Research Challenges in Combating Terrorist Use of Explosives in the United States 2024

Austin C. Doctor
Samuel T. Hunter
Gina Scott Ligon
Gary Wes Carter
Dan Polanski

See next page for additional authors

Follow this and additional works at: https://digitalcommons.unomaha.edu/ncitereportsresearch
Please take our feedback survey at: https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE
Authors
Austin C. Doctor, Samuel T. Hunter, Gina Scott Ligon, Gary Wes Carter, Dan Polanski, and Jimmie Oxley
Research Challenges in Combating Terrorist Use of Explosives in the United States

2024
ABOUT THIS REPORT
April 2024

As expressed in the original 2008 report, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, improvised explosive devices (IEDs) are generally easy to develop, difficult to combat, and cause disproportionate physical and psychological harm to the citizenry. Research, development, test, and evaluation options to assist domestic counter-IED efforts are plentiful, easily overwhelming the ability of government and industry to fund. This updated report outlines 10 challenge areas where concentrated research can be most beneficial when combating IED use in the homeland and is a summation of interagency efforts to analyze operational capabilities and gaps, as well as their associated research needs.

ABOUT THE NATIONAL COUNTERTERRORISM INNOVATION, TECHNOLOGY, AND EDUCATION CENTER

The National Counterterrorism Innovation, Technology, and Education (NCITE) Center was established in 2020 as the Department of Homeland Security (DHS) Center of Excellence for counterterrorism and terrorism prevention research. Sponsored by the DHS Science and Technology Directorate (S&T) Office of University Programs, NCITE leads an elite academic consortium of more than 50 researchers at partner institutions across the U.S. and Europe. Headquartered at the University of Nebraska at Omaha, NCITE is the principal U.S. academic partner for counterterrorism research, technology, and workforce development.

ABOUT THE NATIONAL STRATEGIC RESEARCH INSTITUTE

In 2012, the U.S. Strategic Command (USSTRATCOM) sponsored the establishment of the National Strategic Research Institute (NSRI), a University Affiliated Research Center (UARC), through the award of an Indefinite Delivery Indefinite Quantity (IDIQ) contract. Under the original IDIQ contract, the University of Nebraska System has performed dozens of task orders while developing core competencies in research and development, test and evaluation, systems innovation, integration, and engineering in support of Department of Defense (DOD) warfighting capabilities and countering weapons of mass destruction.

PREFERRED CITATION


AWARD ACKNOWLEDGEMENT AND DISCLAIMER

The research in this report was supported by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) under Contract Award No. 70RSAT21G00000002 / 70RSAT22FR0000050: “Workshop and Report on Research Challenges in Combating Terrorist Use of Explosives in the United States.” The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.
RESEARCH TEAM

Members

Austin Doctor (Principal Investigator), University of Nebraska at Omaha, NCITE
Sam Hunter, University of Nebraska at Omaha, NCITE
Gina Ligon, University of Nebraska at Omaha, NCITE
Paul Gill, University College London
Gary Wes Carter, National Strategic Research Institute
Dan Polanski, National Strategic Research Institute
Jimmie Oxley, University of Rhode Island

Staff

Blake Ursch, University of Nebraska at Omaha, NCITE
Sara Vetter, University of Nebraska at Omaha, NCITE
Angie Benda, University of Nebraska at Omaha, NCITE
Lauren Moss, University of Nebraska at Omaha, NCITE
Keira Nevius, University of Nebraska at Omaha, NCITE
Philip Doherty, University College London
Though it has been more than a decade since the National Science and Technology Council Subcommittee on Domestic IEDs (D-IED SC) published the seminal report *Research Challenges in Combating Terrorist Use of Explosives in the United States*, the study of improvised explosive devices (IEDs) remains equally as relevant today. Given they are relatively easy to build and cause grave harm, the threat of IED attacks remains pervasive. As such, it’s vitally important that we continue to provide federal, state, local, and tribal law enforcement and responders with the knowledge and tools necessary to combat this threat.

This updated report, produced by the Department of Homeland Security’s National Counterterrorism Innovation, Technology, and Education (NCITE) Center of Excellence, on behalf of DHS’s Science and Technology Directorate and the Cybersecurity and Infrastructure Security Agency’s Office for Bombing Prevention, will be a key resource. Beyond the report, the 10 timely, cross-cutting Grand Challenges outlined herein are a call to action, and partnership will be key to future success.

The development of this report was an outstanding display of collaboration, bringing together multiple federal agencies, state and local law enforcement organizations, and academic partners. I encourage those federal agencies with responsibilities in the counter-IED mission space to leverage this momentum to foster interagency collaboration and coordination in tackling the Grand Challenges for a more secure Homeland.

Dimitri Kusnezov, Ph.D.
Under Secretary for Science and Technology
The University of Nebraska System is one of the very few centers of gravity for innovative and rigorous national security research and workforce development.

American communities and critical infrastructure continue to be threatened by the actions of individuals and groups motivated by violent extremist ideologies. Having enduring memories of the days following the 9/11 World Trade Center attacks in New York, I have a unique perspective on how important it is to prevent extremist actions on our homeland soil. For terrorists, improvised explosive devices remain a reliable and accessible tool for wreaking destruction and harm. And, as this report demonstrates, this threat is evolving.

The updated Research Challenges in Combating Terrorist Use of Explosives in the United States report, led by the National Counterterrorism Innovation, Technology, and Education Center (NCITE), will surely serve as a key resource for the national security community – including law enforcement, intelligence, military, and first responders – working tirelessly to keep Americans safe.

I am encouraged to see this report made possible by the partnership of two leading applied research teams in the University of Nebraska multi-campus community. The collaboration between NCITE, a Department of Homeland Security Center of Excellence, and the National Strategic Research Institute (NSRI), a Department of Defense University Affiliated Research Center (UARC), is an exemplar of the University of Nebraska System’s operational mission and commitment to developing novel solutions – based upon successful partnerships – to address the most complex, persistent challenges.

Jeffrey P. Gold, M.D.
President-Elect
University of Nebraska System
EXECUTIVE SUMMARY

Terrorists continue to use improvised explosive devices (IEDs) to cause destruction, harm, and disruption. The threat is also evolving as violent extremists develop new methods of IED design and use. Efforts to counter terrorist IED attacks in the United States are inhibited by knowledge and capability gaps; some are persistent, others are emerging. The related operational challenges can be supported by the scientific community through targeted research, development, test, and evaluation (RDT&E) initiatives.

The Department of Homeland Security has tasked the National Counterterrorism Innovation, Technology, and Education (NCITE) Center with identifying the future threat related to terrorist use of explosives within the United States and with recommending pathways to mitigate it through targeted RDT&E. This includes the identification and prioritization of the knowledge and capabilities needed to disrupt the chain of events leading up to an IED attack, protect vulnerable targets, and effectively respond to IED incidents. This report is meant to aid efforts to coordinate, synchronize, and deconflict the array of interconnected RDT&E efforts funded across the U.S. government.

Changes in policy will likely be the most significant driver in creating new standards and capabilities to combat the U.S. homeland IED threat. The scope of this report focuses specifically on needs tied to knowledge and capability gaps that can be met by the development of scientific and technological solutions. Based in part on expertise and valuable inputs from the interagency counter-IED (C-IED) mission community, the project team identified ten such needs – Grand Challenges – deemed to be both important and urgent:

| Soft Target Protection |
| Characterization of the IED Threat Landscape |
| Remotely Commanded IEDs |
| Unmanned Systems (UxS) |
| Explosive Precursor Chemicals and Bomb-Making Materials |
| Malign Use of Emerging Commercial Technologies |
| Standoff and Checkpoint Detection |
| Incident Response |
| Information Management and Sharing |
| Assessment, Training, and Evaluation |

The descriptions of the needs contained herein form the basis upon which the federal agencies with responsibilities in the C-IED mission may build their programs and foster interagency collaboration and coordination. This report is designed to meet the needs of government entities and their partners in academia and private industry on the development of science and technology related to combating terrorist use of IEDs.
INTRODUCTION

Improvised explosive devices (IEDs) are relatively simple to make, difficult to combat, and cause disproportionate harm and disruption.⁰ Accordingly, they continue to be used as a weapon of choice by terrorists at home and abroad. As terrorists identify and adapt to the current barriers and protections, they develop new capabilities to circumvent these restrictions and exploit novel vulnerabilities. The enduring and evolving nature of the IED threat to U.S. national and homeland security requires that practitioners are equipped to stay ahead of the innovation curve with up-to-date knowledge and capabilities.

Thus, a key challenge is defining the set of urgent advancements in scientific technology needed by the counter-IED (C-IED) mission community to disrupt the chain of events leading up to an IED attack, protect vulnerable targets, and/or respond to an IED incident.² Relatedly, to maximize the utility of scientific contributions to this immense effort, it is necessary to coordinate, harmonize, and deconflict the numerous research, development, test, and evaluation (RDT&E) funded activities conducted across the basic and applied research community.

