture radar imaging, monitoring, and management [6, 7]. The possibilities where the capabilities could be leveraged to augment and enhance homeland security are analyzed. Some specific use cases with high potential are summarized next.

> ***Homeland security can be significantly enhanced by using upcoming ISAC technologies.***

1. **Border Surveillance and Monitoring:** ISAC systems can be deployed at border locations to detect unauthorized movement while maintaining communication with patrol units. Integrated radar capabilities detect potential threats, while communication ensures secure, real-time updates to command centers.
2. **Air Defense and UAV Tracking:** In airspace monitoring, ISAC allows the same system to detect and track UAVs or other aircraft while communicating with

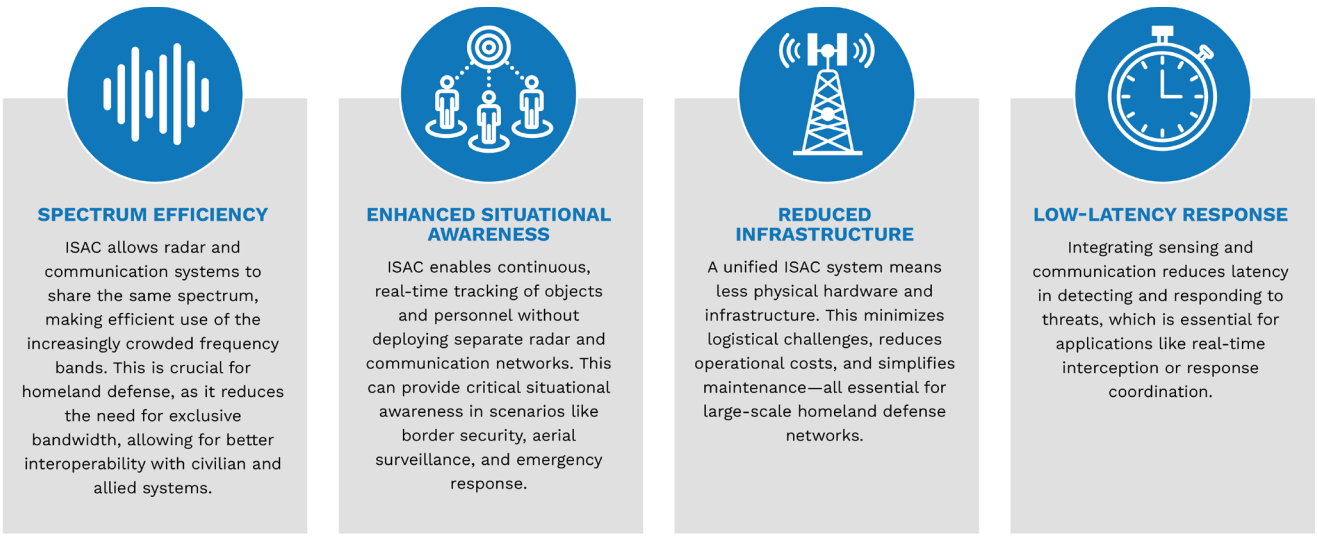


Figure 1. Advantages of Using ISAC *(Source: Canva)*.

nearby ground stations or fighter jets. This dual functionality is especially valuable in counter-drone operations. A notional counter-drone use case is depicted in Figure 2, where air defense and tracking show UAV detection. This is followed by communication with a command-and-control center, which directs air vehicles for monitoring and interception.

3. **Maritime Domain Awareness:** Coastal defense can benefit from ISAC systems on naval vessels, combining radar sensing for ship tracking with secure communication for naval operations and fleet coordination.
4. **Critical Infrastructure Protection:** ISAC can monitor the perimeter of critical sites (e.g., power plants and government facilities) and maintain communication with security teams, integrating threat detection and secure response.

Requirements

Effective UAV detection for homeland defense requires a multisensor, adaptable system that operates in real time, classifies UAVs accurately, integrates seamlessly with response mechanisms, and is designed to handle various environments and threat types. By combining radar, radio frequency (RF), electro-optical and infrared (EO/IR) cameras, and acoustic sensors with advanced processing and artificial intelligence (AI), homeland security can address the evolving threat posed by UAVs.

Salient requirement parameters of ISAC-based UAV detection in homeland security specific use cases are introduced in Tables 1–4.

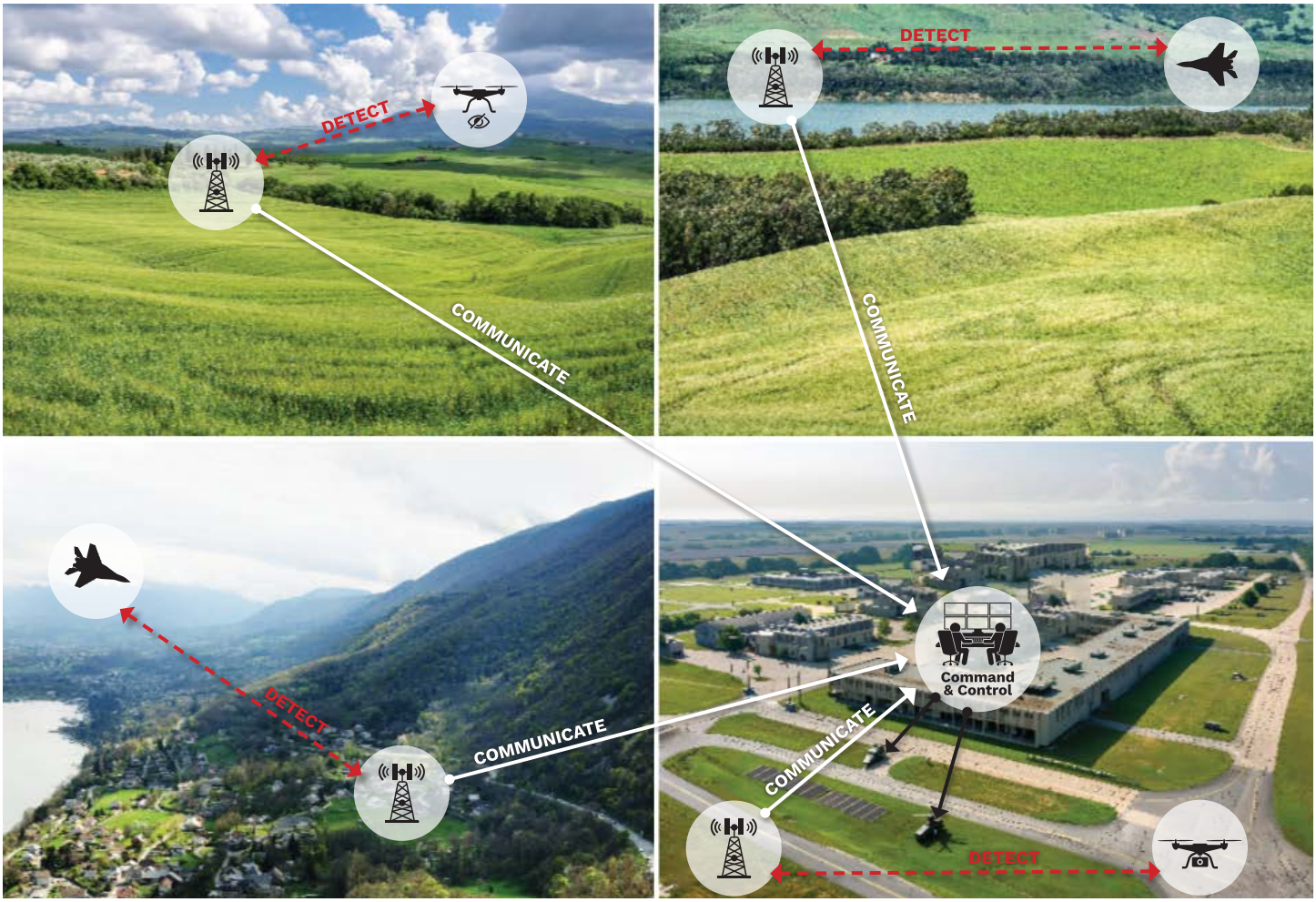


Figure 2. Notional Air Defense and UAV Tracking Use Case *(Source: A. Soomro and M. Norton).*

Table 1. Detection Range and Coverage

DETECTION RANGE AND COVERAGE	
Long-Range Detection	Systems should be able to detect UAVs from distances of several kilometers, particularly for early warning systems at sensitive locations. The detection range depends on UAV size and speed, with larger UAVs requiring longer detection ranges.
Coverage	Detection systems should ideally offer 360° horizontal coverage and sufficient vertical (elevation) coverage to handle various approach angles. Many UAVs are small and agile, making them hard to track consistently without wider coverage.
Low-Altitude Detection	Detection systems shall detect UAVs at low altitudes.
MULTISENSOR FUSION	
Radar	High-resolution radar systems should detect small, fast-moving objects at a distance. For example, radars with micro-Doppler capabilities may identify unique UAV signatures by analyzing rotor blade movement.
EO/IR Cameras	Cameras may complement radar by visually identifying UAVs, especially in low-light or night conditions. EO/IR cameras should have pan-tilt-zoom capability to track targets dynamically.
RF Detection	RF sensors should detect UAVs based on emitted signals, providing another layer of detection for active transmission. UAVs should communicate with ground controllers via specific RF frequencies.
Acoustic Sensors	The ISAC systems may complement their capability with acoustic sensors, which are particularly useful for identifying UAVs at close range or in dense environments where line of sight is limited. Microphone arrays may detect the unique acoustic signature of UAVs (e.g., the hum of rotor blades).
Passive and Active Detection	For situations where stealth is critical, passive detection techniques (e.g., RF and acoustic) may be used to reduce the risk of detection while gathering data.
Command and Control Integration	Coordination should occur with air traffic control systems such as Traffic Alert and Collision Avoidance System and Automatic Dependent Surveillance-Broadcast [8].

Table 2. Tracking and Classification Capabilities

TRACKING AND CLASSIFICATION CAPABILITIES	
Object Tracking	Detection systems should track UAVs in real time to distinguish between stationary and moving objects, including tracking flight patterns and velocities.
Classification and Identification	Classification should involve size, shape, and movement pattern analysis to confirm UAV presence. Advanced algorithms should differentiate UAVs from birds, aircraft, and other moving objects.
Automated Threat Assessment	Threat assessment software should analyze UAV flight path and behavior to determine if they pose a risk once a UAV is detected and classified. Potential threats should be flagged for human or automated response.
Micro-Doppler Analysis	Micro-Doppler may be used on small, periodic, or subtle movements within the target, such as rotating, vibrating, or oscillating parts. Micro-Doppler detects distinct frequency modulations within the radar return signals.
REAL-TIME PROCESSING AND RESPONSE	
Low-Latency Processing	Detection and tracking should be done with minimal delays for timely responses. In-phase and quadrature-phase signal processing should occur in real time, allowing immediate threat assessment and alerting.
Integration With Countermeasures	Detection systems should integrate seamlessly with counter-UAV systems, allowing for automated response (e.g., jamming and interception) when threats are detected.
Data Fusion and Centralized Control	The data from multiple sensors should be fused to provide a unified control system, thereby providing a comprehensive picture and helping operators make informed decisions in real time.

Table 3. Adaptability to Diverse Environments

ADAPTABILITY TO DIVERSE ENVIRONMENTS	
Urban Environments	Detection systems should handle dense environments and distinguish UAVs from background clutter. This is especially important in urban areas prone to high RF noise, clutter, and obstacles that affect radar and RF detection accuracy.
Rural and Open Areas	Radars should have long-range capability and include EO/IR sensors, as they are generally more effective in environments where there is less clutter. Long-range capabilities are necessary to cover larger areas.
All-Weather Operation	Systems should function reliably in all weather conditions, including rain, fog, and snow. EO/IR and radar systems should have weather-resistant capabilities, and RF detectors should be resilient to environmental interference.
COMPLIANCE AND PRIVACY CONSIDERATIONS	
Frequency Regulations	RF detection and countermeasures shall comply with local and international frequency regulations to avoid interference with legitimate communications.
Privacy Protections	Detection systems deployed in civilian areas shall comply with privacy laws, especially when recording video or collecting data on individuals.

Table 4. Operational and Maintenance Requirements

OPERATIONAL AND MAINTENANCE REQUIREMENTS	
Reliability and Low False Alarm Rate	UAV detection systems should maintain a low false positive rate to avoid unnecessary alerts, as false alarms can overwhelm operators and lead to alert fatigue.
Ease of Installation and Maintenance	Systems should be modular and easy to deploy, maintain, and upgrade. They should support regular software updates to enhance detection algorithms and adapt to evolving threats.
Interoperability With Existing Security Infrastructure	Detection systems should integrate easily with existing security networks, databases, and control systems to streamline threat detection and response coordination.
ADVANCED ANALYTICS AND AI INTEGRATION	
Machine Learning for Pattern Recognition	Machine learning may be used to improve classification accuracy by analyzing historical data and distinguishing between common UAV flight patterns and anomalous behavior.
Predictive Analytics	AI systems may be used to assess potential future movements of detected UAVs. This will assist operators in anticipating where the UAV might go and preparing appropriate countermeasures.

