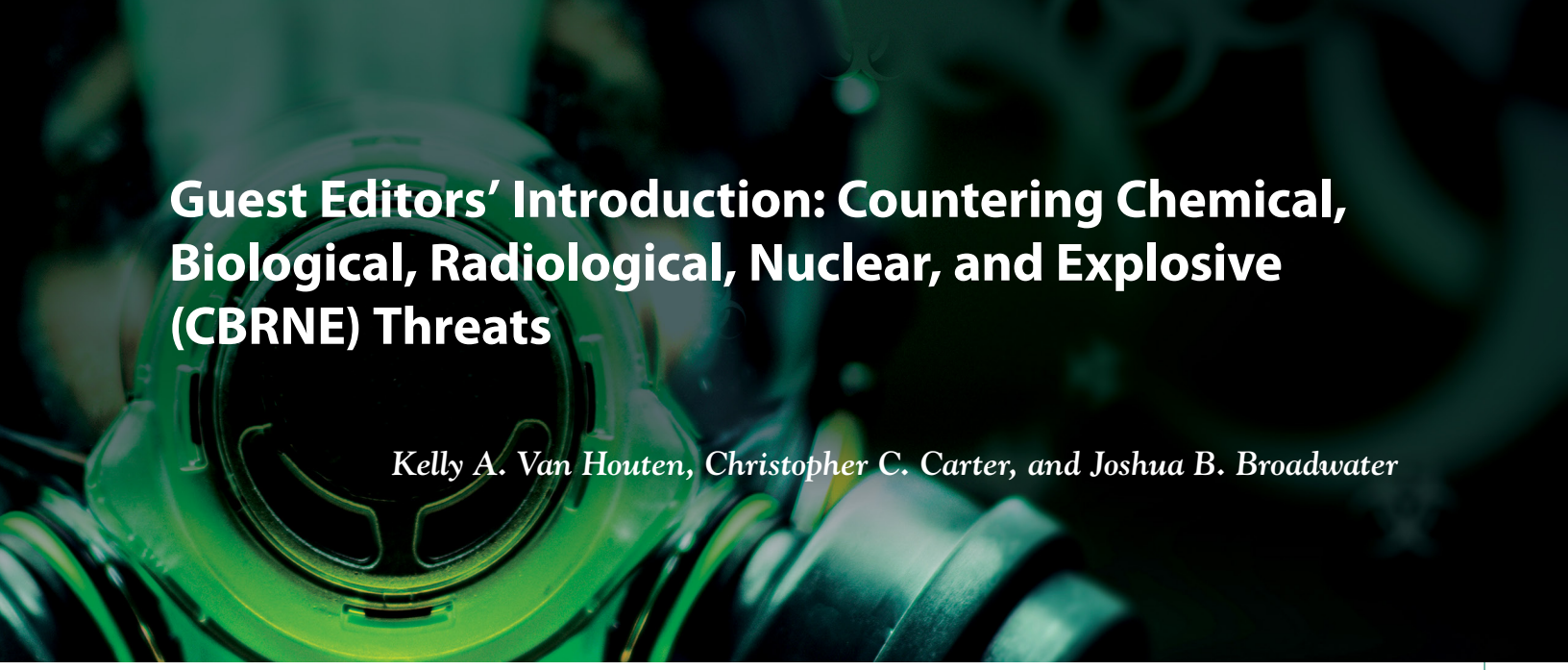

Guest Editors' Introduction: Countering Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Threats

Kelly A. Van Houten, Christopher C. Carter, and Joshua B. Broadwater

ABSTRACT

The Johns Hopkins University Applied Physics Laboratory (APL) plays a crucial role in helping the United States anticipate, counter, and prevail against chemical, biological, radiological, nuclear, and explosive (CBRNE) threats. APL researchers create innovative technologies and methodologies that enhance national security and provide decision-makers with actionable intelligence in the face of evolving threats. The counterterrorism and homeland security landscape has dramatically changed since the Johns Hopkins APL Technical Digest *last published a comprehensive review on these topics in 2003. In the years since, APL's expertise has expanded significantly, integrating advancements in artificial intelligence, data analytics, autonomous systems, and sensor technologies to address increasingly sophisticated CBRNE challenges. This issue highlights APL's latest contributions to detecting, identifying, and mitigating CBRNE threats to strengthen national and global security.*