In support of this priority, in 2008, the National Science and Technology Council (NSTC) Subcommittee on Domestic IEDs (D-IED SC) published the first Research Challenges in Combating Terrorist Use of Explosives in the United States report.³ The report identifies high-priority science and technology challenges to be addressed through targeted RDT&E initiatives. Since the time of the report’s publication, sponsored RDT&E programs have made notable advancements in support of the domestic C-IED workforce and across critical mission areas. However, major knowledge and capability gaps persist, and new ones have emerged as the terrorism and IED landscape has evolved. Therefore, to ensure a sustained proactive posture against the IED threat, it is necessary to update the recommended set of scientific contributions needed to equip and empower the future counterterrorism and C-IED workforce.

The Department of Homeland Security Science and Technology Directorate (S&T) and the Cybersecurity and Infrastructure Security Agency (CISA) Office for Bombing Prevention (OBP) is tasking the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, the Center of Excellence for counterterrorism research, with identifying the future threats related to terrorist use of explosives within the U.S. and recommending pathways to mitigate it through advancement science and technology. The completion of this initiative leveraged the valuable inputs of experts in academia, industry, and government. Much of the interagency C-IED mission community at the federal as well as state, local, tribal, and territorial levels of government actively contributed their unique perspectives to this effort:

**Department of Homeland Security (DHS)**
- Headquarters (HQ)
- Science and Technology Directorate (S&T)
- Cybersecurity and Infrastructure Security Agency (CISA)
  - Office for Bombing Prevention (OBP)
  - Protective Security Advisor Program (PSA)
- Transportation Security Administration (TSA)
- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- Federal Law Enforcement Training Centers (FLETC)
- U.S. Secret Service (USSS)
Knowledge and Capability Gaps: Identification and Prioritization Process

The NCITE project team focused on identifying the pressing, cross-cutting knowledge and capability gaps within the C-IED mission that could effectively be resolved through targeted RDT&E. To do so, the project team identified a number of potential operational needs through the following methods: (1) environmental scan of the existing public and academic knowledge base; (2) comprehensive interviews with IED research and operational subject matter experts; (3) qualitative analysis of said interviews; (4) distribution of a C-IED mission survey among practitioners; and (5) qualitative analysis of the relevant dataset.

Subject matter experts from across the C-IED stakeholder community participated in extensive semi-structured interviews involving a standardized set of questions as well as additional follow-up questions based on the information they provided. All responses were collated and analyzed to look for common patterns and themes across interviews. A list of preliminary operational requirements – over 90 relevant knowledge and capability gaps – was identified by the research team. Upon review, these were aggregated into a set of 42 unique operational challenges.

The NCITE project team hosted a workshop with select leaders from across the C-IED mission community that met in person to discuss the problem set. As part of the workshop, all attendees completed a survey in which they provided their individual opinions on a set of identified operational challenges. Respondents ranked each on two scales:

- **Urgency**: The timeliness of the problem and how fast it should be addressed.
- **Importance**: The value of the problem that should be addressed.
Through the quantitative analysis of the data, and based on this prioritization process, the NCITE project team identified the following 10 operational areas as highly urgent and important:

**Grand Challenges**

1. Soft Target Protection
2. Characterization of the IED Threat Landscape
3. Remotely Commanded IEDs
4. Unmanned Systems (UxS)
5. Explosive Precursor Chemicals and Bomb-Making Materials
6. Malign Use of Emerging Commercial Technologies
7. Standoff and Checkpoint Detection
8. Incident Response
9. Information Management and Sharing
10. Assessment, Training, and Evaluation

In the following report, each Grand Challenge is summarized (1) to inform the C-IED community of the need, (2) to address challenges faced within the operating environment and, (3) to propose ways forward through funded science and technology initiatives to combat and prevent the use of IEDs. The order in which the Grand Challenges are presented does not necessarily reflect relative urgency or importance. The Grand Challenges require sustained attention from all stakeholders, from research and testing to the application of advancements. Further, they underscore the need for continued multi-sector, interagency collaboration in the effort to combat terrorists’ use of explosives in the United States.
# TABLE OF CONTENTS

About the Report ........................................................................................................................................... 2

Forewords.......................................................................................................................................................... 4

Executive Summary ......................................................................................................................................... 7

Introduction .................................................................................................................................................... 8

**Grand Challenge 1:** Soft Target Protection ............................................................................................... 15

**Grand Challenge 2:** Characterization of the IED Threat Landscape .......................................................... 17

**Grand Challenge 3:** Remotely Commanded IEDs ..................................................................................... 19

**Grand Challenge 4:** Unmanned Systems (UxS) ......................................................................................... 21

**Grand Challenge 5:** Explosive Precursor Chemicals and Bomb-Making Materials .................................. 24

**Grand Challenge 6:** Malign Use of Emerging Commercial Technologies ................................................... 26

**Grand Challenge 7:** Standoff and Checkpoint Detection ........................................................................... 28

**Grand Challenge 8:** Incident Response ................................................................................................. 30

**Grand Challenge 9:** Information Management and Sharing ................................................................. 33

**Grand Challenge 10:** Assessment, Training, and Evaluation ................................................................. 35

Conclusion ...................................................................................................................................................... 39

Appendix A .................................................................................................................................................... 40

Appendix B .................................................................................................................................................... 41

References ..................................................................................................................................................... 42

Endnotes ......................................................................................................................................................... 43
Research Challenges in Combating Terrorist Use of Explosives in the United States
Anatomy of an IED*

**IMPROVISED EXPLOSIVE DEVICE**
An unconventional explosive weapon that can take any form and be activated in a variety of ways. It may incorporate military and/or nonmilitary components.**

**POWER SOURCE**
A device that stores or releases electrical or mechanical energy. The key elements of information about a power source are its type and source, number of batteries and their configuration (series or parallel), its voltage (if electrical), and how it is connected to close an IED switch.

**MAIN CHARGE**
The explosive charge that is provided to accomplish the end result in a munition or improvised device. Examples include bursting a casing to provide blast and fragmentation, splitting a canister to dispense sub-munitions, or producing other effects.

**CONTAINER**
A vessel for concealing an IED and for holding the main charge together. The container may also add to fragmentation.

**SWITCH**
A device for making, breaking, or changing a connection in an IED. A single switch can have multiple functions (e.g., arming and firing). The firing switch that initiates the IED explosive train determines the device type by category (command/time/victim operated). If present, the arming switch should also be categorized.

**INITIATOR**
Any component that may be used to start a detonation or deflagration. An initiator will be categorized as either a detonator or an igniter.

---

*All content sourced from the Improvised Explosive Device (IED) Incident Reporting Guide (2024).
**Alternative IED Definition (UNMAS 2016): A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components. Refers to a type of IED incident that involves a complete functioning device.
1 - Soft Target Protection

Introduction

Soft targets and crowded spaces remain attractive for terrorist plots involving improvised explosive devices (IEDs). In the *Security of Soft Targets and Crowded Places Resource Guide*, the Department of Homeland Security (DHS) defines soft targets as “locations that are easily accessible to large numbers of people and that have limited security or protective measures in place.”¹ These include critical infrastructure sites, such as power substations or transportation hubs, and more public sites such as event venues, shopping malls, houses of worship, and schools.

By nature, soft targets tend to be vulnerable to attack. Moreover, the impact of an IED on soft targets can be especially devastating. For example, a densely populated area with minimal security measures increases the impact of an IED detonation and lowers the chance of detection in the lead-up to an attack (e.g. during hostile reconnaissance) or prior to detonation. Many soft targets provide or facilitate the goods and services that serve as a key pillar of U.S. national and economic security and the well-being of the American people. The relevant stakeholder community is broad and includes the general public, site owners and operators, private industry like state, local, tribal, and territorial (SLTT) partners, and the federal government.

Threats and plots against these targets are on the rise as both international and domestic violent extremists have encouraged violence in densely populated areas and mobilization against infrastructure such as the energy, communications, and public health sectors.² Summarized succinctly in a recent DHS assessment, the threat against soft targets remains persistent and dynamic as terrorists “are constantly adapting their techniques to gain access to and potentially compromise these entities.” IEDs are commonly integrated into attack plots against these targets.

In order to bolster the resilience and safety of American communities, policymakers have underscored that the hardening and protection of soft targets are necessary, therefore immediate steps must be taken in preventing and protecting against future threats. Hardening in this context involves implementing measures to fortify vulnerable locations, making them more resistant to potential threats. Given the ubiquity of soft targets, efforts to resolve this issue face additional challenges of scale and feasibility. Solutions to persistent knowledge and capability gaps in this area must balance between maximizing the openness of local communities, the affordability and availability of needed resources, and the safety of the American people.

Challenges

There are multiple challenges that the domestic counter-IED (C-IED) mission community faces when attempting to protect U.S. soft targets and crowded spaces, and these influence where targeted research, development, test, and evaluation (RDT&E) initiatives can best support.