From a user perspective, the following four broad categories are identified:

1. Detection range and coverage
2. Tracking and classification capabilities
3. Adaptability to diverse environments
4. Operational and maintenance requirements

From a technology perspective, several configuration options and capabilities are grouped into three broad categories—multisensor fusion, real-time processing and response, and advanced analytics and AI integration. Finally, a broad category of compliance with regulatory frameworks such as privacy protections and frequency regulations is identified. Several subcategories of each category and their associated requirements are listed in the tables.

TECHNOLOGIES

Modulation Possibilities

Several modulation schemes have been proposed to address distinct requirements on joint signal design

for communications systems and sensing systems. Whereas 3GPP communications standards' focus for communications has been on spectral efficiency, interference robustness, and operation in fading channels, the performance of sensing systems is measured by target parameter estimation at high resolutions. The disparate technical requirements of sensing signal design are prepared first, and then an overview is presented of different modulation schemes researched for ISAC.

Key performance metrics to assess ISAC signals for sensing applications are resolution, Doppler sensitivity and tolerance, peak-to-average power ratio, mutual information, and data information rate. The *resolution* metric measures the effectiveness of a signal to distinguish multiple targets in space domain. The *Doppler sensitivity* metric captures the robustness of the signal to estimate the target motion, whereas *Doppler tolerance* signifies the range of the target velocity estimate within certain error bounds. The *peak-to-average power ratio* metric captures the output power amplifier's dynamic range requirements. The *mutual information* metric is a measure of the signal to carry target information in reflected echo. Finally, the *data information rate* metric measures the data information rate of the signal. The sensing signal performance metrics are summarized in Liu et al. [3] and Wei et al. [9].

Key performance metrics to assess ISAC signals for sensing applications are resolution, Doppler sensitivity and tolerance, peak-to-average power ratio, mutual information, and data information rate.

3GPP fourth generation and fifth generation (5G) signals are based on orthogonal frequency division multiplexing (OFDM). Therefore, several proposed ISAC modulation schemes are variations or modifications of the OFDM modulation scheme [9]. Though the unchanged 5G OFDM signal can be used for ISAC with acceptable performance, a high peak-to-average-power-ratio requirement to detect the original and reflected signal simultaneously opens the door to search for alternatives.

The modified OFDM modulations schemes can be placed into three classes [9]—combinations of OFDM and linear frequency modulation, combinations of OFDM and phase coding, and combinations of OFDM and spread spectrum techniques. Additionally, the following modulation schemes proposed for 5G Advanced and sixth generation (6G) 3GPP standard have been studied for ISAC applications:

1. Filter Bank Multi Carrier
2. Generalized Frequency Division Multiplexing
3. Discrete Fourier Transform – OFDM
4. Orthogonal Time Frequency Space

The modifications aim to improve sensing performance metrics while reducing impact on key communication performance metrics.

Communication Channels

Accurate channel models are needed to provide a basis to test new waveforms for ISAC applications. Whereas, sufficiently valid models exist for communication signal design, three differing ISAC application characteristics call for new models. First, the UAV objects are often moving, sometimes in clusters, which makes the RF channel vary over time and space. Second, in higher frequencies like millimeter-wave-terahertz, the channel characteristics are different. Third, ultra-massive, multiple-input multiple-output technologies at high frequencies provide needed directionality in ISAC applications for directing beams and receiving faint echoes. However, these characteristics present channel variations over space, time, and frequency in two ways—in communication literature as channel nonstationarity and consistency [10].

3GPP is considering how to develop criteria and accept validated models to

form a basis for over-the-air interface standardization. Extensive research has been reported to propose, analyze, and adopt these models in 3GPP standardization bodies [10, 11]. Due to a wide variety of ISAC application scenarios and corresponding requirements applicability, different technical aspects are prioritized to make trade-offs. Validating the models in field trials is time consuming, and more experimental data would be welcomed. However, progress is being made at a fast pace due to active interest by researchers, institutions, businesses, and standards bodies in ISAC.

Assessments

The ISAC paradox refers to the complex trade-offs between two critical functions—sensing (like radar) and communication (like data transmission)—that share the same spectrum, hardware, or operational resources. The paradox emerges because each function has inherently different requirements, and optimizing for one often degrades the performance of the other. The following five key dimensions are reviewed, wherein conflicting requirements compel tradeoffs:

1. **Spectrum Sharing:** Sensing (e.g., radar) and communications both demand large amounts of bandwidth, but they use it in fundamentally different ways. Communication systems prioritize high data rates and low latency, whereas sensing systems often require high resolution and waveforms designed to optimize the radar's ability to detect and measure target information (i.e., position, velocity, and target shape). When these systems operate on the same frequencies, interference management becomes challenging, potentially reducing the performance of both.

> ***3GPP is considering how to develop criteria and accept validated models to form a basis for over-the-air interface standardization.***

2. **Waveform Design:** ISAC requires waveforms that balance the needs of sensing and communication. Communication waveforms typically prioritize signal efficiency, such as high modulation and coding schemes, which may not be ideal for sensing applications. On the other hand, sensing waveforms are designed to extract spatial and velocity information, often requiring different pulse structures that may not carry information efficiently for communication.
3. **Power and Resource Allocation:** High power levels benefit radar sensing, as they improve detection accuracy and range. However, in a communication context, high power can cause interference and degrade the quality of service for users. Striking the right balance in power allocation for ISAC applications is difficult and can limit the performance of both functionalities.
4. **Security and Privacy Concerns:** Since ISAC systems use shared hardware and resources, securing both functions simultaneously can be difficult. Communication signals may be encrypted to prevent interception; however, such encryption can hinder their use in sensing applications, especially if low latency is needed for sensing (like in military or autonomous applications).
5. **Latency and Reliability:** Sensing may require real-time responses, especially in military or critical infrastructure contexts. Communications, while also latency-sensitive, often have more flexibility. However, when integrated, latency-sensitive sensing requirements can impact communication network design and may force compromises in data rate and reliability.

The ISAC paradox is about balancing these competing needs within a single integrated system, especially in scenarios where efficiency, real-time performance, and security are paramount—e.g., in military, autonomous, and industrial IoT applications.

ISAC implementations for UAV detection necessitate distinct optimizations in private and public networks due to differing operational goals and constraints. In private networks, such as those deployed for critical infrastructure protection, defense, or industrial facilities, UAV detection systems must prioritize high accuracy, rapid response times, and robust security to identify and mitigate potential threats in real time. These systems may leverage dedicated spectrum resources, advanced radar-like sensing integrated with 5G/6G, and localized processing to provide precise tracking and identification of UAVs in controlled environments. However, public 5G networks, which serve a wide range of consumer and commercial applications, must implement UAV detection in a way that balances scalability, cost-efficiency, and minimal interference with ongoing communications services. Public network solutions would rely on standardized protocols and shared spectrum to provide generalized UAV detection. That is, their focus would be on broad area coverage and interoperability with existing infrastructure rather than high precision or security.

ISAC implementations for UAV detection necessitate distinct optimizations in private and public networks due to differing operational goals and constraints.

CONCLUSIONS

Current research suggests that integrating ISAC protocols in 3GPP standards would lead to future innovations in autonomous UAV detection systems. These could support new forms of autonomous airspace management, offering a flexible, cost-effective solution for tracking drones in dynamic environments. The technology could be particularly relevant for defense applications, such as enhancing security around critical infrastructure and providing early warning systems for UAV intrusions. It may also facilitate advancements in autonomous air traffic management systems for civilian and military use. ■

ACKNOWLEDGMENTS

The authors are grateful to their collaborators at the DoD Chief Information Officer 5G Cross Functional Team for their invaluable input and partnership throughout this project.

REFERENCES

[1] ITU-R. "Future Technology Trends of Terrestrial International Mobile Telecommunications Systems Towards 2030 and Beyond." https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2516-2022-PDF-E.pdf, accessed on 25 March 2025.

[2] 3GPP. "TR 22.837 Feasibility Study on Integrated Sensing and Communication (Release 19)." https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4044, accessed on 19 November 2024.

[3] Liu, F., Y. Cui, C. Masouros, J. Xu, T. Xiao Han, Y. C. Eldar, and S. Buzzi. "Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond." *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1728–1767, June 2022.

[4] Jiang, W., A. Wang, Z. Wei, M. Lai, C. Pan, Z. Feng, and J. Liu. "Improve Sensing and Communication Performance of UAV via Integrated Sensing and Communication." *International Conference on Communication Technology Proceedings*, ICCT, Institute of Electrical and Electronics Engineers Inc., pp. 644–648, 2021.

[5] Yang, W., Y. Chen, N. Cardona, Y. Zhang, Z. Yu, M. Zhang, J. Li, Y. Chen, and P. Zhu. "Integrated Sensing and Communication Channel Modeling and Measurements: Requirements and Methodologies Toward 6G Standardization." *IEEE Vehicular Technology Magazine*, vol. 19, no. 2, pp. 22–30, June 2024.

[6] Cui, Y., F. Liu, X. Jing, and J. Mu. "Integrating Sensing and Communications for Ubiquitous IoT: Applications, Trends, and Challenges." *IEEE Netw.*, vol. 35, no. 5, pp. 158–167, September 2021.

[7] Bisio, I., C. Garibotto, H. Haleem, F. Lavagetto, and A. Sciarrone. *RF/WiFi-Based UAV Surveillance Systems: A Systematic Literature Review*. Elsevier B.V., 1 July 2024.

[8] Nassif, C. M. "Electronic Conspicuity: Exploring the Use of Advanced Radiofrequency Technologies to Enable Unmanned Aircraft Systems Integration." https://www. transportation.gov/sites/dot.gov/files/2025-01/Electronic-Conspicuity_White-Paper_011625.pdf, accessed on 25 March 2025.

[9] Wei, Z., H. Qu, Y. Wang, X. Yuan, H. Wu, Y. Du, K. Han, N. Zang, and Z. Feng. "Integrated Sensing and Communication Signals Toward 5G-A and 6G: A Survey." *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11068–11092, July 2023.

[10] Cheng, X., Z. Huang, and L. Bai. "Channel Nonstationarity and Consistency for beyond 5G and 6G: A Survey." *IEEE Communications Surveys and Tutorials*, vol. 24, no. 3, pp. 1634–1669, September 2022.

[11] Liu, T., K. Guan, D. He, P. Takis Mathiopoulos, K. Yu, Z. Zhong, and M. Guizani. "6G Integrated Sensing and Communications Channel Modeling: Challenges and Opportunities." *IEEE Vehicular Technology Magazine*, vol. 19, no. 2, pp. 31–40, June 2024.