INTRODUCTION

Although asymmetric threats are a focus of international security efforts, the risk of a chemical, biological, radiological, nuclear, and explosive (CBRNE) attack remains ever-present, and capabilities are constantly evolving. These threats can be anthropogenic (e.g., chemical warfare agents or explosions) or naturally occurring (e.g., disease outbreaks) and are among the most insidious challenges facing our nation. Their impact, evidenced in the terrorist attacks on 9/11 or the COVID-19 pandemic, can be catastrophic in both the immediate and long terms. APL is dedicated to developing game-changing capabilities to enhance resilience, detect and neutralize threats before they materialize, and create asymmetric advantages for national security.

APL leverages a broad range of expertise to counter CBRNE threats, employing advanced competencies in molecular and cell biology, omics characterization, public health and epidemiology, aerosol science, chemical synthesis, chemical and nuclear engineering, nuclear physics, advanced analytics, and sensor design and development. Additionally, we integrate artificial intelligence, data science, complex systems, and autonomy to develop innovative technologies and systems that transform vast amounts of data into actionable intelligence and strategic advantages.

This issue highlights APL's latest contributions to detecting, identifying, and mitigating CBRNE threats to strengthen national and global security.

THE ARTICLES

This issue begins with "Simulants for Chemical and Explosive Threats" in which Lawrence and Van Houten describe the development of a systematic process to design and select effective simulants. Because working with real chemical warfare agents and explosives is dangerous and highly regulated, simulants (nontoxic substances that mimic the key properties of chemical warfare agents and explosives) are used to facilitate research, training, and technology development. The systems-engineering-based approach ensures that selected simulants closely match the properties of real threats but are safe to handle. The article also describes how these simulants help improve detection technologies, decontamination methods, and training exercises for security and defense personnel.

Next, in "Large-Scale Production of Radiopure ^{135}Xe from Bremsstrahlung γ-Irradiation of Solid Xenon Difluoride," Lloyd et al. present a novel method for producing the radioactive xenon isotope ^{135}Xe, which plays a critical role in monitoring nuclear tests worldwide. This research was conducted in APL's linear accelerator facility, which was established in 2022 to support experiments requiring extremely high radiation fields. The team successfully generated ^{135}Xe from solid xenon difluoride (XeF_2) using an innovative approach that significantly increases yield while ensuring the isotope remains pure and free of contaminants. This breakthrough enhances the calibration of nuclear test monitoring equipment, improving the ability to detect illicit underground nuclear explosions. Additionally, the study outlines strategies for refining the process to enable more efficient large-scale production.

In "APL's Contributions to the Odor Detection Canine Community," Klimkiewicz and Deglau highlight 15 years of advancements in odor detection canine research. These canines play a crucial role in security, law enforcement, and disaster response, assisting in detection of explosives, narcotics, and other hazardous materials. APL has contributed to multiple aspects of advancing canine detection capabilities, including breeding high-performance detection dogs, developing advanced training methodologies, and designing safer training aids that mimic real threats without using dangerous substances. Additionally, APL researchers have explored methods to enhance communication between dogs and handlers and have optimized deployment conditions through airflow monitoring and other tools. These innovations significantly improve the effectiveness and reliability of odor detection canines in real-world operations. Through ongoing research and collaboration, APL continues to advance the role of detection dogs in national security and public safety.

The next few articles highlight advancements in artificial intelligence and machine learning. First, in "Using Knowledge Graphs to Counter Weapons of Mass Destruction," Mariner et al. describe the development of a knowledge graph system designed to help US government agencies combat weapons of mass destruction. Many government databases contain critical yet fragmented information about CBRNE threats, making it challenging to track emerging risks. To address this, APL developed the CBRNE Semantic Framework, a structured data model that organizes and connects disparate sources of information, enabling more effective pattern recognition and threat detection. This framework powers a tool that allows analysts to rapidly retrieve relevant data, assess potential risks, and anticipate how adversaries might develop weapons of mass destruction. By leveraging this technology, agencies can enhance their ability to detect, prevent, and respond to evolving threats.