First is the limited nature of security inherent to these locations and traditional sites (i.e., schools, transportation centers, event venues, and open-air retail spaces). Many soft targets feature few physical obstacles to entry, multiple access and exit points, and limited infrastructure for identifying potential active threats. Security personnel tend to be assigned to such sites on an ad hoc, rather than permanent, basis.

Second, financial and operational concerns also affect the practical feasibility of protecting the numerous and varied soft targets vulnerable to a potential terrorist IED attack. The implementation of security measures can incur significant costs, particularly when necessitating physical alterations, augmentations to existing infrastructure, the engagement of additional security entities, or
training personnel. Relatedly, business owners, local government leaders, or site operators may not be able to rely on financial incentives such as funding, subsidies, or tax breaks to bolster the execution of recommended security enhancements.

Finally, weak coordination processes and information sharing present a persistent challenge to interagency and multi-sector collaboration. Insufficient coordination among agencies can impede effective action due to regulatory gaps and the ambiguous division of responsibilities, among other factors. Intelligence and law enforcement agencies might face legal constraints hindering their ability to divulge restricted information to operators of susceptible sites. Resultingly, at the operational level, potential misinterpretations might surface between site owners and users, local law enforcement and first responders, and community stakeholders.

**Key Operational Considerations**

Soft targets encompass a wide range of environments with varying levels of both physical and personnel security already in place. To improve prediction, deterrence, prevention, detection, and defeat capabilities of the C-IED mission community, it is helpful to consider the following operational considerations:

- A need for promising and best practices that may be systematically promoted among a wide range of SLTT stakeholders, business operators, and local communities for physical security around soft targets and crowded spaces.

- Solutions and best practices should be sufficiently flexible to be compatible with a wide range of location and environmental parameters.

- Deterrence, detection, disruption, and defeat measures developed for soft targets and crowded spaces should have minimal impact on crowd movements, be cost effective, and observe strict adherence to all relevant civil rights and liberties.

**Key Science and Technology Contributions**

Through the advancement of science and technology, the following are areas in which additional support from RDT&E can contribute to protecting soft targets:

1. Develop and validate a data framework and analytic model for forecasting potential soft target attacks based on location characteristics as well as relevant environmental conditions.

2. Develop a system for determining site-specific planning, protective, and response measures to prevent and minimize the impact of IED incidents.

3. Develop affordable, rapidly deployable, and scalable blast protection for high-risk and sensitive sites.

4. Research and share promising best practices for the improvement of public reporting of suspicious activities around soft targets through the National Suspicious Activity Reporting Initiative and related efforts.

5. Assessment of best practices in the incorporation of protective features and materials in architectural and environmental design.
Introduction

Combating the terrorist use of improvised explosive devices (IEDs) requires, at minimum, a foundational understanding of two key elements of the threat landscape: the attacker and the device. This means first characterizing the motivations, networks, and ideologies of the person(s) likely to perpetrate an IED attack in the United States. It also means identifying the persistent and emerging tactics, techniques, and procedures (TTPs) available to aspiring attackers.

In the United States, foreign terrorist organizations, homegrown violent extremists, and/or domestic violent extremists all share a similar motivation when conducting a terrorist attack: to cause destruction and/or disruption. This intent can be driven by a wide range of ideological agendas, grievances, and perceived relationship to the status quo. Despite these fundamental differences, terrorists’ use of IEDs has proved to be a point of commonality, a preferred tool. Instructions for the construction of IEDs and the call for their use are featured in radical Islamist publications, racially and ethnically motivated violent extremist channels, and anarchist violent extremist texts.

Violent extremists will continue to innovate, drawing on emerging technologies and creative problem solving to develop new methods of IED design and use. An improved and updated characterization of the IED threat landscape will enable authorities to identify potential attackers, improve efforts to anticipate attack methods, and respond more effectively.

Challenges

The terrorist actor landscape has become more complex. International terrorism remains a serious threat, while the U.S. domestic terrorism environment has become more fragmented, ideologically diverse, and geographically dispersed. The rise of seemingly lone offenders – those without a clear organizational or group affiliation – challenge efforts to identify, investigate, and disrupt IED attack plots. IEDs will continue to be seen as an appealing attack method across this diverse violent extremist milieu.

Different types of targets (e.g., public crowded spaces, the power grid, police stations, or election sites) will likely carry unique symbolic or practical value for different types of violent extremists. Some may focus on accelerating societal chaos, others on generating mass casualties. Of rising concern is the growing number of threats, plots, and attacks against U.S. public officials and elected representatives at all levels of government. Attention to an expanding attack surface will require efficient and effective targeting of resources by the domestic counter-IED (C-IED) community.

Despite the proliferation of IED attacks, the data and frameworks that exist to categorize and assess IED attack profiles are not standardized. Disrupting the IED attack chain (i.e., tactical adoption, operational planning, and attack execution) requires a robust understanding of how terrorists develop and spread new TTPs, source materials, and select targets. Some novel TTPs may originate from innocuous sources, such as chemistry textbooks or hobbyist communities, which presents additional monitoring challenges to authorities. Others may be inspired by major domestic or international terrorist incidents, such as the Boston Marathon bombing and the 10/7 Hamas
operation. The internet and social media have created ample opportunity for violent extremists to connect with like-minded individuals worldwide and disseminate tactics through messaging platforms and online images, videos, and publications.

Finally, many existing analytical approaches are based largely upon static models and frameworks that build on previously utilized terrorist methods. However, terrorists’ capacity for agility and innovation has proven capable of exploiting these cognitive biases. Thus, essential to understanding and anticipating the evolving IED threat, a flexible conceptual framework should be paired with a dynamic computational approach rooted in social and behavioral principles.

**Key Operational Considerations**

In today’s changing threat landscape, efforts to understand the underlying motivations, forecast novel and high-impact methods, and anticipate likely targets of IED terrorist attacks will require close attention to the following considerations:

- Historically, IED-related trends based outside the contiguous United States (OCONUS) have driven the nature and pace of C-IED research, development, test, and evaluation (RDT&E) initiatives in the United States. In so far as threats in OCONUS locations are distinct from those present in the U.S. homeland operational environment, or application constraints vary, there is a need to reevaluate the way in which knowledge products are prioritized and selected by U.S. law enforcement and first responders for continued RDT&E investments. Relatedly, distinct frameworks may need to be developed for specific operational environments.

- There is a credible risk that solutions will be dated quickly. To match the dynamic nature of the rapidly shifting IED threat landscape, there is a need for flexible tools and frameworks that can be updated or built upon to maintain an edge over anticipated novel or evolving threats.

- The capabilities should be sufficiently flexible and scalable to be usable across the C-IED community of interest including federal, state, local, tribal, and territorial policymakers, law enforcement, fusion centers, and first responders.

- Any frameworks or tools developed in response to this subset of knowledge and capability gaps need to integrate privacy protections and be compliant with all relevant legal authorities in all phases of design, development, and deployment.

**Key Science and Technology Contributions**

Key knowledge and capability gaps persist that inhibit identification and understanding, proactive action, and effective response. These include the need for a science-based assessment and anticipation of the evolving violent extremism landscape, the exchange of novel and evolving TTPs, and their implications for the future IED threat as evidenced in the activity of homegrown violent extremists, domestic violent extremists, and lone attackers. Specifically:

1. Research on the ideological, group, and environmental factors which shape terrorist tactical adoption of IEDs.

2. Research on international and domestic diffusion and adoption of IED-related TTPs, including on the internet and online networks such as social media, encrypted communication programs, and extended reality platforms.

3. Prediction of target selection and pre-attack staging areas based on observed behavioral patterns of violent extremists in both the contiguous United States and OCONUS.

4. A systems architecture for identifying and tracking potential and unknown threats relating to violent extremist use of explosives.
The increase in connectivity enabled by new technologies risks exacerbating long-standing challenges in combating RCIEDs. Signal disruption technology plays a pivotal role in countering potential remote commanded threats, but its effectiveness is contingent on being both portable and possessing sufficient range. Many scenarios require the ability to neutralize radio-controlled and Wi-Fi-connected devices remotely, necessitating portable jamming equipment. Furthermore, the range must be ample enough to provide security personnel with the capacity to safely render RCIEDs inoperable, mitigating potential hazards.

Historically, scientific efforts have focused on developing radio frequency jammers that would not disrupt critical telecommunications while remaining effective at standoff distances. However, the advent of internet-operable devices has added new dimensions to this mission. The ubiquitous presence of radio, Wi-Fi, and Bluetooth-connected devices in many U.S. environments further complicates the ability to isolate and target specific devices or networks without unintended disruptions. Therefore, the development of signal jamming technology capable of distinguishing between legitimate integrated technologies and potential threats is crucial to maintain the integrity of critical systems while effectively countering remote IED threats.
Outside of the issues inherent in signal detection and disruption, one of the most pressing challenges in combating RCIEDs is the steady expansion and rapid proliferation of accessible technology. Innovations in remote control and communication devices continually outpace existing countermeasures and solutions, making it difficult to keep up with emerging threats. Consequently, there is a pressing need for adaptive countermeasures that can keep pace with the ever-evolving tide of technology and terrorist TTPs, ensuring that dated solutions do not become obsolete and ineffective in the face of new, sophisticated threats.