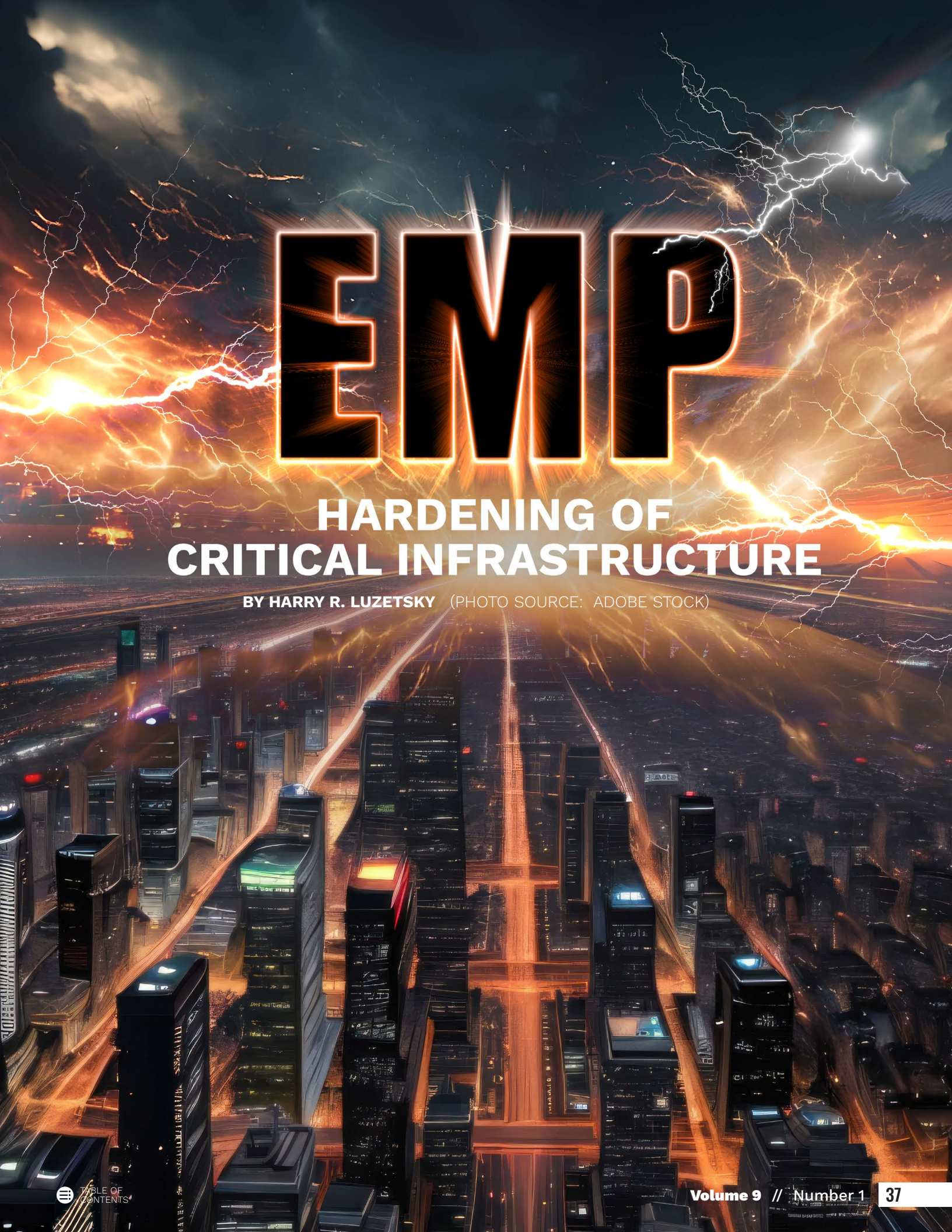
BIOGRAPHIES

AMJAD SOOMRO is a member of AMZE Technologies, a consulting firm. His research interests include wireless communications, computer communications, digital signal processing, and real-time processing. He previously worked as a senior computer engineer at the U.S. Air Force Research Laboratory, a senior member of the research staff at Philips Research, and a research and development engineer in the digital signal processing group at Hewlett Packard. He is credited with 40 granted patents and 15 publications in referred scientific journals and conferences. Dr. Soomro holds a B.S. and M.S. in electrical engineering from King Fahd University of Petroleum and Minerals and a Ph.D. in electrical engineering from the University of Maryland at College Park.

MARK NORTON serves as the chief communications engineer for Analytic Services and supports the DoD Chief Information Officer, Command, Control, Communications, and Infrastructure 5G Cross Functional Team. His focus is developing and standardizing 5G technologies through active participation in the Institute of Electrical and Electronics Engineers and 3GPP working groups. He previously held program management positions at the U.S. Army Communications-Electronics Research Development and Engineering Center, the National Reconnaissance Office, and the Defense Airborne Reconnaissance Office. Mr. Norton holds a B.S. in physics from Johns Hopkins University, an M.S. in electrical engineering from George Washington University, and an M.S. in telecommunications from George Mason University.

WANT TO READ MORE?

If you found this publication insightful and engaging, please check out our back issues on https://hdiac.dtic.mil. We also offer similar journals covering the cybersecurity and defense systems spheres, which you can find at https://csiac.dtic.mil and https://dsiac.dtic.mil.



HARDENING OF CRITICAL INFRASTRUCTURE

BY HARRY R. LUZETSKY (PHOTO SOURCE: ADOBE STOCK)

INTRODUCTION

An electromagnetic pulse (EMP) can have devastating consequences for electronic components, electrical systems, and the nation's critical infrastructure. While EMPs can be both natural and man-made, the events can damage and/or disrupt significant portions of the nation's infrastructure, including the electrical grid, communication systems, water treatment processes, electronics, and transportation systems. In addition, an EMP event can have cascading effects, initially impacting one or more infrastructure sectors, spilling over into additional sectors, and expanding beyond the initial affected geographic region due to the interconnectivity of the various infrastructure sectors throughout the national grid. Therefore, it is critical to provide adequate protection to critical infrastructure systems.

A recently developed and demonstrated composite material provides a means of providing passive protection against the deleterious effects of EMPs by providing integrated electromagnetic (EM) shielding within the composite laminate while having minimal impact on its structural characteristics. The material can be formed into various configurations that can be used to enclose critical infrastructure elements, thereby providing EM shielding and protecting their functionality. Upon implementation, this material can minimize potential damage from the components of an EMP event, resulting in an energy and communication infrastructure capable of uninterrupted operation.

> ***An electromagnetic pulse can have devastating consequences for electronic components, electrical systems, and the nation's critical infrastructure.***

EMP EVENT INFRASTRUCTURE IMPACT

An EMP is characterized as a burst of EM energy that can disrupt or damage electronic devices and systems. It can have devastating consequences for electronic components, electrical systems, and the nation. EMPs can be natural or man-made, as illustrated in Table 1. Natural occurrences of EMPs can emanate from a geomagnetic disturbance (GMD) or "space weather," lightning, electrostatic discharge (ESD), meteoric EMP, and coronal mass ejection (CME). Man-made EMPs can emanate from civilian equipment like transformer overloads, electrical circuity switching, and power line surges and military events like nuclear EMP (NEMP), nonnuclear EMP (NNEMP), high-altitude EMP (HEMP), specialized conventional munitions, and nonnuclear, directed-energy devices. Any of these EMP events can damage and/or disrupt significant portions of the nation's infrastructure, including the electrical grid, communication systems, water treatment facilities, critical electronic devices, and transportation systems.

An EMP event can have cascading effects initially impacting one or more

Table 1. EM Spectrum

THREAT	NATURAL	CIVILIAN	MILITARY
EMI/EMC	• Lightning • Electrostatic discharge • Solar flares • Auroras	• Communication (cell towers) • Generators • Power supplies • High-voltage electrical transmission lines	• Jammers • Installed electrical equipment • Radios
EMP	• Lightning EMP • ESD • Meteoric EMP • CME	• Electric circuity switching • Electric motors • Gasoline ignition systems • Continual switching of digital electric • Power line surges	• NEMP • NNEMP • HEMP
HPM	• Supernova	• High-power radars with relativistic klystron amplifier	• Backward wave oscillator • Directed energy weapon

Note: EMI = electromagnetic interference, EMC = electromagnetic compatibility, and HPM = high-power microwave.

infrastructure sectors, spilling over into additional sectors, and expanding beyond the initial affected geographic region due to the interconnectivity of the various infrastructure sectors throughout the national grid. An example of cascading effects occurred on September 2, 1859, when a storm of charged particles emanating from the Sun slammed into Earth's atmosphere, producing telegraph wire shorts and igniting widespread fires. Known as the Carrington Event, this geomagnetic storm was believed to be caused by a CME from the Sun colliding with Earth's magnetosphere. At the time, the telegraph would have been considered state of the art. Since that time, other events impacting electrical and radio systems have been recorded in 1872, 1921, 1938, 1941, 1958, 1960, 1972, and 1989. In addition, there have been other events classified as near misses. Some of the more significant events since the Carrington event occurred in 1921 and 1989.

In 1921, a three-day geomagnetic storm, named the New York Railroad Storm, was caused by the impact of an extraordinarily powerful coronal mass ejection on Earth's magnetosphere [1]. This storm has been classified as the most intense geomagnetic storm of the 20th century. The result of its electrical current initiated fires worldwide, including one near Grand Central Terminal New York, hence the name "New York Railroad Superstorm." Undersea telegraph cables were adversely affected as well as telegraph systems across Europe and the southern hemisphere.

In 1989, a geomagnetic storm emanating from severe solar storms produced a 9-hr outage of Hydro-Québec's electricity transmission system [2]. Additional storms during the same year resulted in communication blackouts; loss of control of some satellites in polar orbits; communication interruptions with the Geostationary Operational Environmental Satellite, resulting in anomalous images; and the Space Shuttle Discovery, which was aloft at the time and experienced sensor malfunctions that resolved when the solar storm subsided.

In 1989, a geomagnetic storm emanating from severe solar storms produced a 9-hr outage of Hydro-Québec's electricity transmission system.

These examples demonstrate that even though there have been technology improvements in electronics and electrical systems, they remain vulnerable to effects from an EMP. Due to the greater reliance on advanced electronics and associated electrical systems with a sensitivity to EM radiation and power surges, the impact of an EMP event can be devastating to the nation's electrical infrastructure.

To combat the deleterious effect of EMPs on the nation's infrastructure, it is necessary to develop the tools and techniques necessary to mitigate the effects to infrastructure from any event that produces an EMP. Once implemented, these tools and techniques would minimize potential damage from the various components of an EMP event and result in an energy and communication infrastructure capable of uninterrupted operation. Without the appropriate tools, the nation's infrastructure is at risk of being severely damaged, potentially irrevocably, compromising its ability to respond to the source of the EMP event and recover from it.

EMP DESCRIPTION

On March 26, 2019, presidential executive order (EO) 13865, "Coordinating National Resilience to Electromagnetic Pulses," was signed that directs action in five areas to reduce the risk that EMPs pose to U.S. critical technology and infrastructure systems [3]. These five areas included the following:

1. Identify national critical functions and associated priority critical infrastructure at greatest risk from EMPs.
2. Improve understanding of EMP effects.

3. Evaluate approaches to mitigate the effects of EMPs.
4. Strengthen critical infrastructure to withstand the effects of EMPs.
5. Improve national response to EMP events.

This EO was based on the "Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment" report dated February 5, 2019 [4]. The report was a collaborative effort between the Department of Homeland Security Science and Technology Directorate, the Federal Emergency Management Agency Integrated Public Alert and Warning System Program, and the Cybersecurity and Infrastructure Security Agency. It summarizes recommendations that federal, state, and local agencies and private sector critical infrastructure owners and operators can employ to protect against the effects of an EMP event.

To provide protection against an EMP event, it is necessary to understand the EM environment and parameters necessary to mitigate effects from the event. Elements of the EM spectrum are provided in Table 1, where EMP is a major player. The EM threats identified in the table are frequency dependent and require differing shielding levels, as identified in Table 2. Of the three threats, the Air Force Global Stike Command (AFGSC) has recognized the need to create a robust and resilient nation that is well prepared to face EMP threats, protecting its citizens, critical infrastructure, and military capabilities [5].

Table 2. Frequency and Shielding Ranges for EM Threats

THREAT TYPE	FREQUENCY RANGE	EM SHIELDING RANGE
EMI/EMC	9 kHz – 40 GHz	60 – 100 dB
EMP	100 MHz – 100 GHz	80 – 120 dB
HPM	1 GHz – 35 GHz	100 – 140 dB

To provide protection against an EMP event, it is necessary to understand the EM environment and parameters necessary to mitigate effects from the event.

An EMP event can be challenging for electronics and electrical systems. An EMP on unprotected systems can produce upsets, hard failures, and power surges that can damage electrical and communication networks. Present systems typically have minimal protection to address low levels of EM radiation. This protects against EMI while allowing EMC with EM radiating systems like communication systems (i.e., cell towers), generators, power supplies, and high-voltage electrical lines.

EMI is the interference caused by an EM disturbance affecting the performance of a device or system which can emanate from natural and man-made sources. Natural sources of EMI include electrostatic discharge, electrical storms, solar flares, and auroras, while man-made sources include communication systems (i.e., cell towers), generators, power supplies, and high-voltage electrical lines. While natural sources may be rare and even sporadic, man-made sources of EMI are prolific in the operating environment. When insufficient protection is present, EMI often manifests itself as undesirable noise that may disrupt the proper operation of electrical, electronic, and radio frequency (RF)-dependent systems.

There are four types of EMI—conducted, common mode, differential mode, and radiated. Conducted EMI requires direct contact with a source of EMI and flows through the wires of the system. Common and differential modes define high-frequency and low-frequency EMI, respectively, flowing through conductors or adjacent wires. Radiated EMI is the most common form that results from radiating EM fields, with the most common form appearing as static noise on radio receivers and snow on TV monitors.

EMC represents the ability of a system to operate in the presence of EM radiation and the ability not to generate EM radiation that can impact other nearby operating systems.

EMI/EMC frequency range is 9 kHz to 40 GHz. The shielding required to provide adequate protection is between 60 and 100 dB, as indicated in Table 2. While there is some overlapping between EMI/EMC and EMP, an EMP event affects a greater frequency range and can require greater shielding protection to provide shielding for the event. An EMP event is a form of EMI; however, it is referred to as a transient electromagnetic disturbance, characterized by a pulse of brief, high-intensity EM radiation. While there are various sources of an EMP, the most common is a GMD, whereas the most severe is associated with HEMP. As such, the parameters associated with HEMP are used to define the guidelines to provide protection for an EMP event.