Next, in "MLM: Machine Learning for Threat Characterization of Unidentified Metagenomic Reads," Baugher et al. describe their development of a machine learning system to analyze unidentified genetic material in biological samples. The Machine Learning for Metagenomics (MLM) pipeline is designed to detect potential biological threats by analyzing DNA sequences that do not match known organisms. Using advanced classification models, the system assigns threat levels to these unidentified sequences, providing forensic and military investigators with real-time hazard assessments. Tests of the system have demonstrated its high accuracy in identifying threats, highlighting its value for monitoring emerging or engineered biological dangers. The technology is being refined for deployment in field-ready devices, enhancing rapid threat detection and response capabilities.

In "Assessment of Sequencing for Pathogen-Agnostic Biothreat Diagnostics, Detection, and Actionability for Military Applications," Bradburne et al. explore the use of genomic sequencing as a tool for detecting biological threats in military and field settings. While traditional methods, such as polymerase chain reaction (PCR), remain the fastest, most cost-effective, and most reliable option for identifying known pathogens, sequencing can be valuable when dealing with unknown threats. The researchers tested different sequencing methods and found that a hybrid enrichment approach was the most effective for detecting biothreats in simulated patient samples. However, sequencing remains slower and more expensive than PCR, making it most useful in cases where the infectious agent is unknown or emerging. As sequencing technology advances and costs decline, it may become a more viable tool for military and field applications, improving biothreat detection and response capabilities.

In "Wearables-Based Disease Surveillance: SIGMA+ Human Sentinel Networks Concept of Operations," Stanish et al. describe how wearable technology, such

as smartwatches, could be used to detect and monitor disease outbreaks in real time. A network of volunteers wearing sensors could provide early warning of infectious disease outbreaks, ranging from seasonal flu to biothreats such as anthrax. By analyzing changes in heart rate, temperature, and other physiological markers, the system can alert individuals to seek medical testing, enabling public health officials to rapidly respond. Modeling showed that tracking just 5% of a population with these sensors could detect outbreaks days earlier than traditional surveillance methods. This innovative approach has the potential to enhance early disease detection, improve emergency response efforts, and strengthen public health preparedness.

CONCLUSION

The articles in this issue reflect the breadth and depth of APL's sustained commitment to countering CBRNE threats through innovation, scientific rigor, and cross-disciplinary collaboration. From advancing threat-based training tools and pioneering new methods for nuclear test detection to enhancing real-time biosurveillance through wearable technology and applying cutting-edge machine learning to genomic data, APL continues to push the boundaries of what is possible in national and global security. These capabilities are not only advancing threat detection and response, but they are also reshaping the landscape of preparedness and resilience in an era of increasingly complex and asymmetric threats. As adversaries evolve and technologies advance, APL remains at the forefront of developing the tools, systems, and strategies necessary to protect our nation and its allies.

Kelly A. Van Houten, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Kelly A. Van Houten is the supervisor of APL's Applied Chemistry and Physics Group, which is responsible for developing solutions to detect, defeat, and deny chemical and nuclear threats. She has a BA in chemistry from Johns Hopkins University, a PhD in chemistry from the University of Maryland, College Park, and an MBA from Johns Hopkins University. She has over 20 years of experience developing novel detection methodologies for organophosphates, designing and synthesizing chemical simulants, and developing chemistry-based warfighter tools. Her email address is kelly.van.houten@jhuapl.edu.

Christopher C. Carter, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Christopher C. Carter is the acting manager of APL's Counter Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Threats program area. He has a BS in physics from Washington & Jefferson College and an MS and a PhD in chemical physics from Ohio State University. He has a broad technical background in physics, chemistry, CBRNE defense systems, and optical/laser-based techniques, with experience in research and development of systems for the detection, identification, and defeat of CBRNE species. His email address is christopher.carter@jhuapl.edu.

Joshua B. Broadwater, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Joshua B. Broadwater is the manager of APL's Health Protection and Assurance program area. He has a BEng in electrical engineering and applied mathematics from Vanderbilt University, an MS in electrical engineering from the Georgia Institute of Technology, and a PhD in electrical engineering from the University of Maryland, College Park. His primary technical skills include detection and pattern recognition algorithms for electro-optical/infrared remote sensing systems, and his specialty is hyperspectral/multispectral imaging. Joshua's other research includes work on adaptive and semi-supervised classification methods, incorporation of physics models into pattern recognition systems, and statistical signal processing techniques. His email address is joshua.broadwater@jhuapl.edu.