**Key Operational Considerations**

To successfully combat RCIEDs, the potency of countermeasures hinges upon the portability and range of signal jammers, the delicate balance between effective communication and potential signal interference, the ongoing protection of secure communications and internet access, and compliance with telecommunications regulations and laws. These intricacies call for meticulous attention to safety, which can be accomplished through the following operational considerations:

- Portability and range of signal jammers may affect render safe operations at standoff distances.
- Communication operations must consider potential interference from any utilized signal jammers.
- Continued protection for Wi-Fi access in secure locations remains necessary to prevent malevolent actors from using the network to deploy RCIEDs.
- Collaboration with telecommunications regulations and laws.

**Key Science and Technology Contributions**

These pressing knowledge and capability gaps can be mitigated through the development of appropriate technologies and future-focused research plans. These efforts should encompass enhancing detection and neutralization capabilities, understanding the methods employed in managing threats, and assessing vulnerabilities stemming from the expanding use of connected devices. The following science and technology contributions collectively aim to bolster security and safety in an ever-evolving landscape of risks:

1. Research and develop systems for the detection and render safe of radio and internet commanded devices.
2. Research and catalogue known and anticipated methods of operating and connecting to cellular, Bluetooth, and Wi-Fi-enabled IEDs.
3. Research and catalogue the risks and vulnerabilities associated with the potential use of sensor-initiated devices commanded through the IoT.
4 - Unmanned Systems (UxS)

Introduction

One of the fastest-moving evolutions in the improvised explosive device (IED) threat landscape is found in terrorists’ use of unmanned systems (UxS) for the purposes of operational planning or the delivery of explosives in an attack. The term “unmanned systems” encompasses a range of autonomous or remotely operated systems, which often comprise a vehicle as well as a control platform and communication link. These are broadly categorized by their primary domain of operation, including unmanned aerial systems (UAS), unmanned ground systems (UGS), and unmanned maritime systems (UMS). UxS may be used to support IED attack planning through intelligence, surveillance, and reconnaissance or to deliver an IED.

The highly publicized surge in the use of armed UxS by militants and other armed actors in hostile environments abroad risks inspiring similar attempts by violent extremists based in the United States. Indeed, the threat has already materialized.¹ As technological advancements increase the operational range, payload capacity, and accessibility of commercial-off-the-shelf (COTS) unmanned systems, they become more susceptible to exploitation by violent extremists for planning operations and delivering explosives. Compounded by the concurrent advancement of other emerging technologies, such as additive manufacturing (AM), artificial intelligence (AI), and how-to tutorials available on the internet, the potential for terrorist use of UxS in attack planning and IED-based attacks presents a host of novel challenges to current security infrastructure and protocols.² A proactive response to this evolving security challenge requires a robust understanding of UxS design and use, target vulnerability, as well as the development of cost-efficient and effective counter-UxS technologies.

Challenges

The set of challenges related to the incorporation of UxS in IED attack planning and execution are vast and evolving. First, the nature of the UxS threat is widely acknowledged but remains understudied. Knowledge gaps around UxS-related terrorist tactics, techniques, and procedures (TTPs) inhibit effective mitigation and response. Due to their operational range and mobility and capacity for customization, UxS are well suited to circumventing physical barriers and other security protocols in numerous ways, presenting a credible threat to a variety of targets. Unencumbered by bureaucracy and regulations, violent extremists are often positioned to maintain an edge over the homeland security enterprise.

In the United States, while the threat is identified, counter-UxS infrastructure remains underdeveloped and poorly synchronized. Among the most daunting challenges are the difficulties that acquisition programs face in keeping pace with emerging systems and the slow development of regulations to ensure the safe use of commercial UxS. Countering a UxS-based attack requires the successful execution of a specific task sequence (i.e., “the kill chain”: detect, track, identify, and defeat).³ The status quo has produced a non-integrated set of tactical tools. No systems currently excel at all tasks, and integration of independent systems remains a challenge. Relatedly, many of the more mature counter-UxS technologies have been developed through military and defense initiatives and are therefore often not suitable for use in U.S. civilian spaces.
Key Operational Considerations

The prioritization of UxS and counter-UxS research and development is urgent and important. This includes addressing critical knowledge and capability gaps relating to the intersection of the UxS and the explosives threat. These considerations include:

- The suite of UxS and UxS-related technologies is expanding at a pace that can quickly date or exhaust efforts to identify, categorize, and assess their potential for exploitation by U.S.-based violent extremists.

- The risks related to UxS use in IED attacks in the United States may differ from the patterns of malign UxS use in hostile environments outside the contiguous United States (OCONUS). This includes unique supply-chain constraints and local availability of device materials.

In addition, it is imperative that systems and procedures be developed to safely deter or disrupt UxS from reaching their targets and/or deploying an IED. A single-system approach is unlikely. Instead, counter-UxS infrastructure will likely come to rely on a suite of integrated components as different kinds of systems are better at handling different elements of the kill chain. Violent extremists will likely innovate when faced with new counter-UxS technology and methods, making a single-system solution a costly liability. Other key considerations include:

- To be viable and sustainable, a counter-UxS approach must be cost effective.

- Counter-UxS efforts will likely require a variety of technologies and key enablers to yield their full potential. This may include communication networks, data management systems, artificial intelligence, and information dissemination platforms to deter, detect, and defeat UxS and maximize the utility of the data collected from intercepted systems.

- Tools developed for the defeat of identified UxS threats should be made in such a way that they can navigate population-dense environments in accordance with constitutional rights and privacy laws.

Key Science and Technology Contributions

Unfortunately, as UxS attack methods are highly dependent on the requirements of each individual and their specific attack type, minimizing the threat from these systems must include scenario and horizon scanning techniques; these techniques try to identify methods that could arise from the development and adoption of new technologies. Science and technology can contribute to the development of advanced assessment and diagnostic tools and techniques in the following areas:

1. Research on how autonomous unmanned vehicles and remotely controlled unmanned vehicles may be used to support or conduct IED attacks. This assessment would benefit from a comparison of overlap and points of distinction between these UxS categories.

2. Development of future-oriented methods, such as forecasting and horizon scanning, for identifying likely technologies, targets, and tactical design in UxS-based attacks.

3. Development of detection systems for UxS-borne IEDs. These should also be capable of communication and/or integration with co-located defeat systems.

4. Research on promising best practices for safe protection against and response to UxS-based attacks for public safety bomb squads, first responders, and law enforcement.

5. Development of systems for the safe defeat of explosives-laden UxS, including remotely commanded IEDs, under a wide range of environmental conditions.
ways. Considering the readily available nature of precursor chemicals and the information required for HME production, the risk of terrorist attacks involving IEDs within the United States remains.

IEDs are often constructed of materials widely commercially available in brick-and-mortar and online outlets. Bomb-making materials may include metal pipes, pressure cookers, exploding targets, single-board computers, electronic matches for detonation, or commercial-off-the-shelf (COTS) quadcopter aerial drones. The ease of access and general affordability of these products and technologies expands the terrorists’ capabilities even without specialized training.

**Challenges**

The ongoing fight to combat terrorists’ use of explosive precursor chemicals and bomb-making materials faces numerous challenges, some of which may be resolved through targeted RDT&E initiatives. A critical component of evaluating the current threat of IEDs is identifying trends in the materials and devices used by bombers. These efforts are limited by the inconsistency of publicly available data and lexicons. Necessary information is rarely publicly available, generally incomplete, and poorly structured for cross-case comparison. The data available for the purposes of this report are limited due to several factors:

- The data are voluntarily reported to the Department of Justice (DOJ) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) from state and local law enforcement and, therefore, may not provide a complete representation of related incidents.

Explosive precursor chemicals (i.e., chemical substances that can be used for legitimate purposes, but can also be misused to manufacture explosives) are commonly used in the production of homemade explosives (HMEs). Due to their widespread range of legitimate uses, precursor chemicals can be obtained legally from brick-and-mortar retailers (e.g., hardware, drug, and garden supply stores) or online.

These chemicals are described in-depth in the 2018 National Academy of Science report, *Reducing the Threat of Improvised Explosive Device Attacks by Restricting Access to Explosive Precursor Chemicals*, and include ammonium nitrate, nitromethane, sodium nitrate, potassium nitrate, sodium chlorate, potassium perchlorate, nitric acid, and hydrogen peroxide. Although chemical precursors typically used in IEDs have not significantly changed over time, they continue to be combined in novel combinations.
Solutions should take the following operational priorities into special consideration:

- Testing and red teaming new ways that known precursor chemicals and bomb-making materials may be maliciously employed.
- Addressing the wide availability of precursor materials and the “know-how” needed to make IEDs.
- Strengthening the regulatory framework, including the enhancement and enforcement of U.S. laws regulating the security of explosives and their precursors.
- Supporting voluntary programs enhancing industry’s ability to detect, report, and prevent the nefarious acquisition, theft, or diversion of explosives and other bomb-making materials.
- Gathering and disseminating information to prevent or respond to terrorist incidents.
- Minimizing the burdens on legitimate commerce and commercial use.