As illustrated in Figure 1, there are three components associated with a HEMP event, according to the International Electrotechnical Commission [6]. They are designated as E1, E2, and E3.

E1 results when gamma radiation from the nuclear event ionizes atoms in the upper atmosphere and consists of a fast, large amplitude pulse, with frequency content in the hundreds of megahertz uncommon

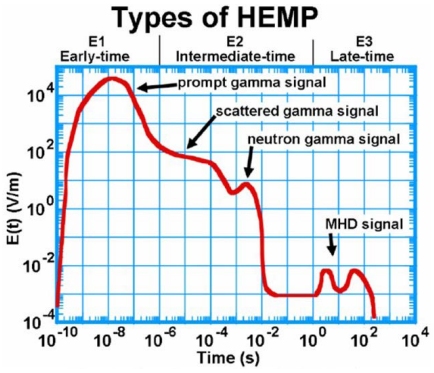


Figure 1. Types of HEMP *(Source: Radasky and Savage [6]).*

for a natural-occurring EMP event like from a GMD. The damage resulting from E1 causes conductive objects like control cables and power lines to behave as antennae and absorb the RF pulse. Referred to as the conductive threat, the E1 field couples to overhead lines, control cables, etc., and generates conducted voltage and current transients that adversely affect connected equipment. In addition to the conductive threat, there is a radiated threat which occurs when the E1 field couples directly with equipment-inducing voltages and current transients at the circuit board level, resulting in device upset or damage. Figure 2 illustrates the differences between the conducted and radiated threats associated with the E1 waveform [7].

The brief but intense field from E1 induces high voltage in electrical conductors, causing most of the damage through excessive electrical breakdown voltages. This single component of a HEMP can damage or disrupt electronic devices, communication systems, and control and acquisition systems. Since it changes in nanoseconds, ordinary surge protectors cannot react in an expeditious manner to provide protection. In addition, the resulting voltage surges can also cause insulation flashover of distribution-class insulators and transformers.

E2 is a lower intensity event occurring over a greater time through producing gamma rays and gammas from inelastic neutron scattering. The time pulse is intermediate, occurring from approximately 1 μs to 1 s after event initiation (i.e., explosion). The E2 aspect of the HEMP event patterns the profile associated with lightning

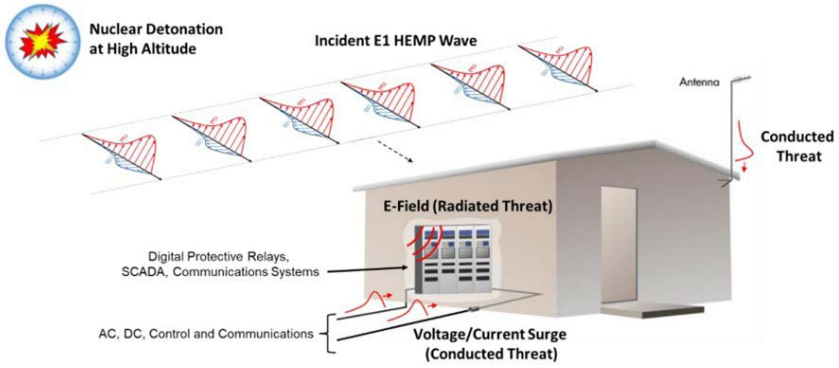


Figure 2. Example of Radiated and Coupled Threat Associated With E1 *(Source: U.S. Department of Energy [7]).*

having a lower energy-induced E2 (as illustrated in Figure 3), which overlays lightning with the pulse associated with HEMP.

The main threat with E2 is that since it follows E1, it can produce damage to devices that would normally be protected against E2 but have been compromised from the E1 pulse. Like lightning strikes, EM fields from the E2 pulse couple through the air to overhead lines and cables, posing a threat from both radiated and conductive EMI. Since the amplitude is generally less than that associated with lightning, transmission voltage and distribution systems may have adequate lightning protection. However, some systems have less protection than others, particularly in areas that experience less lightning phenomenon than others or when protection is considered a significant cost element.

E3 differs from both E1 and E2, with a lower pulse intensity occurring over a longer time. This component of HEMP produces a geomagnetically induced current in transmission lines and bulk transformers with grounded Y-type windings. The result can be magnetic saturation that causes harmonic currents and absorbs significant quantities of reactive power, leading to hotspot heating in windings and structural components. This can translate to direct impacts to the electric power grid and result in voltage collapse (regional blackout), protective equipment failure from harmonics, and transformer damage due to heating above from the design. In addition, certain sensitive electronics may also be prone to damage or disruption from harmonic voltage distortion transferred from the voltage transmission system to medium- and low-voltage systems.

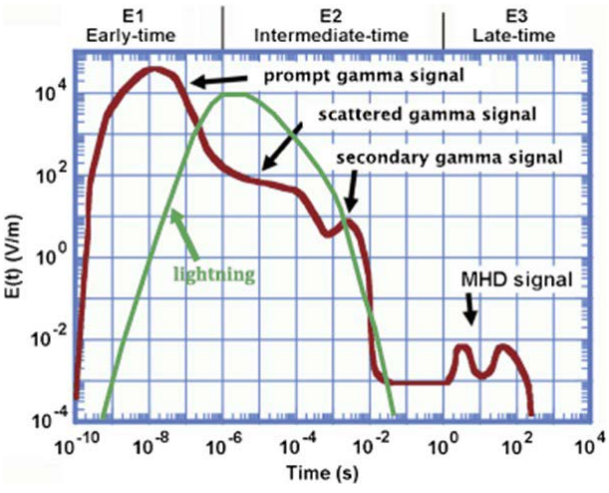


Figure 3. Types of High-Altitude EMPs With Lightning Overlay *(Source: Gombosi et al. [8])*.

EMP MITIGATION AND PROTECTION

Protecting elements of the infrastructure from the effects of EMP requires addressing the three pulse elements (E1, E2, and E3) associated with a HEMP event. With this approach, most of the main effects associated with an EMP are mitigated. Methods to protect against the effects of EMP require a layered approach comprised of four distinctive layers: (1) isolation, (2) EMP/HEMP filtering, (3) surge protection, and (4) EM shielding [9].

Isolation

This is the most assured method for protecting against EMP; however, it is the least practical in totality for various aspects of the U.S. infrastructure. For isolation to be totally effective, the isolating structure must be sized sufficiently to shield EM radiation and be free of penetrations or cabling passthroughs that result in point of EM entrance, either directly or through traversing conductive cabling like power lines. Essentially, the structure acts like a giant all-encompassing faraday cage. Many aspects of the electrical infrastructure cannot take advantage of isolation, such as transformers, power stations, communication hubs, computing systems that utilize the internet, and satellite links. However, where possible, isolation can be used to

> ***Many aspects of the electrical infrastructure cannot take advantage of isolation, such as transformers, power stations, communication hubs, computing systems that utilize the internet, and satellite links.***

reduce some of the EMP magnitude-lessening impact on infrastructure elements.

EMP/HEMP Filtering

This is a device that is placed in line with the power line designed to suppress HEMP waveforms in the power line. The operating feature of an EMP/HEMP filter is a suppression circuit exhibiting a high off-state impedance during its normal operation, which is transparent to circuits further down the line from the filter. In case of a voltage overshoot exceeding the filter-switching voltage, the filter suppression circuitry switches to a very low-impedance, high-attenuation mode that shorts out the excessive voltage and absorbs the excess energy. During the duration of the high-voltage event, the EMP/HEMP filter maintains suppression until a voltage drop decreases to a level below the switching voltage deemed to be safe [10].

It is important to distinguish EMP/HEMP filtering over EMI/EMC filters typically used for commercial applications. While protection is afforded by some EMI/EMC filters for the waveforms associated with E1, E2, and E3 phases of an EMP/HEMP event, they cannot defend against the power levels and fast transients associated with E1 and E2 waveforms. In addition, the EMI/EMC filters typically do not have the ability to provide adequate suppression over 80 dB of attenuation from 10 MHz to 10 GHz [10]. EMP/HEMP filtering is designed to focus on the E1 power levels and fast transient associated with the E1 phase of the EMP/HEMP event, while surge protection can be used to address the E2 phase, as the power and transient levels mirror that associated with a lightning event.

Surge Protection

As illustrated in Figure 2, while the E2 phase of an EMP/HEMP event results from radiation interactions with the atmosphere, its waveform, power levels, and time transients closely resemble the effects associated with lightning. Although the induction effects are different than a direct lightning strike on power lines or electrical systems, the use of adequately sized surge protectors can mitigate the impact to electrical systems as well as those systems downstream from a power surge, such as that from a direct lightning strike. Surge protectors utilize grounding wires to divert power levels that exceed the design level to the suppressor's grounding wire. The actual method of execution differs with various arrestor designs, but the premise is the same. Suppressors use two basic circuit designs—a parallel design and a series design. The parallel design diverts excess electricity away from the standard path to another circuit, while a series design does not shunt excess electricity away from the standard path but retards its progress through the hot line. In a series design, excess voltage is detected, stored, and gradually released. It is argued that the series design reacts more quickly and does not direct the excess to the ground line, thereby potentially upsetting or disrupting the electrical system feeding the components impacted.

As a backup to surge protectors, built-in fuses are often used. Once the current exceeds a specified level, the resulting heat burns the fuse breaking the circuit and curtailing continued movement of the power surge through the line to the protected equipment. The fuse works once, and while the functionality of the protected equipment is spared, the operation is disrupted until fuses are replaced.

EM Shielding

This addresses all three phases of the EMP/HEMP event (E1, E2, and E3) by blocking EM radiation across all frequencies regardless of power levels and transient times when

properly designed. EM shielding provides passive protection against direct absorption effects of EM waves for equipment and power systems enclosed by the shielding. Various materials with different weights, sizes, and costs are available, as well as the various levels of protection afforded by the materials. Considering other protection features, the level of protection can be sized to the electrical systems and protected equipment. In some instances, shielding may be designed to reduce the EM radiation to a level that can be easily handled by other techniques like EMP/HEMP filters and surge protectors. EM shielding can be integrated into new construction and retrofitted to existing structures.

The common shielding methodology involves constructing boxes or enclosures for electronic systems that require protection with highly conductive metallic materials. When properly sized from a thickness perspective, these systems can yield EM shielding levels across the entire frequency spectrum of 90 dB, with peaks above 120 dB and an approximate average of 100 dB (as shown in Table 2). The most common material for these enclosures is copper; however, aluminum and steel are also used. More exotic metals are employed when magnetic effects are of concern. Large structure like buildings can be shielded with metal sheeting, foils, conductive paint, and conductive concrete (emerging technology). When considering the shielding methodology, weight and cost implications must be considered.

Emerging technologies explore the application of nonmetallic materials, especially composites [11]. These technologies offer a lower weight alternative to metallic structures and a versatility to customize the shielding for various structure configurations. Figure 4 illustrates some of these advancements, but their performance is typically less than that realized by metallic structures.

A recently developed multifunctional composite material has been developed with EM shielding properties like that associated with a 1/8-in-thick aluminum enclosure box, as shown in Figure 5. The material exhibited EM shielding effectiveness levels across all frequencies of the EM spectrum, exceeding those levels of other existing composite materials (see Figure 4), and a shielding effectiveness comparable to an aluminum enclosure [12]. When compared to an identically sized enclosure, the developed composite material achieved a comparable EM shielding level at a weight ~24% of that of the aluminum (1/8-in-thick) enclosure.

Finally, grounding, also known as earthing, is necessary to provide a safe path for excess electricity to escape

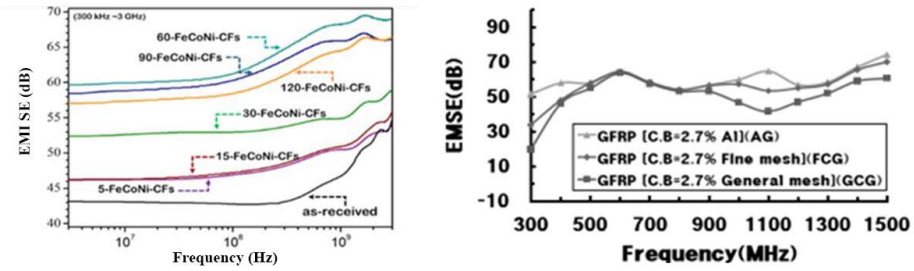


Figure 4. EM Shielding Effectiveness of Different Materials *(Source: Piner et al. [11])*.

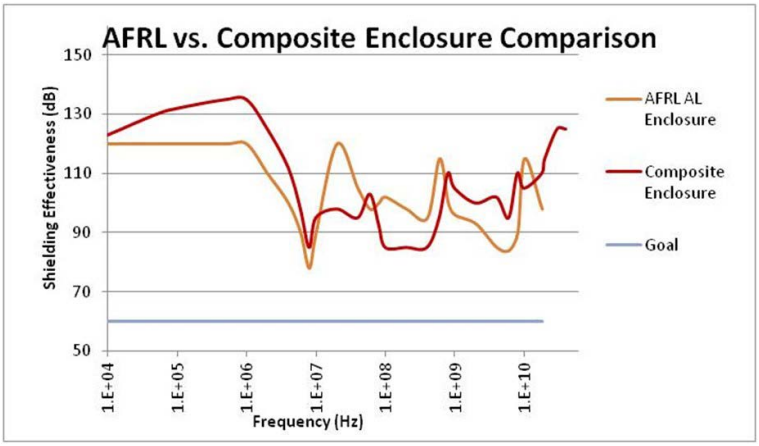


Figure 5. Shielding Effectiveness of Multifunctional Composite and Aluminum Enclosures *(Source: Luzetsky et al. [12])*.

to the ground. Without grounding, electricity can build up in the wires or electrical devices and cause irreparable damage.

CONCLUSIONS

EMP protection, from natural and man-made events, is critical for the electrical infrastructure in the United States. Historically, past events have shown that a GMD can and has disabled electrical systems regionally and globally. With the greater proliferation and reliance on electrical systems, the impact on the infrastructure can have cascading effects that disable water systems, shut down the electrical grid and computing systems, disrupt communications, and result in societal unrest.

Fortunately, there are techniques to mitigate the effects, and the government recognizes the problem; however, implementation has been slow to affect appropriate modifications. While there is significant work being done to develop advanced EMP shielding techniques, this work has largely centered on the military aircraft industry. There has been an increased interest in transferring this technology to the country's electrical and electronic infrastructure. This increased interest is evidenced by the involvement and directives from the AFGSC for EM protection of the country's infrastructure and by the release of Small Business Innovation Research (SBIR) AF233-0036 titled "Commercial Technologies for EMP Hardening and Electrical System Protection" [13], which highlights EMP protection technology. ■

While there is significant work being done to develop advanced EMP shielding techniques, this work has largely centered on the military aircraft industry.

REFERENCES

[1] Phillips, T. "The Great Geomagnetic Storm of May 1921." Spaceweather.com, 12 May 2020.

[2] Boteler, D. H. "A 21st Century View of the March 1989 Magnetic Storm." *Space Weather, AGU* (*Advancing Earth and Space Sciences*), vol. 17, issue 10, pp. 1427–1441, 10 October 2019.

[3] Federal Register. Presidential EO 13865 - "Coordinating National Resilience to Electromagnetic Pulses." Executive Office of the President, *The Daily Journal of the Federal Government* (*National Archives*), vol. 84, no. 61, 29 March 2019.

[4] National Coordinating Center for Communications. "Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment." Version 2.2, National Cybersecurity and Communications Integration Center, Arlington, VA, 5 February 2019.

[5] U.S. Department of the Air Force. Instruction 10-2601 - "Electromagnetic Pulse Survivability Program," p. 29, 11 January 2022.

[6] Radasky, W., and E. Savage. "High-Frequency Protection Concepts for the Electric Power Grid." Meta-R-234, Metatech Corporation, prepared for Oak Ridge National Laboratory, January 2010.

[7] U.S. Department of Energy. "High-Altitude Electromagnetic Pulse Waveform Application Guide." CESER Technical Analysis Report, Office of Cybersecurity, Energy Security, and Emergency Response, July 2023.

[8] Gombosi, T. I., D. N. Baker, A. Balogh, P. J. Erickson, J. D. Huba, and L. J. Lanzerotti. "Anthropogenic Space Weather." *Space Science Review*, 24 March 2017.

[9] The National Institute of Building Sciences. "High Altitude Electromagnetic Pulse (HEMP) Effects and Protection." Whole Building Design Guide (WBDG), https://www.wbdg.org/resources/high-altitude-emp-effects-protection, accessed on 17 November 2024.

[10] API Technologies Corp. "EMP/HEMP Filters: New Electronics Assembly Level Solution in the Battle Against Intentional EMI and Electronic Warfare." EMP/HEMP Filters: New Electronics Assembly-Level Solution in the Battle Against Intentional EMI and Electronic Warfare, accessed on 4 November 2024.

[11] Piner, R., D. Motes, and T. Kneen. "Development of EMI Shielding Capabilities of Fiber Reinforced Composites." DSIAC Technical Inquiry (TI) Response Report, February 2022.

[12] Luzetsky, H. R., M. Klein, and G. Ostrander. "Multifunctional Structural Composite With Integrated Electromagnetic Shielding." Vertical Flight Society 73rd Annual Forum and Technology Display Conference, Multifunctional Structural Composite with Integrated Electromagnetic Shielding, 8 May 2017.

[13] U.S. Department of Defense. "Commercial Technologies for EMP Hardening and Electrical System Protection." SBIR AF233-0036, 2023.

BIOGRAPHY

HARRY R. ("RICK") LUZETSKY is a subject matter expert in composites and survivability at SURVICE Engineering Company's Aberdeen Research Organization – Research and Analysis Group. He currently supports the U.S. Army Evaluation Center in the survivability assessment of military platforms and has been involved in developing a ballistic-tolerant composite drive shaft, armored actuators, a thermoplastic tail cone, and a multifunctional composite material with structural and integrated EM shielding capabilities for military platform structures. He has over 40 years of experience with vertical lift aircraft, specializing in composite materials and survivability technology enhancements to improve platform performance. He holds two autonomous, self-sealing, fuel bladder patents. Mr. Luzetsky holds a B.S. in materials engineering from Drexel University.

In-Flight UV-C Disinfection After COVID-19

BY K. M. BELLAND AND C. A. DEJOHN (PHOTO SOURCE: ADOBE STOCK)

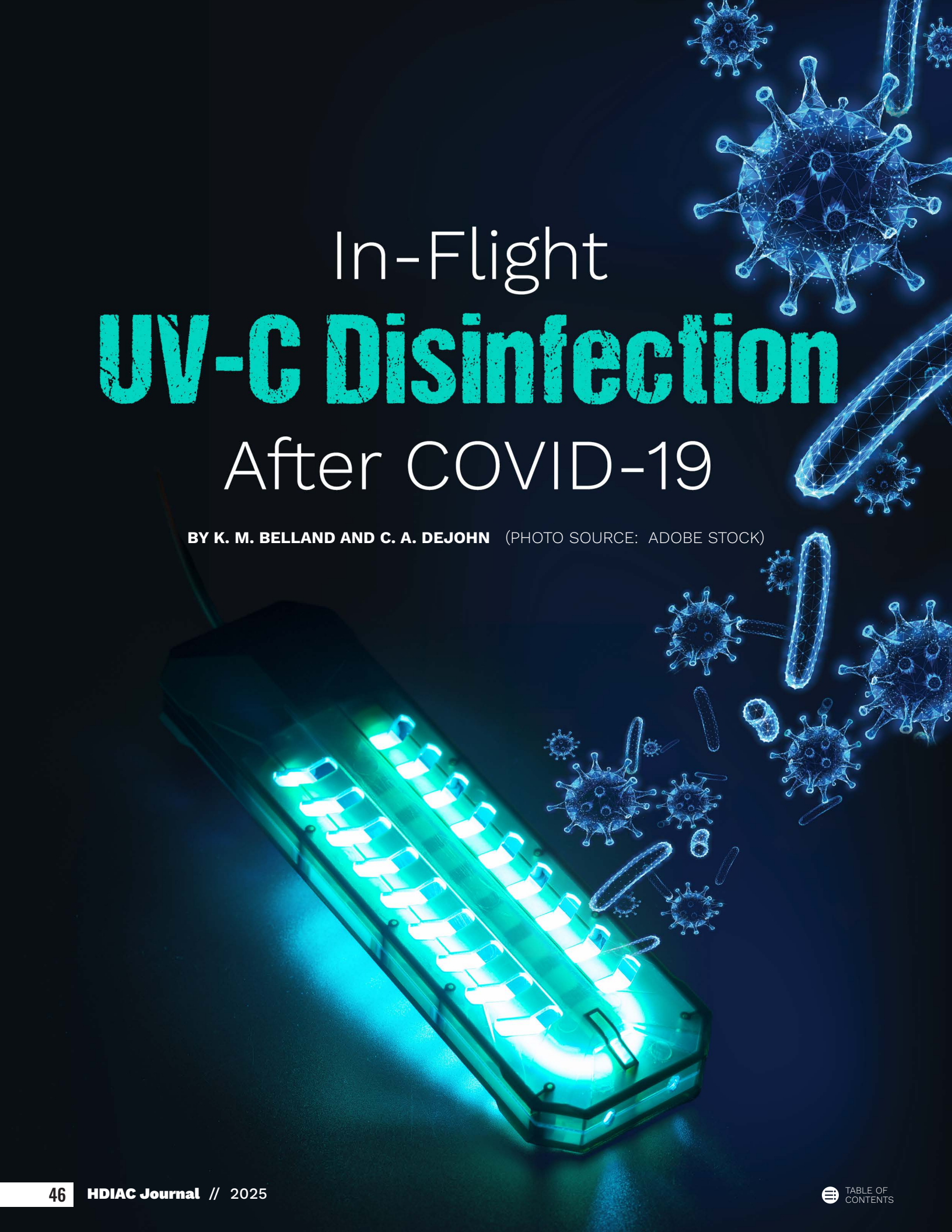


TABLE OF CONTENTS

PROBLEM STATEMENT

Although rare, aircraft cabins have been associated with disease transmission, including severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and influenza A. A recent risk-benefit analysis estimates that such transmissions have led to up to 10,000 deaths annually (from 2020 to 2023) and a $200 billion economic burden. Ultraviolet-C (UV-C) air disinfection could mitigate up to 80% of these impacts, enhancing passenger safety and reducing transmission [1–4].

INTRODUCTION

The aviation industry seeks effective cabin disinfection strategies, with UV-C offering a chemical-free solution to reduce disease transmission. This article examines UV-C's effectiveness, safety, risks, benefits, and regulatory considerations compared to other methods.

> ***The aviation industry seeks effective cabin disinfection strategies, with UV-C offering a chemical-free solution to reduce disease transmission.***

LITERATURE REVIEW

Researchers have become increasingly intrigued by UV-C disinfection as a tool to reduce the spread of infectious agents, both on surfaces and in the air. Existing studies point to UV-C's ability to lower infection rates, cut healthcare costs, and keep workforces healthy. Questions remain about its overall safety, cost-effectiveness, and best-use scenarios. In the sections that follow, UV-C technology's strengths and weaknesses will be explored.

Historical Background on UV-C Disinfection

Researchers recognized the impact of light on microorganisms as early as 1845, with a breakthrough in 1877 showing sunlight inhibited microorganism growth in Pasteur's solution. Studies later found shorter wavelengths to be most effective. In 1933, the concept of airborne infection via droplet nuclei emerged, and by 1935, experiments confirmed ultraviolet germicidal irradiation (UVGI) deactivated airborne microorganisms. The 1960s and 1970s saw the introduction of upper-room UVGI, followed by extensive efforts in the 1990s to evaluate its efficacy and safety [5].

UV-C light has long been used for water treatment and air purification, including during World War II for disinfecting hospitals and military facilities. Advancements in the 1950s boosted its accessibility, leading to its widespread adoption today for decontamination. Far-UVC light shows potential for safely inactivating airborne pathogens in occupied spaces [6–8]. UV-C supplements other disinfection methods by neutralizing bacteria, viruses, and pathogens [9, 10]. During the coronavirus disease 2019 (COVID-19) pandemic, UV technologies were crucial for decontaminating personal protective equipment and reducing pathogens on aircraft surfaces [9, 11].

UV-C Disinfection in Aviation

The aviation industry's interest in UV-C disinfection emerged recently to address disease transmission and translocation risks in aircraft. The SARS outbreak, H1N1 (swine flu) pandemic, and COVID-19 pandemic underscored the vulnerability of enclosed spaces like aircraft cabins. These events led to exploring UV-C as a supplementary disinfection method with manual cleaning and high-efficiency particulate air (HEPA) filtration. The United Nations International Civil Aviation Organization (ICAO) and Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation applied the James Reason Swiss Cheese Model for layered risk mitigation during the COVID-19 pandemic. UV-C proved highly effective against bacteria, viruses, and spores, enhancing air quality and surface disinfection [1].

There is increasing interest in using continuous UV light during flights instead of episodic disinfection between flights. UV-C light can reduce airborne transmission risk in aircraft cabins by up to 90% by targeting pathogens in the air. Using Direct Irradiation Below the Exposure Level (DIBEL) technology enables safe inactivation of pathogens in occupied cabins during flight [3, 12].