Key Operational Considerations

There are numerous ways by which would-be attackers may gain access to dangerous precursors and materials. Proactive identification of explosive precursor chemicals will help detection if there are new derivatives of known chemicals already used. Many materials used in IED construction are themselves inert and serve non-malicious needs for the majority of users; therefore they are more difficult to restrict. The list of potential “dual use” products is immense and requires a systematic, regular cadence of categorization and prioritization.

Despite training and awareness programs, local stakeholders, retailers, store operators, and staff may be ignorant of what signs to look for in customer purchases of explosive precursors. Knowing what to report is critical in identifying potential threats. While this is a challenge for brick-and-mortar outlets, online sales present unique challenges as the mechanisms for monitoring, regulating, and reporting online purchases are difficult; furthermore, malign actors have demonstrated their capacity to adapt their methodologies in response to regulatory measures targeting specific materials.

Key Science and Technology Contributions

Science and technology can contribute to the development of actionable analytic frameworks and advanced assessment tools and techniques in the following areas:

1. Identify and quantify a list of explosive precursor chemicals that have been used or are susceptible to use in IEDs through defensible testing.
2. Identify and analyze the movement of priority precursor chemicals and bomb-making materials through commercial outlets and develop effective control strategies.
3. Develop a systems architecture capable of addressing the known HME threats and extending the system to materials of future threats.
4. Develop an easy reporting tool for commercial manufacturers to report incidents of excessive precursor purchases.
5. Research, develop, and validate evidence-based guidelines, training, support, and informational tools for commercial manufacturers about precursor chemicals purchases.
6. Identify and evaluate existing control measures, in the United States and internationally, for the priority precursor chemicals, including vulnerabilities in the existing framework of voluntary and regulatory controls.
7. Research best practices in preventing the acquisition of explosive precursors and bomb-making materials purchased online.
**Introduction**

The democratization of emerging commercial technologies has come at an increasing rate over the past 15 years and is expected only to continue. The immediate concern is specific to commercial off-the-shelf (COTS) technologies, which are highly accessible to the public and may be put to malevolent use with relative ease. Many emerging technologies have the potential to be used throughout all phases of the attack cycle, from planning an attack to conducting an attack to posting within virtual communities about a successful improvised explosive device (IED) operation.¹

The malign use of emerging technologies provides feasible means of novel IED design and employment. Among others, the set of commercial technologies that may amplify the terrorist IED threat include: unmanned systems (UxS), extended reality, artificial intelligence (AI), additive manufacturing (AM), 6G networks, and single-board computers and microcontrollers. As these become more affordable, more reliable, and widely available, the threat they present will only become more pervasive.

Some emerging technologies provide violent extremists with enhanced methods of communication and coordination. Extended reality technologies and related online environments, such as the metaverse and digital twins, can be used by violent extremists to recruit new members, disseminate and improve tactics, or plan and coordinate operations. This concern grows as online communication platforms are enhanced and broadened to share knowledge faster and replicate face-to-face interactions.

The amount of information available through online platforms is likely to increase the information that may be integrated into AI and machine learning applications. Generative AI tools such as ChatGPT, DALL-E, and other programs based on machine-learning models may be used to easily gather and synthesize information without having to sort through multiple sites. Thus, AI-based programs may provide violent extremists with new tools for the development of novel homemade explosives, identification of target vulnerabilities, and design of operations.

Rapid advancements in AM, i.e., the process of creating a three-dimensional (3-D) object by building up a series of successive layers of material(s) over time, are a key part of the evolving IED threat landscape. Recent efforts have demonstrated the possibility of using 3-D printing to create energetic materials related to explosives, propellants, and pyrotechnics. Logistically, AM may reduce time sensitivities, provide opportunities for rapid prototyping, and develop device boosters completed in an operationally secure environment circumventing current prevention barriers.² AM may also enable terrorists to develop novel IED containers and other device components in an affordable and discreet manner.

The growing knowledge and use of microcontrollers (e.g., Arduino Uno) and single-board computers (e.g., Raspberry Pi) present a worrying new means of device construction, with disquieting implications for their application. They provide a low-cost, easy way for novices and experts alike to construct IEDs that interact with motors and sensors. Moreover, the legal online exchange of information among hobbyists...
"is a growing avenue through which individuals and groups with malign intent may become sufficiently knowledgeable and skilled in their use with relatively little cost or time."³ This underscores the critical need for a core competency to be advanced within the counter-IED (C-IED) community, i.e., to develop research, prediction methods, and mitigation techniques related to evolving threats connected to emerging technologies.

**Challenges**

It is difficult to know what the limits and capabilities of the technology are prior to its use in an attack. New commercial technologies are created to help solve consumer problems, but malign users may also find novel ways to use the technology for their own benefit. To support a proactive counter posture, one main challenge is to predict which emerging technologies will be co-opted by violent extremists in the future – and how. Relatedly, a second challenge lies in identifying early markers of malign use. Rigorous horizon scanning, red teaming, and other future-oriented methodologies can be useful in this regard. Monitoring and regulating emerging technologies should be considered throughout the development process so that guidance and misuse discourages terrorist innovation.

**Key Operational Considerations**

Combating the impact that new technology can have on the attack process requires input across the C-IED community from public safety bomb technicians to commercial manufacturers to researchers and policymakers. To that end, the following should act as special considerations:

- Need for frameworks that accurately identify which emerging commercial technologies are most likely to be incorporated into terrorist attacks and plots involving IEDs.
- Red teaming of possible malign applications of emerging technologies and integration into training scenarios for bomb squad technicians, first responders, and law enforcement.
- Efforts to proactively mitigate these threats may benefit from close coordination with the developers, manufacturers, and retailers of emerging commercial technologies.
- Engaging commercial manufacturers, researchers, and practitioners across all phases of technology development can be used to identify risks and ways to mitigate them.
- Amplifying the amount and attention given to regulatory frameworks within the technology itself.

**Key Science and Technology Contributions**

Research and scientific efforts offer tools needed to maintain a proactive posture against these potential evolving threats:

1. Research on how the metaverse, gaming, and extended reality technologies may shape terrorist attacks.
2. Research on how single-board computers and microcontrollers may facilitate new methods of IED construction and attack planning and execution. This includes integration of IEDs with the Internet of Things (IoT) and 5G or 6G telecommunications networks.
3. Research on the threats presented by the application of AM tools to the construction and use of IEDs.
4. Research on how AI and machine learning may be leveraged to improve terrorist tactics, techniques, and procedures (TTPs); develop explosives and IEDs; select targets; and carry out attacks.
5. Research on enabling operators’ mitigation and defeat capabilities for emerging technologies.
6. A systems architecture for identifying and tracking potential and unknown threats relating to violent extremist use of explosives, including IEDs used in foreign environments as a predictor for what tools and technology may be used in the future.
Introduction

For most terrorist organizations and violent extremist actors, the improvised explosive device (IED) has become a weapon of choice. The preemptive disruption of IED plots is paramount. A key to achieving this end is the detection of explosives and devices both at standoff distances and screening checkpoints. Advancements in the development of technology for the detection of explosives through research, development, test, and evaluation (RDT&E) initiatives can greatly enhance efforts to proactively mitigate the impacts of an IED incident.

As the IED threat evolves, so does the detection mission area. The persistent problem of detection is complicated by many factors, including: a wide variety of explosives, both homemade explosives (HMEs) and commercial explosives; multiple possible modes of delivery such as pipe bombs, pressure cookers, person-borne (PBIED), and vehicle-borne (VBIED); and diverse detection environments such as screening checkpoints or standoff. In addition, recent trends indicate a broad target profile comprising public officials, government buildings, transportation hubs, universities, retail venues, power substations, and health care facilities.¹ As a result, the scale of presence and vigilance required for effective detection is growing.

The problem of IED detection can be split into two operational categories: (1) checkpoint screening applications, wherein the detection system occupies a fixed location and observes persons, objects, and vehicles passing through the checkpoint for evidence of an IED; and (2) applications that may be needed to detect an IED at various distances.² Knowledge and technological advancements in counter-IED (C-IED) detection and related screening approaches remain a pressing operational need.

Challenges

The persistent challenges and tension of explosives detection are rooted in the variety of explosives, devices, and operational environments that may characterize terrorist IED plots. There is little hope of a one-size-fits-all solution, but it is also infeasible to field and maintain an unlimited number of bespoke detection technologies. The wide range of HME materials, and their availability in commercial spaces, makes their detection an especially difficult problem.