> ***UV-C light can reduce airborne transmission risk in aircraft cabins by up to 90% by targeting pathogens in the air.***

Comparative Analysis of Disinfection Methods

Several disinfection methods are used in aircraft, each with strengths and limitations. These methods are as follows:

- **Manual Cleaning and Chemical Disinfection:** Manual cleaning with chemical disinfectants effectively reduces surface contamination but has limitations, including variability in thoroughness, recontamination risks, and potential environmental and toxic effects [1, 4]. Additionally, proper contact or "dwell time" is crucial for efficacy, as insufficient contact time can leave pathogens behind and potentially spread infections.
- **HEPA Filtration:** HEPA filters, common in commercial aircraft, effectively capture particles 0.3 μm or larger, including submicron viruses like SARS-CoV-2 [13]. However, their efficiency depends on airflow, leaving areas of reduced circulation like near seats and aisles at higher risk [1, 3, 14]. HEPA filters do not address surface contamination and are less effective for particles around 0.15 μm, a size linked to SARS-CoV-2 [13]. Studies confirm that airborne transmission risks persist even with the use of HEPA filtration systems [14].

To address these concerns, UV-C technology has emerged as an essential tool for enhancing air quality and infection control, aligning with the American Society of Heating Refrigeration and Airconditioning Engineers (ASHRAE) standards that emphasize maintaining safe and healthy indoor environments. ASHRAE recognizes the effectiveness of UV-C disinfection in reducing airborne pathogens, particularly when integrated into HVAC systems [13]. UV-C systems are frequently employed to sanitize components of air-handling units, effectively preventing microbial growth that can degrade air quality. The implementation of UV-C technology supports ASHRAE's commitment to improving ventilation, filtration, and air cleaning, thereby mitigating the spread of infectious diseases. This proven, energy-efficient solution complements other mechanical ventilation strategies, offering a robust approach to maintaining healthier indoor environments [13].

- **UV-C Disinfection:** UV-C light provides several advantages over traditional methods, including rapid, residue-free disinfection of airborne and surface pathogens. It can be automated to reduce human error and sanitize aircraft cabins in minutes, improving efficiency. For example, SARS and influenza A can be 90% inactivated within 15 minutes in occupied cabins [4]. Combined with HEPA filtration, UV-C ensures continuous in-flight air and surface disinfection, addressing risks from infected passengers boarding post-cleaning [1, 4].

Unlike vaccines, which require time to develop and adapt to mutations, UV-C light acts immediately and is effective against a broad spectrum of viruses, including many known human pathogens, by damaging their genetic material (DNA or RNA). While UV-C light is highly effective, viruses like those causing diseases such as COVID-19 can mutate over time. These mutations may alter the virus's structure, potentially impacting the efficacy of UV-C in inactivating them, although UV-C's broad mechanism of action generally limits this risk.

> ***Unlike vaccines, which require time to develop and adapt to mutations, UV-C light acts immediately and is effective against a broad spectrum of viruses, including many known human pathogens, by damaging their genetic material.***

EFFECTIVENESS OF UV-C IN PATHOGEN INACTIVATION

UV-C light effectively inactivates microorganisms by damaging their DNA or RNA, preventing replication, and it is effective against bacteria, viruses, and fungi [15]. Studies show UV-C can significantly reduce airborne pathogens in aircraft cabins, lowering disease transmission risks [16]. A cost-benefit analysis found that combining continuous UV-C disinfection with HEPA filtration and mask-wearing could reduce in-flight transmission of SARS-CoV-2 and influenza A by up to 98% [1, 4].

A prepublication analysis estimates that due to the combined transmission of SARS-CoV-2 and influenza A aboard commercial aircraft in the United States from 2020 to 2023, there were about 10,000 annual deaths, declining to 3,000/year going forward and creating an estimated annual economic burden of $200 billion [3]. Up to 80% of the deaths and economic burden might be saved by supplementing the typical 30 air changes per hour of the aircraft ventilation system with a presently available 120 air changes per hour by using a UV-C disinfection system. The risks due to accidental overexposure to UV-C are orders of magnitude lower than the benefits. The 0.00003% risk of acute (one-time) overexposure for any given passenger may result in a 1–2-day skin or eye irritation, with no long-term effects or risks. This compares to the 15,000× greater risk at 0.5% of contracting COVID-19 or influenza A that persists for several days to weeks and carries a risk of hospitalization or death. The estimated risk of nonmelanoma skin cancer is virtually nil.

SAFETY CONCERNS AND MITIGATION STRATEGIES

While effective, UV-C disinfection poses safety risks, such as skin and eye damage from prolonged exposure, including erythema and photokeratitis [15]. In aircraft cabins, these risks are addressed by using far-UV-C light, which is less penetrating and therefore safer, and using engineering controls that limit exposure to safe exposure levels. Automated systems with redundant safety features like passive infrared, ultrasound, and light detection and ranging sensors (LIDAR) can shut off UV-C emitters when individuals are detected nearby, thus enhancing safety [17].

SUMMARY OF FINDINGS

The literature shows UV-C disinfection effectively reduces airborne and surface pathogens in aircraft cabins. Its advantages include continuous disinfection without harmful chemicals and improved efficiency, making it a valuable addition to aviation protocols. However, implementation requires careful engineering, maintenance, and adherence to safety limits, with advanced controls to mitigate risks [1, 4].

UV-C DISINFECTION IN AIRCRAFT CABINS

As air travel rebounds and aircraft cabins remain densely populated for hours on end, the need for robust infection-control measures is more pressing than ever. UV-C disinfection offers a scientifically validated means of curbing both airborne and surface pathogens in real time. Although it has garnered praise for enhancing passenger safety and reducing infection rates, considerations such as financial viability, operational logistics, and practical limitations must also factor into the decision-making process. The following subsections will weigh the benefits and challenges to provide a

balanced perspective on UV-C's role in fostering safer skies.

Mechanisms of UV-C Disinfection

UV-C light in the germicidal range of 200–280 nm damages the genetic material of pathogens through pyrimidine dimer formation (as shown in Figure 1), preventing replication and effectively inactivating them [16, 18].

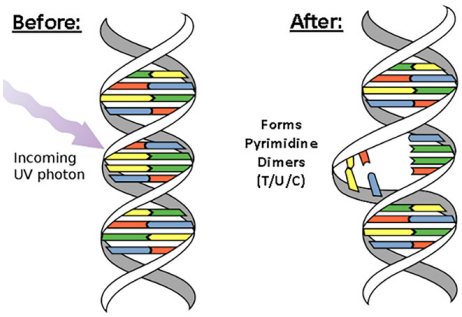


Figure 1. Inactivation of a Virus by UV-C Light *(Source: Allen [19])*.

Implementation in Aircraft Environments

Aircraft cabins, with confined spaces, high passenger density, and limited airflow (shadow spaces), pose challenges for disinfection. UV-C disinfection addresses these effectively by continuously sanitizing air and surfaces. The low humidity in aircraft cabins at cruise altitude dries out the mucous membranes of the respiratory tract, reducing their effectiveness in trapping and neutralizing airborne pathogens. This increases the risk of viral infection and replication. Additionally, dry cabin air causes virus-laden aerosols to lose moisture, stripping away their protective barrier that typically slows transmission and shields against natural UV light. In aircraft cabins, where UV-A and UV-B light are absent, these desiccated aerosols remain airborne longer (as shown in Figure 2), further elevating the risk of transmission. The combination of impaired mucous membranes and prolonged aerosol suspension creates an environment conducive to the rapid spread of airborne viruses [1].

The lack of moisture around viruses facilitates direct transmission, highlighting the need for enhanced disinfection measures during these critical periods.

Advantages Over Traditional Methods

UV-C disinfection offers several advantages over traditional methods, making it an attractive option for use in aircraft cabins.

- **Continuous Disinfection:** Unlike manual cleaning or chemical disinfection between flights, UV-C systems continuously disinfect during flights, reducing recontamination risks from infected passengers [15]. This avoids extending ground time and potential scheduling delays.
- **Chemical-Free Disinfection:** UV-C disinfection avoids chemical residues, protecting passengers, crew, and sensitive aircraft materials and making it safer and more eco-friendly than chemical disinfectants [17].
- **Rapid and Effective Pathogen Inactivation:** UV-C light can inactivate pathogens within minutes during initial cabin decontamination, resulting in quick turnarounds and improving efficiency in flight scheduling [12, 21].
- **Reduction of Human Error:** Automated UV-C systems minimize human error and standardize

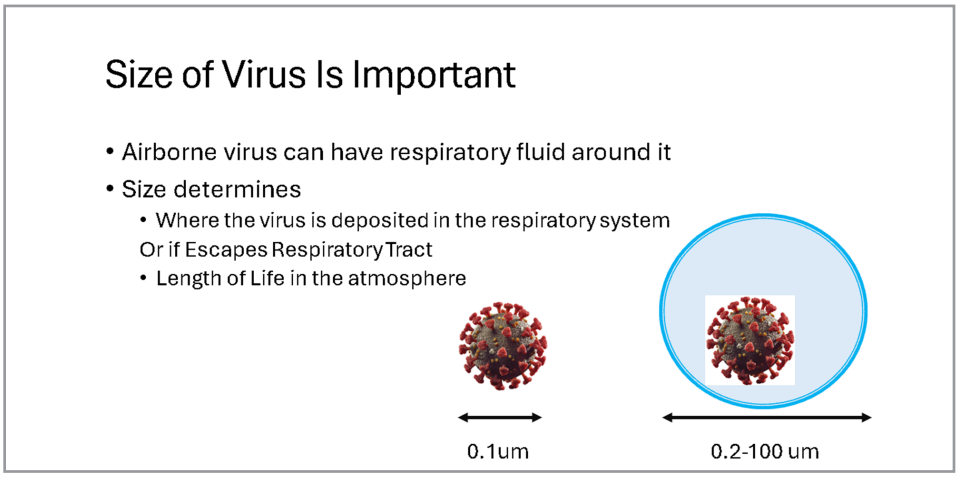


Figure 2. Comparing Virus Size With and Without Respiratory Fluid Retention *(Source: Belland et al. [20])*.

disinfection, ensuring consistent, thorough coverage across the cabin [1].

Challenges and Considerations

While UV-C disinfection offers significant benefits, its implementation in aircraft cabins must be carefully managed to address several challenges.

- **Safety Concerns:** The primary safety concern with UV-C disinfection is overexposure, which can cause skin burns (dermatitis/sunburn) and eye injuries (photokeratitis). Strict engineering controls and safer far-UV-C light, because of its limited penetration, mitigate these risks and enable continuous disinfection [17].
- **Engineering Controls:** Implementing UV-C disinfection in aircraft cabins requires sophisticated engineering solutions to ensure that UV-C light is effective while remaining within safe exposure limits. This includes the use of sensors and automated systems that can detect when passengers or crew are present and adjust the intensity or turn off the UV-C light to prevent overexposure [1].
- **Integration With Existing Systems:** UV-C systems must integrate with aircraft ventilation and lighting without affecting operational efficiency, requiring careful design and testing for compatibility [1].
- **Cost and Maintenance:** Installing and maintaining UV-C systems represents increased cost and weight, but advances in technology are expected to offset these costs and improve accessibility for airlines [1].

Conclusion

UV-C disinfection offers continuous, chemical-free air and surface sanitization, thus enhancing passenger safety against airborne diseases. Effective implementation requires addressing safety, engineering, and cost challenges. As technology advances, UV-C is set to play a growing role in aviation health measures [1].

CURRENT APPLICATIONS AND CASE STUDIES IN THE AVIATION INDUSTRY

The integration of UV-C disinfection technology in the aviation industry has gained significant traction, particularly in response to the COVID-19 pandemic.

Current Applications

Airlines and aircraft manufacturers have explored the following various applications of UV-C to enhance cabin hygiene and reduce the risk of disease transmission during flights:

- **Robotic UV-C Disinfection Systems:** Airlines like Swiss International Air Lines and JetBlue Airways have used robotic UV-C systems to sanitize cabins, autonomously disinfecting high-touch areas like tray tables and lavatories [1].
- **UV-C Integration With HVAC Systems:** UV-C technology, integrated into aircraft HVAC systems, continuously disinfects recirculated air to enhance quality and reduce pathogens. As an example, Boeing has explored the use of UV-C within its HVAC systems to enhance air quality and reduce airborne pathogens [1].
- **Far-UV-C Continuous Disinfection:** Far-UV-C light, safer for human exposure, enables continuous in-flight disinfection. Tested configurations include ceiling-mounted units for air pathogen inactivation [1].

Case Studies

The following case studies describe the different UV-C methods used in the airline industry for sanitizing and disinfecting surfaces:

- **JetBlue Airways – UV-C Robotic Disinfection:** JetBlue Airways, partnering with Honeywell, introduced the Honeywell UV Cabin System for rapid UV-C disinfection of aircraft interiors between flights, sanitizing high-touch surfaces in under 10 minutes and significantly reducing turnaround times [1, 4].

- **Qatar Airways – Comprehensive UV-C Implementation:** Qatar Airways adopted a UV-C strategy integrating robotic surface disinfection with the HVAC. UV-C robots were deployed for surface disinfection. The HVAC systems were upgraded to include UV-C emitters that continuously disinfected recirculated air, reducing the risk of in-flight transmission of COVID-19 and other infectious diseases [1].
- **Boeing – UV-C Wand and Far-UV-C Research:** Boeing developed and tested a UV-C wand as part of its "Confident Travel Initiative," aimed at improving passenger safety during the pandemic. The UV-C wand was designed for manual use by cleaning crews to disinfect surfaces in the aircraft cabin.
- **DIBEL –** DIBEL is currently being utilized in various settings, including high-traffic public spaces like airports, healthcare facilities, schools, and industrial workplaces. The following are examples where DIBEL is being used:
  - Multiple dental offices employing UV-C technologies
  - Public buildings (e.g., town of Southbury, CT)
  - Cast Nylons Ltd.
  - North Canton City Civic Center
  - The Long Island Aquarium
  - REV Fire Group
  - Gillette Stadium (e.g., New England Patriots)
  - Otis Elevator
  - Columbia University Irving Medical Center

ENGINEERING AND DESIGN CONSIDERATIONS

The successful implementation of UV-C disinfection systems in aircraft cabins requires careful consideration of several engineering and design factors. These considerations ensure that UV-C technology is both effective in inactivating pathogens and safe for passengers and crew.

System Integration With Aircraft Infrastructure

A key challenge in implementing UV-C disinfection is integrating it with HVAC, lighting, and structural systems, ensuring compatibility within the limited space of aircraft cabins and cargo areas. The following are examples of systems that would benefit from UV-C implementation:

- **Ventilation Systems:** Integrating UV-C with HVAC systems enables continuous air disinfection and requires precise lamp placement, light intensity, and airflow design to ensure effectiveness while avoiding passenger exposure [1].
- **Lighting Systems:** UV-C emitters can integrate with aircraft lighting by using ceiling or wall-mounted designs to disinfect surfaces. Advanced optics focus light on high-touch areas while minimizing exposure risks [1].

> ***A key challenge in implementing UV-C disinfection is integrating it with HVAC, lighting, and structural systems, ensuring compatibility within the limited space of aircraft cabins and cargo areas.***

Safety Mechanisms and Exposure Limits

Passenger and crew safety is paramount when designing UV-C disinfection systems for aircraft. Overexposure to UV-C light can cause skin burns and eye injuries, necessitating the implementation of the following robust safety mechanisms:

- **Exposure Controls:** UV-C systems require sensors to deactivate UV-C lights when passengers or crew are present. Designed for continuous operation during flights, far-UV-C systems must be calibrated to emit light at wavelengths and intensities safe for human exposure [17].
- **DIBEL:** DIBEL is a critical concept when discussing the safety of UV-C light-emitting diodes (LEDs), which emit ultraviolet light primarily in the 200–280-nm range. UV-C light

is highly effective in disinfection and sterilization because it can destroy the DNA and RNA of microorganisms, making it a popular choice for applications in healthcare, water purification, and surface disinfection [1, 4].

- **Redundant Safety Systems:** Redundant safety systems like LIDAR, ultrasound, and passive infrared sensors detect human presence and shut off UV-C emitters automatically. To deactivate the system in case of an emergency, manual override controls provide additional safety [1].

Operational Considerations

The operational efficiency of UV-C systems in aircraft depends on several factors, including durability and maintenance and energy consumption. These factors are described as follows:

- **Durability and Maintenance:** UV-C systems must be durable to withstand frequent flights, vibrations, and environmental changes. Components should be easy to maintain and replace with minimal downtime and be supported by regular maintenance schedules to ensure efficiency and timely repairs [1].
- **Energy Consumption:** UV-C systems should be energy efficient to minimize aircraft electrical demands. UV-C LEDs, with lower power use and heat output, are a promising alternative to mercury-vapor lamps. Optimal placement and scheduling can further reduce energy consumption while ensuring effective disinfection [1].

Design for Redundancy

UV-C systems must prioritize redundancy and reliability for cabin hygiene. Redundant emitters and real-time monitoring (as shown in Figure 3) ensure continuous disinfection during flights [1].

Compliance With Regulatory Standards

Aircraft UV-C disinfection systems must meet strict safety and health regulations, including International Air Transport Association, Federal Aviation Administration (FAA), and International Electrotechnical Commission (IEC) guidelines, and ensure safe use in occupied cabins without interfering with critical systems [1].

Conclusion

Designing UV-C disinfection systems for aircraft involves integrating safety, efficiency, redundancy, and compliance to ensure effective pathogen protection. Evolving technology will shape their implementation and adoption in aviation.

REGULATORY AND SAFETY STANDARDS

The integration of UV-C disinfection systems in aircraft cabins is subject to rigorous regulatory oversight to ensure passenger safety and compliance with industry standards. This section outlines the key regulatory frameworks and safety standards governing the use of UV-C technology in aviation.

FAA Regulations

In the United States, ICAO and the FAA regulate the use of novel disinfection systems in aircraft.

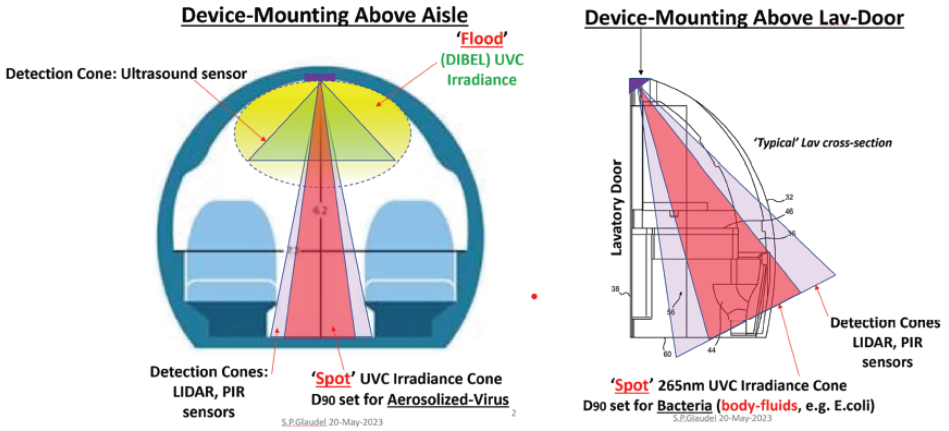


Figure 3. Examples of Engineering Control Systems *(Source: DeJohn et al. [4])*.

The FAA's regulations focus on ensuring that these systems do not interfere with the aircraft's safety or operational integrity. These regulations involve the following [1]:

- **Certification and Approval:** All aircraft systems require FAA certification, including tests for electromagnetic interference, structural integrity, system compatibility, and radiation effects on cabin materials like plastics and fabrics.
- **Operational Safety:** The FAA mandates safety features for aircraft systems, including automatic shut-offs, redundant controls, and crew guidelines, along with regular inspections to ensure safe operation.

Compliance and Certification for UV-C Systems

Compliance with regulatory standards is critical for implementing UV-C disinfection in commercial aircraft. The Project Specific Certification Plan (PSCP) outlines the steps to ensure the system meets FAA standards while maintaining airworthiness and safety. The process begins with the PSCP development and application for a supplemental-type certificate, which is granted after successful certification and compliance with FAA safety standards.

Key certification steps include the following:

- **Technical Standards Orders:** Ensures all components meet FAA criteria for reliability and safety in aircraft environments.
- **System Safety Analysis:** Conducts a failure hazard assessment to identify risks and ensure redundancies and fail-safes.
- **DO-160 Testing:** Verifies system performance under conditions like vibration, temperature changes, and electrical stress.
- **Flammability Testing:** Confirms components do not contribute to fire hazards.
- **Radiometric Validation:** Ensures UV-C irradiance levels stay within safe exposure limits.

Compliance is documented in the "Instructions for Continued Airworthiness, Responsibilities, Requirements, and Contents" which details maintenance procedures and standard operating procedures for safe and effective system use [22]. For new production aircraft, integrating UV-C systems during the design phase allows manufacturers to optimize placement and operation, with the system included in a type certificate, and certify compliance from the outset. This rigorous, phased process ensures UV-C systems align with all safety and regulatory standards.

IEC Standards

The IEC sets global safety standards for UV-C use, including aviation. IEC 62471:200 specifically addresses the photobiological safety of lamps and systems, such as the following [23]:

- **Photobiological Safety:** IEC 62471:200 defines UV-C hazard levels and sets exposure limits to ensure aircraft systems are safe for passengers and crew in occupied spaces.
- **System Design Compliance:** Aircraft UV-C systems must meet IEC standards for shielding, filters, and other protective measures to limit radiation exposure. IEC guidelines for testing and verification ensure systems operate within safe limits for passenger safety.

Occupational Safety and Health Administration (OSHA) Guidelines

For airline personnel, OSHA provides additional guidelines on UV-C exposure in the workplace. These guidelines are intended to protect maintenance workers, cleaning staff, and other personnel who may be exposed to UV-C radiation during aircraft servicing and include the following [1]:

- **Workplace Safety Standards:** OSHA recommends that airlines implement comprehensive training programs to educate employees about the risks associated with UV-C radiation and the proper use of personal protective equipment (PPE). OSHA also advises regular

monitoring of UV-C exposure levels in work environments to ensure they remain within safe limits.

- **PPE:** OSHA guidelines suggest the use of PPE, such as UV-blocking eyewear and protective clothing, for workers who may be exposed to UV-C radiation during maintenance or disinfection procedures. These precautions help minimize the risk of acute injuries, such as photokeratitis or erythema, and protect workers from potential long-term health effects.

Future Regulatory Developments

As UV-C technology evolves, regulatory bodies are likely to update and refine their standards to reflect new research and emerging best practices. Future developments may include stricter guidelines on the use of far-UV-C light in occupied spaces, enhanced safety protocols for continuous disinfection, and new certification processes for innovative UV-C systems.

Regulatory agencies are closely monitoring ongoing research into the long-term effects of UV-C exposure, particularly with the newer far-UV-C technologies. This research will inform future regulatory updates and ensure that safety standards remain aligned with the latest scientific findings and technological advancements [1, 21, 13].

PROSPECTS AND INNOVATIONS

The integration of UV-C disinfection technology in the aviation industry is poised to evolve significantly as research advances and new innovations emerge. This section explores the prospects of UV-C technology in aircraft disinfection, focusing on potential innovations that could enhance its effectiveness, safety, and accessibility.

Advancements in Far-UV-C Technology

The electromagnetic spectrum is shown in Figure 4. Far-UV-C light, which operates in the 207–222-nm wavelength range, represents one of the most promising developments in UV-C technology

Unlike UV-A and UV-B light, far-UV-C is less penetrating—it can inactivate pathogens effectively without posing a significant risk to human skin and eyes (as shown in Figure 5). This makes far-UV-C particularly suitable for continuous use in occupied spaces like aircraft cabins.

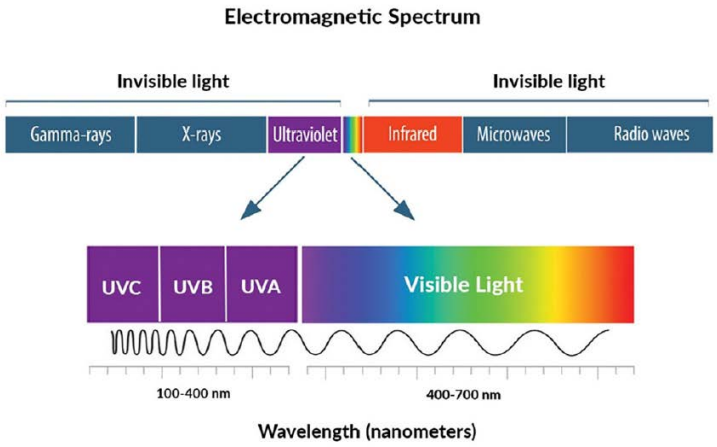


Figure 4. The Electromagnetic Spectrum *(Source: National Institute of Health [NIH] [24]).*

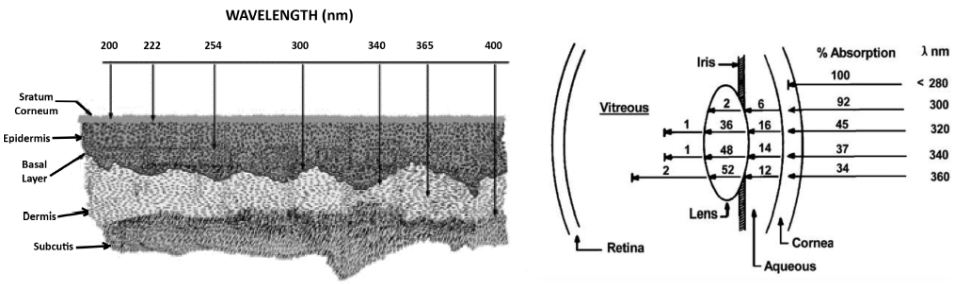


Figure 5. Ultraviolet Penetration of Skin and Eye *(Source: DeJohn et al. [4]).*

As the evidence around far-UV-C technology grows, it is becoming clearer how continuous disinfection could be integrated into everyday flight operations. At the same time, advancements in device miniaturization hint at targeted, portable solutions for high-contact surfaces. The following points illustrate how airlines could harness far-UV-C for both safer in-flight conditions and more versatile deployment options:

- **Increased Adoption and Safety:** With research supporting far-UV-C safety, airlines can adopt this technology for continuous in-flight disinfection. Integration into existing lighting and ventilation systems, along with smart sensors adjusting intensity based on occupancy, enhances real-time pathogen reduction and safety [1].
- **Miniaturization and Portability:** Advances may yield compact far-UV-C devices for targeted disinfection of aircraft touchpoints [1].