The detection of explosives or IEDs hidden in vehicles or various types of bulky containers – both at checkpoints and at a standoff distance – presents unique challenges. Because many concealment and container materials are metal, HMEs are difficult to detect with technologies currently in the field.

Person-borne IEDs are typically employed by terrorists where large concentrations of people congregate, such as at major entertainment events, airports, or shopping malls. The presence of a crowd makes the detection problem more difficult due to clutter and possible interferences. The challenge unique to PBIEDs is the need for detection before the bomber is in a position to initiate and with enough time to allow an effective response. The problem is further complicated by the fact that PBIEDs are usually concealed.

At checkpoints, existing detection tools are often used in a relay system without a unified mechanism for detection. Thus, in addition to creating new capabilities and enhancing existing ones, there is a need to integrate relevant capabilities to provide a more comprehensive approach to explosives detection. Because no detection technology can perform flawlessly, the use of multiple complementary detection methods may improve overall detection
system capabilities. Relatively, a consistent obstacle to effective detection is the transition of technological tools developed in controlled or laboratory settings to the field.

**Key Operational Considerations**

Solutions to detection and screening needs should be guided by the following operational considerations:

- Solutions to standoff detection of IEDs should provide security personnel with the ability to detect explosives at a sufficient distance safely for both the operator and public, to a reasonable degree of certainty, and in sufficient time, to allow reasoned decisions to be made and effective actions to be taken to safely deal with the threat.

- Solutions to the detection of HMEs should provide a capability to detect HMEs and their precursors in a variety of venues and situations.

- For use at a security checkpoint, the technology must be adaptable for use by people who have not received advanced training.

- In cases of a PBIED in a crowded space, solutions must be able to detect the device without impeding pedestrian traffic flow.

- For mobile standoff detection, applications should be compact enough to be transported on a bomb squad response vehicle or trailer, require minimal effort to set up and operate, and have a small footprint.³

- Solutions should require minimal training to operate and maintain safe procedures for using developed equipment and must be cost effective.

- The technology should be sufficiently adaptable to address the evolving and emerging nature of the threat.

**Key Science and Technology Contributions**

Science and technology should support the development and testing of explosives detection solutions to standards that meet the requirements of end users at the federal, state, local, and tribal levels of administration. The technological solutions should be designed to be integrated into current tactics, techniques, and procedures. Among the key contributions that may be provided by investments in science and technology are:

1. Detection of trace involatile threat materials (e.g., inorganic species and mixtures) under a wide range of environmental conditions.

2. Improved capability in rapid standoff detection of PBIED and VBIEDs across the threat spectrum (i.e., in noisy environments, in crowded environments, and under extreme time limitations) so that both the operator and target remain outside of the hazard zone.

3. Development of standoff methods of detecting explosives residues deposited on a vehicle or individual.

4. Mobile sampling and detection systems provide rapid, accurate detection of an IED threat under a wide range of environmental conditions.

5. Unified system integration of distinct detection methods and technologies, especially at screening checkpoints.
Introduction
A swift and cohesive emergency response to an improvised explosive device (IED) incident holds the power to steer the course of an unfolding crisis. An IED incident includes any event that involves a real or suspected IED threat, including IED detonations, bomb threats, the use of hoax devices, discovery of bomb-making components, or the theft of explosives or precursor materials.¹ The incident response community may include law enforcement, canine detection teams, public safety bomb squad units, emergency first responders, site owners, and the local community. Considering the complexity and consequence of emergency response operations, maintaining a common operating picture is key for both safety and success in the event of an IED incident.

Incident response involves rapidly deploying resources and personnel to minimize harm and bolster security in the face of unexpected crises. The scope of needs and responsibilities associated with response to IED incidents often transcends organizational boundaries and jurisdictions, necessitating cross-functional collaboration among multiple response units. Without clear communication and coordination – prior to, during, and in the aftermath of an IED incident – a response team risks being ineffectual or exacerbating any second order negative impacts of the incident.

The ability to make well-informed decisions and quickly act upon them is a linchpin of successful incident response. Thus, establishing an infrastructure for information sharing and team responsibilities prior to a crisis can strongly influence the success of response efforts. As part of a well-coordinated infrastructure, an adaptive and proactive response plan is crucial for protecting both the public and incident response personnel. An adaptive response plan should provide guidance for roles and responsibilities for all response units before, during, and after an incident has occurred, while still being responsive to needs and developments on the ground. In addition, it should be ensured that response unit capabilities meet the needs of the jurisdiction as related to appropriate allocation of equipment and personnel.

Challenges
Efforts to respond to IED incidents face a series of challenges. First, as emergencies often involve multiple levels of government, lack of coordination among units from different agencies, jurisdictions, and specialties can severely hinder the speed and success of response operations. The challenge of coordination is multiplied by the need for both preemptive security planning and decisive post-incident cooperation between disaggregated units. This can be addressed, in part, through joint multi-unit scenario-based training initiatives, but these are often limited by cost, time, and planning constraints. Because of this, it can be difficult to provide combined response units with adequate experience in responding jointly to explosion incidents. These challenges are compounded when different response teams employ distinct communication systems, processes, and tools.

Related to coordination is the persistent challenge of distance between top-level decision-making and on-the-ground implementation of response efforts. Frequently, multiple response agencies establish mutual aid agreements to provide assistance when an incident escalates. These agreements are intended to prevent an incident from overwhelming a single agency by promoting integrated cooperation. Yet, the risk of disconnect between strategy and execution can hamper the development of effective response plans.
Finally, despite improvements in data and forecasting models, the unpredictability of crises remains one of the greatest barriers to response efforts. A major challenge in incident response planning lies in creating an adaptive transition between general security protocols and specific post-incident action plans. An adaptive transition plan should consider, for example, realistic human behaviors in the aftermath of an attack. It should also account for dynamic decision-making based on real-time information and available resources to provide harm reduction and care for the affected. Consideration of these issues in incident response planning will provide improved situational awareness and help streamline coordinated response efforts.

**Key Operational Considerations**

Effective operational planning requires a seamless connection between strategy and implementation, emphasizing the need for best practices that are both comprehensive and adjustable. These practices should serve as a bridge between high-level strategic objectives and the on-the-ground execution of operational plans. Flexibility is key, as conditions can vary widely, and a rigid approach may prove ineffective. By developing proactive best practices and adaptable response plans, organizations can navigate diverse situations while ensuring a coherent alignment with strategic goals. The following specific operational considerations should be taken into account:

- It is essential to design solutions that not only improve coordination and communication capabilities between different agencies or jurisdictions but also avoid exacerbating disconnect within response teams.

- When assessing and diagnosing situations, it is encouraged to employ approaches that can be readily understood and applied by responders without an extensive scientific or technical background.

- Empower responders to make informed decisions by enhancing information sharing of best practices, which will better enable rapid and effective response in emergencies. These practices can be employed during training to ensure adequate preparation and troubleshoot potential issues.

- Improve technical exploitation of possible IED technologies to better inform operators during render safe operations.

While simulation and training programs are valuable tools for preparedness, their effectiveness depends on their relevance to local response cohorts. To ensure practicality, these programs should make use of the actual teams and tools available locally. By tailoring simulations to the specific context, responders can hone their skills and be better equipped to handle real-world scenarios. Training evaluations can be further enhanced by incorporating informal after-action reviews while all agencies are present. Lessons learned from these training sessions can be implemented in future exercises, significantly improving future responses.

Ultimately, preserving the safety of the local community and first responders is the main imperative of successful response operations. An important consideration for response safety lies in mitigating second-order harm in the aftermath of an IED detonation. This entails a comprehensive approach that not only addresses the immediate impact but also anticipates and minimizes the potential cascading effects, such as secondary explosions, structural damage, or environmental hazards. To further reduce harm and improve safety for first responders, the tools employed for render safe and bomb disposal must possess a high degree of adaptability for countering emerging threats. Adaptability in this context involves not only the capacity to handle diverse explosive devices but also the capability to integrate advancements in detection and disposal methods. As the nature of threats and technologies evolves, proactive innovation in render safe tools will be paramount to maintaining the effectiveness and safety of response operations.
**Key Science and Technology Contributions**

Reimagining the future of emergency response structures is critical, especially when addressing the societal and economic costs associated with incidents involving improvised explosive devices. Science and technology contributions of notable value may include:

1. Intelligent quick decision-making support tools to facilitate effective and safe mitigation of IEDs found in a variety of environments.

2. Analytic models of human crowd behaviors during and after an IED attack.

3. Development of evidence-based frameworks and tools to strengthen and/or reimagine IED-incident response structures, focusing on enhanced communication and coordination of response capabilities to reduce the societal and economic costs of IED-related incidents.

4. Development of an information sharing system to disseminate real-time relevant event and risk information at appropriate classification levels.

5. Research on promising and best incident response practices across different operational environments (e.g., rural versus urban), including those that may minimize negative second-order effects in the immediate aftermath of an IED incident.

6. Research in innovations for bomb technicians to adequately render safe and maintain forensic data.
Introduction

Coordinated action is imperative to successful counter-improvised explosive device (C-IED) operations. Swift, unhindered information sharing between state, local, tribal, and territorial (SLTT) operators, first responders, and federal agencies is the first step in countering IEDs. Effective sharing of critical incident information is crucial. It not only enables safety personnel to be well-informed and prepared but also contributes to the prevention of future incidents. However, challenges arise due to the classification and sensitivity of much of this information, leading to limited sharing with non-law enforcement partners. Considering the lack of a central repository for critical information sharing, the current arrangement of multiple information sharing systems, each with distinct membership and classification standards, further complicates the process and can lead to information silos.

Efficient sharing of timely information is imperative for the rapid detection and prevention of similar incidents across sectors, which necessitates better communication between researchers and policymakers. Overcoming the tendency for interagency communication to be slow and compartmentalized is necessary to combat information silos that inhibit productive research, development, test, and evaluation (RDT&E) efforts in this arena. The capability gaps inherent in the current information sharing system highlight the complexity of information sharing challenges and the need for systematic knowledge capture, interagency lexicons, and the sharing of best practices outlined in the science and technology contributions section to come.

Challenges

Varying levels of classification and a multitude of information sharing platforms make for a broadly inaccessible and disorganized means of disseminating critical information across the C-IED mission space. Therefore, the first challenge to cohesive interagency communication lies in the overclassification of IED-related information. The current system of classification creates barriers to sharing with non-law enforcement partners and relevant community stakeholders, limiting the scope of comprehensive IED prevention efforts. To prepare adequately for potential attacks, first responders and public safety bomb squad technicians require timely access to the most up-to-date IED incident information.

Further complicating the situation, various government entities operate multiple information sharing systems, each with distinct membership and classification standards. These fragmented systems often result in overlapping or redundant data, making it difficult to assess the relevance and timeliness of shared information. Additionally, conflicting jurisdictions within the C-IED mission space have resulted in information silos where information does not flow smoothly among relevant entities. The presence of numerous separate entities collecting information also leads to a multiplicity of effort, wasting resources on duplicative activities and undermining their effective allocation.
Key Operational Considerations

To address these challenges, several key operations must be considered. Quick and up-to-date sharing of recent IED event information among interagency law enforcement and other first responders is the most pivotal requirement for enhancing the ability of various sectors to detect and prevent similar incidents. A collaborative approach is essential in fostering information sharing, increasing accessibility, and combating information silos. To this end, internal communications should be downgraded, and classification specifications should be re-evaluated to ensure that information is available to all relevant members of the C-IED community.

To further facilitate effective and collaborative action, information should be funneled through the existing infrastructure to other stakeholders, site managers and owners, and community members when possible. The national network of Fusion Centers, for example, may be relied on to facilitate more frequent updates on the state of the field and recent event data. Timely and unclassified information sharing to community stakeholders and partners through other collectives, such as Joint Terrorism Task Forces (JTTF), should be encouraged.

Key Science and Technology Contributions

In the pursuit of bolstering security through collaborative efforts, a holistic approach should encompass the systematized collection and sharing of IED-related information, foster shared understanding through a common interagency lexicon, and facilitate information exchange with industry leaders. To enhance preparedness and the effectiveness of C-IED operations, adoption of the following collaborative approaches is urged:

1. Development of a platform for the systematized knowledge capture and collection of IED-related information in a centralized, online, tiered-access system available to government and industry stakeholders.

2. Establishment and management of a common interagency lexicon related to IED technical categorization and tactical characterization.

3. Information sharing of best practices around recognizing and responding to suspicious activity with key business and industry sector leaders.
Introduction

Countering the use of improvised explosive devices (IEDs) requires identifying and understanding the knowledge and capability gaps that may be present within local public safety and first responder units. This practitioner community includes public safety bomb squads, detection canine units, emergency medical services, firefighters, police, and other security personnel – all of whom must work together to detect, render safe, and respond to an identified threat or incident. Ensuring that all units are prepared to engage in this effort can be supported through a process of assessing units’ needs, providing and updating training, and evaluating units’ performance. This continuous cycle helps to guide broader strategy as well as coordinated action during a threat response, as performance can be monitored over time and skills and knowledge can be updated based on previous performance.

Regular assessment provides the foundation to equip the counter-IED (C-IED) mission community with the knowledge and skills they need to remain effective. Assessments identify a unit’s needs by determining training and knowledge gaps, along with how units work together, and use tools to generate a current picture of what processes can be improved upon. Assessing capabilities can include a unit-level assessment, whereby subject matter experts use multiple datapoints to determine overall preparedness and readiness to combat IEDs.¹ This helps to determine what tools, personnel, and training gaps may exist and can be improved. In addition to external assessment, local unit leaders and commanders can assess their teams internally to determine immediate needs and how they can be resolved.

Training may be identified as a need following internal and external assessments. To safely and effectively combat IEDs, training is designed to enhance knowledge and skills around the tasks needed for prevention, detection, defeat, and response to IED threats. During active IED incidents, training is designed to improve overall success and performance. Different forms of learning, including direct recall of information pertaining to concealment of IEDs, exercising applied skills by completing simulations using inert IEDs, and practicing render safe skills, can all be involved in training. Monitoring which skills should be trained is important, as it is necessary to determine what is needed to safely defeat IEDs. Training should be completed at all levels – including the individual, unit, and broader response teams – so all are aware of what processes need to be completed and how best to achieve a safe outcome.

The evaluation of C-IED practitioner, public safety, and first responder units is the final step to ensure maximum operability. Without benchmarking and reviewing successes or failures within and across units, growth and need fulfillment is inhibited, and training cannot be determined to be successful. Evaluation consists of measuring how the implementation of training and new tools helps to promote success. Evaluations should be standardized and based off national training standard operating procedures (SOPs) of bomb squad units and local jurisdictions involved in IED response. Records regarding training, simulations, and other metrics such as time of response, successful render safe, number of injuries, and tool use should be maintained and used for comparison over time to gauge if the procedures, knowledge, and training in place are effective and efficient. Together, regular cycles of assessment, training, and evaluation can have significant progress on defeating IEDs, as all first responders will be prepared to act.
Challenges

Numerous challenges exist when implementing more advanced assessment, training, and evaluation standards. The threat environment around IEDs is constantly changing. Therefore, staying ahead of the curve on the needs of public safety bomb squads and emergency service teams can be hard if threats are unknown. Continuously updating assessment and training standards is difficult when the threat is present but does not occur at a regular cadence. Also, each bomb squad has its own unique capabilities and may not meet all national standards, such as smaller squads that may not have the personnel power to engage in simulations or new training based on anticipated events.

To remain agile, first responders often engage in specialized and continuous training. Since first responders receive limited skill performance through real-life events, training in simulations of scenarios likely to occur can prevent knowledge decay by allowing bomb squads and first responders to practice skills and decision-making. Engaging in re-skilling and training events outside of large simulations also can prepare first responders to navigate the current threat environment. However, consistent training is not always available to all, as it requires both finances and time. For teams short on both, engaging in continuous training is challenging, and this can impede their ability to refresh basic skills and learn new ones based on the current threat environment.

The National Bomb Squad Commanders Advisory Board (NBSCAB) has set up nationally recognized training standards for all bomb squad members. Similarly, the Academy Standards Board (ASB) and American National Standards Institute (ANSI) have released standards for selecting, training, and certifying detection canine partners. These standards outline required, optional, and continuous training that canine teams must complete to maintain their certification. National standards indicate operators must undergo continuous training while they are working, but based on the tools available and specific capabilities of each jurisdiction, this training is not always completed or done to its fullest extent.

Additionally, although these standards are in place and should be universally adopted by units depending on the operating capabilities and resources available to the units, they may not always be adopted by all units. In terms of procedures and processes used during an active threat, not having universal adoption impedes having responders on the same operational baseline.

Another challenge tied to training is the financial cost. Training requires personnel to take time off, in addition to costs associated with sending operators to train. One of the largest financial contributions comes when bomb squads and other first responders engage in IED simulations. Simulations are cost prohibitive as they require personnel to not be working, tools to be used, and real-life scenarios using actors to be set up, requiring coordination and time commitments from all units present. To limit costs, multiple jurisdictions can work together in simulations to not only train but identify and assess their preparedness and potential gaps. When simulations can be used, they are a tool that can help prevent knowledge decay, but since they are expensive, simulations cannot be completed regularly.