Innovations in UV-C LED Technology

The development of UV-C LEDs represents a significant innovation that could transform the use of UV-C disinfection in aviation. UV-C LEDs offer several advantages over traditional mercury-vapor lamps, including lower energy consumption, longer life spans, and the ability to produce light in specific wavelengths. These advantages include the following [1]:

The development of UV-C LEDs represents a significant innovation that could transform the use of UV-C disinfection in aviation.

- **Energy Efficiency and Sustainability:** As UV-C LED technology advances, it is expected to become more energy efficient, reducing the operational costs associated with UV-C disinfection and making continuous disinfection more viable.
- **Customizable and Flexible Designs:** UV-C LEDs can be designed to emit light in precise wavelengths, allowing for the customization of disinfection systems based on specific needs. Different areas of the aircraft could be equipped with LEDs optimized for either air or surface disinfection. In addition, flexible LED arrays could also be developed, allowing for the installation of UV-C systems in previously inaccessible areas.

Development of Hybrid Disinfection Systems

The future of aircraft disinfection may lie in hybrid systems that combine UV-C technology with other disinfection methods to provide comprehensive protection against a wide range of pathogens. These systems include the following benefits [1]:

- **Combination With Chemical Disinfectants:** Hybrid systems utilizing UV-C light and chemical disinfectants could offer the best of both worlds, with UV-C providing continuous in-flight disinfection and chemicals offering a powerful adjunct for more stubborn pathogens.
- **Integration With Air Filtration Technologies:** UV-C systems can be integrated with advanced air filtration technologies, such as HEPA filters and electrostatic precipitators, to create a multilayered defense against airborne pathogens.

Regulatory Evolution and Standardization

As UV-C technology continues to develop, regulatory bodies are likely to evolve their standards to accommodate new innovations. This evolution will ensure that UV-C systems remain safe and effective as they become more widely used in the aviation industry. Such standards include the following [1]:

- **Harmonization of Global Standards:** The future may see greater harmonization of UV-C safety standards across different

countries and regions, facilitating the global adoption of UV-C technology in aviation. This harmonization could also streamline the certification process for new UV-C systems, making it easier for airlines to implement cutting-edge technologies.

- **Adapting to Emerging Technologies:** As new UV-C technologies emerge, regulatory bodies will need to adapt their guidelines to address the unique challenges and opportunities these innovations present. This could include setting new exposure limits for far-UV-C light, establishing standards for Internet of Things-integrated systems, and developing guidelines for hybrid disinfection technologies [1].

LESSONS LEARNED AND FUTURE DIRECTIONS

The adoption of UV-C disinfection in aviation highlights the need for integration with existing systems, safety monitoring, and its role in a multilayered strategy. Airlines are advancing the use of UV-C technology, incorporating compact and cost-effective robotic solutions. These innovations highlight the potential to significantly enhance air travel safety, especially in addressing future health challenges.

The adoption of UV-C disinfection in aviation highlights the need for integration with existing systems, safety monitoring, and its role in a multilayered strategy.

CONCLUSIONS

The future of UV-C disinfection in aviation is promising, with innovations in far-UV-C, LEDs, and hybrid systems enhancing safety and effectiveness. Supported by technological innovation, UV-C disinfection is poised to become key to aircraft hygiene and ensure safer travel [1, 4]. ■

REFERENCES

[1] Belland, K., D. Garcia, and C. DeJohn. "Safety and Effectiveness Assessment of Ultraviolet-C Disinfection in Aircraft Cabins." *Aerospace Medicine and Human Performance*, vol. 95, no. 3, pp. 147–57, March 2024.

[2] Rafferty, A., K. Bofkin, W. Hughes, S. Souter, et al. "Does 2×2 Airplane Passenger Contact Tracing for Infectious Respiratory Pathogens Work? A Systematic Review of the Evidence." *PLOS ONE*, vol. 18, no. 2, e0264294, 2 February 2023.

[3] Allen, G. "A Risk vs. Benefit Analysis UV-C Advanced Aircraft Disinfection." *Aerospace Medicine and Human Performance*, in press.

[4] DeJohn, C., K. Belland, D. Garcia. "Methods of Aircraft Disinfection to Reduce Airborne Infectious Disease Transmission." *Aerospace Medicine and Human Performance*, vol. 95, no. 12, pp. 934–936, December 2024.

[5] Reed, N. G. "The History of Ultraviolet Germicidal Irradiation for Air Disinfection." *Public Health Rep.*, vol. 125, no. 1, pp. 15–27, 2010.

[6] Brenner, D. "Far-UVC Light at 222 nm is Showing Significant Potential to Safely and Efficiently Inactivate Airborne Pathogens in Occupied Indoor Locations." *Photochem. Photobiol.*, vol. 990, no. 3, pp. 1047–1050, 4 November 2022.

[7] Blazejewski, C., M. Guerry, P. Sebastien, A. Durocher, and S. Nseir. "New Methods to Clean ICU Rooms." *Infect. Disord. Drug Targets*, vol. 11, no. 4, pp. 365–75, August 2011.

[8] Ramos, C. C. R., J. L. A. Roque, D. B. Sarmiento, L. E. G. Suarez, J. T. P. Sunio, K. I. B. Tabungar, et al. "Use of Ultraviolet-C in Environmental Sterilization in Hospitals: A Systematic Review on Efficacy and Safety." *Int. J. Health Sci.* (*Qassim*), vol. 14, no. 6, pp. 52–65, 2020.

[9] Welch, D., M. Buonanno, V. Grilj, I. Shuryak, C. Crickmore, et al. "Far-UVC Light: A New Tool to Control the Spread of Airborne-Mediated Microbial Diseases." *Sci. Rep.*, vol. 8, no. 1, pp. 2752–2759, 9 February 2018.

[10] Narita, K., K. Asano, K. Naito, H. Ohashi, M. Sasaki, Y. Morimoto, et al. "Ultraviolet C Light With Wavelength of 222 nm Inactivates a Wide Spectrum of Microbial Pathogens." *Journal of Hospital Infection*, vol. 105, no. 3, pp. 459–467, 1 July 2020.

[11] Wang, X. V., and L. Wang. "A Literature Survey of the Robotic Technologies During the COVID-19 Pandemic." *Journal of Manufacturing Systems*, vol. 60, pp. 823–836, 1 July 2021.

[12] Allen, G., K. Benner, and W. Bahnfleth. "Inactivation of Pathogens in Air Using Ultraviolet Direct Irradiation Below Exposure Limits." *J. Res. Natl. Inst. Stand. Technol.*, vol. 126, 1 March 2022.

[13] American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). ASHRAE Standard 241: "Control of Infectious Aerosols." https://www.ashrae.org/technical-resources/bookstore/ashrae-standard-241-control-of-infectious-aerosols, 2023.

[14] Wang, F., R. You, T. Zhang, and Q. Chen. "Recent Progress on Studies of Airborne Infectious Disease Transmission, Air Quality, and Thermal Comfort in the Airliner Cabin Air Environment." *Indoor Air*, vol. 32, no. 4, e13032, 2022.

[15] Blatchley, E., D. Brenner, H. Claus, T. Cowan, K. Linden, Y. Liu, et al. "Far UV-C Radiation: An Emerging Tool for Pandemic Control." *Critical Reviews in Environmental Science and Technology*, vol. 53, no. 6, pp. 733–53, 19 March 2023.

[16] Biasin, M., A. Bianco, G. Pareschi, A. Cavalleri, C. Cavatorta, C. Fenizia, et al. "UV-C Irradiation Is Highly Effective in Inactivating SARS-CoV-2 Replication." *Sci. Rep.*, vol. 11, no. 1, p. 6260, 18 March 2021.

[17] Barnard, I., E. Eadie, and K. Wood. "Further Evidence That Far-UVC for Disinfection Is Unlikely

to Cause Erythema or Pre-Mutagenic DNA Lesions in Skin." *Photodermatology, Photoimmunology & Photomedicine*, vol. 36, no. 6, pp. 476–477, November 2020.

[18] Blatchley, E. R., D. Brenner, H. Claus, T. E. Cowan, and D. Sliney. "Far UV-C Radiation: Current State-of Knowledge." The International Ultraviolet Association (IUVA), https://iuva.org/resources/covid-19/Far%20UV-C%20Radiation-%20Current%20State-of%20Knowledge.pdf, 2021.

[19] Allen, J. "Ultraviolet Radiation: How it Affects Life on Earth." NASA Earth Observatory, Ultraviolet Radiation: How It Affects Life on Earth, 6 September 2001.

[20] Belland, K., D. Garcia, C. DeJohn, G. R. Allen, W. D. Mills, and S. P. Glaudel. "Safety and Effectiveness Assessment of Ultraviolet-C Disinfection in Aircraft Cabins." *Aerospace Medical & Human Performance*, vol. 95, no. 3, p. 148, 1 March 2024.

[21] Yang, J. H., U. I. Wu, H. M. Tai, and W. H. S heng. "Effectiveness of an Ultraviolet-C Disinfection System for Reduction of Healthcare-Associated Pathogens." *Journal of Microbiology, Immunology and Infection*, vol. 52, no. 3, pp. 487–493, 1 June 2019.

[22] FAA. "Instructions for Continued Airworthiness Responsibilities, Requirements, and Contents." FAA Order 8110.54A, https://www.faa.gov/document Library/media/Order/FAA_Order_8110.54A.pdf, accessed on 24 February 2025.

[23] International Electrotechnical Commission. "Photobiological Safety of Lamps and Lamp Systems." IEC 62471:200, https://www.iecee.org/certification/iec-standards/iec-624712006, accessed on 25 February 2025.

[24] NIH. "Protecting Your Eyes From the Sun's UV Light." National Eye Institute, https://www.nei.nih.gov/about/news-and-events/news/protecting-your-eyes-suns-uv-light, 5 July 2022.

BIOGRAPHIES

KRIS M. BELLAND, D.O., MPH, is the president and chief executive officer of Aerospace Medical Strategic Consultation, PLLC, with extensive experience in family and aerospace medicine (board-certified), strategic studies, and public health. He was a former president of the Aerospace Medical Association and served over 30 years in the U.S. Navy. Dr. Belland holds a Doctor of Osteopathic Medicine (DO) from the Philadelphia College of Osteopathic Medicine.

CHUCK A. DEJOHN, D.O., MPH, is an accomplished aerospace medicine expert and medical consultant, where he evaluates the use of direct ultraviolet irradiation to reduce disease transmission aboard aircraft. He served as a Navy instructor pilot, a branch chief at the Naval Aerospace Medical Research Laboratory, and the lead of the Medical Research Team at the FAA Civil Aerospace Medical Research Institute. He has presented to scientific audiences and published numerous articles in scientific journals. Dr. DeJohn holds a Doctor of Osteopathic Medicine (DO) from the Oklahoma Osteopathic Medical School.

WEB EXCLUSIVE

FINANCING OF TERRORISM THROUGH CRYPTOCURRENCIES

By Keven Hendricks | *Photo Source: Canva*

This article examines how terrorist organizations began to incorporate cryptocurrencies as part of their financing networks in tandem with the rise of dark web drugs. Cryptocurrencies remain a persistent medium for the fiduciary networks that enable terrorism around the world.

AVAILABLE ONLY ONLINE

https://hdiac.dtic.mil/articles/financing-terrorism-through-cryptocurrencies

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 https://hdiac.dtic.mil 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.

HTTPS://HDIAC.DTIC.MIL
CONNECT WITH US ON SOCIAL MEDIA