Metrics measuring the outcomes of active threats (e.g., successful diffusion, time it takes to diffuse, if there were injuries, etc.) need to be standardized and updated regularly. Keeping a running record of these outcomes aids the evaluation process and helps determine future needs related to processes, tools, and personnel. Monitoring trends in the use and deployment of IEDs can also be done when record keeping is improved, underscoring the robust utility that metrics hold. Incorporating standardized reporting metrics will guide public safety bomb squads and first responder programs to use objective data to update what needs and competencies are required and how future performance can be enhanced.
Key Operational Considerations

The continuous cycle of assessment, training, and evaluation will guide first responders and bomb squad operators to ensure maximum performance. Having updated procedures and training will help prepare units to tackle IED incidents that are common but also future-oriented. Assessment, training, and evaluation efforts should be designed with the following considerations in mind:

- Need for updated training protocols and timelines to aid knowledge retention in the field.
- Training on future threats when doing simulations and continuous training to further develop decision-making skills.
- Assessment of training standards for all first responders to evaluate coordination and decision-making during joint incident responses.
- Creation of lifelike simulations to promote training that can help responders identify areas where they are proficient or not proficient.
- Objective selection and qualification protocols for those who will be on the bomb squad and operating equipment.
- Integrated systems to monitor and evaluate successful diffusion of IED-related events at the local and state level, to inform success rates and track progress.

Key Science and Technology Contributions

Implementing a consistent cycle of assessment, training, and evaluation begins with conducting research and analysis on the most critical knowledge and skills needed in an active threat. The following are some of the areas in which targeted research, development, test, and evaluation (RDT&E) may best support the future C-IED mission community:

1. Standardized assessment, training, and evaluation protocols for public safety bomb squad units, local law enforcement, and other first responders, including joint simulation exercises, continuous training, and scenario planning.
2. Reinforcement of a scientific basis for canine detection training and evaluation programs and uniform training protocols, including canine selection, initial introduction to scent, proper storage and handling of precursors used for training to avoid cross-contamination, performance upkeep, novel containers, and added threats.
3. Development and implementation of continuous training standards and protocols beyond initial training that reinforce key procedures and maintain knowledge, skills, and abilities, and are used at a set cadence between performance periods and re-certification.
4. Continued development and testing of evaluation and guidelines standards, including timelines for when training programs and materials, such as those for detection canine and public safety bomb squad teams, should be re-evaluated and updated.
5. Development and qualification of chemical precursor training aids, including validation of surrogates, that can be used safely to improve detection and response performance without exposing users and the public to hazards.
CONCLUSION

The persistent use of improvised explosive devices (IEDs) by terrorists poses an ongoing and serious threat to U.S. homeland security. The challenges in combating this threat within the United States are exacerbated by persistent and emerging knowledge and capability gaps across the counter-IED (C-IED) mission community. The scientific community is positioned to address these operational challenges through targeted research, development, test, and evaluation (RDT&E) initiatives. This report serves as the guide to critical needs to coordinate and deconflict interconnected RDT&E efforts across the U.S. government, focusing on the identification and prioritization of knowledge and capabilities crucial for disrupting future IED attacks, protecting vulnerable targets, and efficiently responding to IED incidents.
APPENDIX A

List of Acronyms

- 3-D: Three-dimensional
- AI: Artificial intelligence
- AM: Additive manufacturing
- ANSI: American National Standards Institute
- ASB: American Standards Board
- ATF: Bureau of Alcohol, Tobacco, Firearms and Explosives
- CBP: Customs and Border Protection
- C-IED: Counter improvised explosive device
- CISA: Cybersecurity and Infrastructure Security Agency
- COTS: Commercial-off-the-shelf
- DHS: Department of Homeland Security
- DOD: Department of Defense
- DOJ: Department of Justice
- DTRA: Defense Threat Reduction Agency
- FBI: Federal Bureau of Investigation
- FEMA: Federal Emergency Management Agency
- FLETC: Federal Law Enforcement Training Centers
- HDIAC: Homeland Defense & Security Information Analysis Center
- HQ: Headquarters
- HME: Homemade explosive
- IC: U.S. Intelligence Community
- IED: Improvised explosive device
- IoT: Internet of Things
- JTTF: Joint Terrorism Task Force
- NBSCAB: National Bomb Squad Commanders Advisory Board
- NCITE: National Counterterrorism Innovation, Technology, and Education Center
- NGIC: National Ground Intelligence Center
- NSD: National Security Division
- NSRI: National Strategic Research Institute
- NYPD: New York Police Department
- OCONUS: Outside of contiguous United States
- OBP: Office for Bombing Prevention
- PBIED: Person-borne improvised explosive device
- PSA: Protective Security Advisor Program
- RCIED: Remotely commanded improvised explosive device (also: Radio-controlled IED)
- RDT&E: Research, development, test, and evaluation
- SLTT: State, local, tribal, and territorial
- S&T: Science and Technology Directorate
- SOPs: Standard operating procedures
- TSA: Transportation Security Administration
- TTPs: Tactics, techniques, and procedures
- UARCs: University Affiliated Research Centers
- UAS: Unmanned aerial systems
- UMS: Unmanned maritime systems
- UGS: Unmanned ground systems
- USSS: U.S. Secret Service
- USCG: U.S. Coast Guard
- USPIS: United States Postal Inspection Service
- USPS: United States Postal Service
- UxS: Unmanned systems
- VBIED: Vehicle-borne improvised explosive device
APPENDIX B

Glossary of Terms*

Commercial explosives:
• Explosives produced and used for commercial, industrial, or recreational applications.

Explosion:
• A nuclear, chemical, or physical process leading to the sudden release of energy.

Explosive compounds:
• Homogeneous substances whose molecules contain within themselves the oxygen, carbon, and hydrogen necessary for combustion.

Explosive train:
• A succession of initiating and igniting elements arranged to cause a charge to function.

Homemade explosive:
• Non-standard explosive mixtures/compounds that have been formulated/synthesized from available ingredients. Most often utilized in the absence of commercial/military explosives.

Improvised explosive device:
• A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores but is normally devised from non-military components. Refers to a type of IED incident that involves a complete functioning device.

Remotely commanded improvised explosive device:
• Command switch-initiated devices activated from a distance via wireless transmitting technology, such as radio frequencies, cellular networks, Bluetooth, Internet of Things, Wi-Fi, or telemetric sensors.

Tactical characterization:
• The manner in which an IED incident is planned and conducted (tactical design) and the intent (purpose of device).

Tactical design:
• The specific design of an IED attack – including but not limited to: position of the IED, the type of IED, method of actuation, type of road segment used, concealment technique, use of secondary devices, the time of day, etc. Tactical design addresses the questions of “why here, why now, and why in this way?” Terms used to describe a specific type of device or component of a device (e.g., VBIED) are often used to describe all or part of the tactical design.

Targeting:
• The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.

Technical categorization:
• A description of an IED using a hierarchical construct to identify its key components. The components identified in this categorization are the elements from which technical and forensic information is recovered and exploited.

*All terms sourced from UNMAS Improvised Explosive Device Lexicon (2016)
REFERENCES


Department of Justice. 2017b. “New Jersey Man Charged with Attempting to Provide Material Support to ISIS.” https://www.justice.gov/agp/pr/new-jersey-man-charged-attempting-provide-material-support-isis


Introduction

1 The Cybersecurity and Infrastructure Security Agency (CISA) Office for Bombing Prevention (OBP) has defined an improvised explosive device (IED) as: “A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract.” See: CISA. 2016. “Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance.”

2 The OBP has defined an IED incident as: “Any event that involves a real or suspected IED threat, including IED detonations, bomb threats, the use of hoax devices, discovery of bomb-making components, or the theft of explosives or precursor materials.” See: CISA. 2016. “Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance.”


Challenge 1


Challenge 2


3 The FBI and DHS define a lone actor as an individual motivated by one or more violent extremist ideologies who, operating alone, supports or engages in acts of unlawful violence in furtherance of that ideology or ideologies that may involve influence from a larger terrorist organization or a foreign actor. Source: FBI. 2023. “Strategic Intelligence Assessment and Data on Domestic Terrorism - 2023.” Federal Bureau of Investigation.


Challenge 3

1 Remotely commanded improvised explosive device: Command switch-initiated devices activated from a distance via wireless transmitting technology, such as radio frequencies, cellular networks, Bluetooth, Internet of Things, Wi-Fi, or telemetric sensors.

2 The Internet of Things (IoT) refers to a network of interconnected physical devices and objects, equipped with sensors and technology, that can communicate and exchange data with each other and central systems over the internet. Source: CISA. 2021. “Securing the Internet of Things (IoT).” Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/securing-internet-things-iot


4 Challenge 4

1 In February 2022, FBI Director Christopher Wray reported to the U.S. Senate Homeland Security and Governmental Affairs Committee that the FBI was “investigating, even as we speak, several instances within the U.S. of attempts to weaponize drones with homemade IEDs. That is the future that is here now.” Source: Doctor, Austin, and Sam Hunter. 2023. “The Future of Terrorist Use of Improvised Explosive Devices: Getting in Front of an Evolving Threat.” Combating Terrorism Center at West Point. https://ctc.westpoint.edu/the-future-of-terrorist-use-of-improvised-explosive-devices-getting-in-front-of-an-evolving-threat/

2 Ibid.


Challenge 5


2 Ibid.

3 Ibid.


Challenge 6


2 Ibid.


Challenge 7


3 Ibid.

Challenge 8


3 Ibid.

Challenge 10
