The U.S. Department of Homeland Security (DHS) is responsible for responding to crises generated by a variety of threats and hazards, such as natural disasters, terrorist attacks, and public health emergencies. When confronted with such challenges in the past, DHS has relied on scientific and technical advice to identify gaps in its processes and operations, as well as on solutions to fill these gaps now and in the future. This advice has come from a variety of sources, including DHS components, external research and development (R&D) activities, emergency management and public safety personnel, and the public and private sectors (Science and Technology Directorate [S&T], 2022a). By leveraging this technical advice and support, DHS seeks to improve its understanding of the homeland security threats that it manages and its mission effectiveness.

To support DHS in accessing this type of science and technology advice, the Under Secretary for DHS S&T serves as the science adviser to the Secretary. In this role, the undersecretary establishes deliberate relationships with science and technology communities—one of the main goals of the S&T Strategic Plan for 2021.
(S&T, 2021a). In this context, science and technology communities include interagency; industry and private-sector; academic; research institute; international; and state, local, tribal, and territorial (SLTT) partners (S&T, 2021a). Relationships with partners in these communities provide access to subject-matter experts (SMEs) and external resources, which are critical during times of crisis (Dunlop, Logue, and Isakov, 2014; S&T, 2021a; United Nations Conference on Trade and Development, 2019). Nevertheless, while S&T’s Strategic Plan recognizes that “scientific and technological advances promise substantial social and economic benefits,” it also notes that these advances can pose “significant risks” (S&T, 2021a, p. 3). Therefore, S&T must balance taking advantage of scientific advances to support immediate DHS needs with preparing for future threats and operations (S&T, 2021a).

To enhance DHS’s ability to leverage science and technology communities to support homeland security crisis response and the broader use of science, technology, innovation, and analytical capabilities during crisis response, we sought to understand the following:

- What aspects of homeland security crises make response challenging?
- How have the science and technology communities contributed to preparedness and response?
- What are the components of the science and technology communities that could be leveraged during future crises? In what ways could DHS leverage this expertise?

To answer these questions, we examined peer-reviewed literature, government reports, and news media reporting on how science, technology, innovation, and analytical capabilities have been used during past national security crises. We focused on identifying capabilities rather than assessing how specific organizations may have responded. We also held discussions with six RAND Corporation colleagues who have experience in leadership roles and decisionmaking during homeland security crisis response. This engagement with our colleagues provided additional

---

**Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBP</td>
<td>Customs and Border Protection</td>
</tr>
<tr>
<td>CDC</td>
<td>Centers for Disease Control and Prevention</td>
</tr>
<tr>
<td>COVID-19</td>
<td>coronavirus disease 2019</td>
</tr>
<tr>
<td>DHS</td>
<td>U.S. Department of Homeland Security</td>
</tr>
<tr>
<td>DSTG</td>
<td>Defence Science and Technology Group</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency</td>
</tr>
<tr>
<td>HHS</td>
<td>U.S. Department of Health and Human Services</td>
</tr>
<tr>
<td>HSNRC</td>
<td>Homeland Security National Risk Characterization</td>
</tr>
<tr>
<td>ICE</td>
<td>Immigration and Customs Enforcement</td>
</tr>
<tr>
<td>NBACC</td>
<td>National Biodefense Analysis and Countermeasures Center</td>
</tr>
<tr>
<td>ORA</td>
<td>Operations and Requirements Analysis</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>research and development</td>
</tr>
<tr>
<td>S&amp;T</td>
<td>Science and Technology Directorate</td>
</tr>
<tr>
<td>SAGE</td>
<td>Scientific Advisory Group for Emergencies</td>
</tr>
<tr>
<td>SARS</td>
<td>severe acute respiratory syndrome</td>
</tr>
<tr>
<td>SLTT</td>
<td>state, local, tribal, and territorial</td>
</tr>
<tr>
<td>SME</td>
<td>subject-matter expert</td>
</tr>
<tr>
<td>TSA</td>
<td>Transportation Security Administration</td>
</tr>
</tbody>
</table>
This Perspective is both historical and aspirational, describing how science, technology, innovation, and analysis have been used in the past and how they could be used, and by whom, in the future. To further frame this discussion, we have adopted previously published definitions of the terms science, technology, innovation, analysis, and R&D. These definitions suggest how each capability can be applied during crises:

- **Science** comes from the Greek word meaning *true sense*. It is the pursuit of knowledge of the natural and social world following a scientific method (Gerstein, 2019).
- **Technology** comes from a Greek word that is often translated as *craftsmanship, craft, or art*. It is the application of capabilities for practical purposes. Technology can include capabilities, tools, and methods or processes (Gerstein, 2019).
- **Innovation** incorporates new ways of thinking and novel ideas (Gerstein, 2019).
- **Analysis** is a detailed examination of the elements or structure of something.²
- **R&D** is a structured process that began in the middle of the 20th century and derives from the Industrial Revolution. It is normally associated with an industrial process,³ including production, manufacturing, and procurement (or acquisition). In the application of the term R&D, *research* can be associated with science and scientific discovery, while *development* relates closely to technology (Gerstein, 2019).

In this Perspective, we review DHS’s Homeland Security National Risk Characterization (HSNRC), which provides dimensions for analyzing crisis response scenarios that frame the challenges to be addressed during a crisis response. We then identify the relevant capabilities that are already present in the science and technology communities, providing examples of how these capabilities have contributed to crisis response in the past. Specifically, we sought to develop an understanding of how existing capabilities could be leveraged in the future. In considering these issues, we seek to discuss technical support capabilities in their broadest sense, as they apply across numerous fields of study—from flood mitigation and cybersecurity technologies to the strategic communications and social science aspects of crisis response—to identify where science, technology, innovation, and analysis can be effec-
Crisis response takes many forms in the homeland security domain, in part because of the different threats and hazards that precipitate a crisis.

To that end, we present a conceptual framework for employment of the science and technology communities’ capabilities during crisis response. Finally, we present five imperatives for consideration when providing technical support during a crisis. These critical elements form the basis for providing quality technical support to operational crisis leadership, and we have developed a concept for how to institutionalize that technology support.

**Homeland Security Crises**

A *homeland security crisis* can be defined as any incident, event, or threat “of such severity, magnitude, or complexity that a coordinated federal response is required” (Management Directorate, U.S. Department of Homeland Security, 2017, pp. 162–163). Crisis response takes many forms in the homeland security domain, in part because of the different threats and hazards that precipitate a crisis. Consequently, an examination of the variety of threats and hazards that present homeland security risks to the United States can illustrate the different outcomes and types of operational constraints that must be considered during crisis response. The variation in conditions across crisis types and their associated challenges also creates and shapes the demand for engagement with the science and technology communities to seek their contributions to crisis response. In this section, we review the HSNRC and its dimensions for analyzing threats and hazards (i.e., category, timescale, and impact), which can be used to understand related crises. We also connect these dimensions to specific homeland security crises to show how these crises might motivate engagement with the science and technology communities. These examples characterize the variety of homeland security crises.

**Homeland Security National Risk Characterization Dimensions**

In 2016, the DHS Office of Policy sought to inform DHS strategic planning by identifying and characterizing the greatest homeland security risks to the nation. This effort resulted in the 2018 HSNRC, which assessed a set of threats and hazards that are related to DHS strategic priorities identified in department-level strategy and planning documents and are within the DHS responsibilities for risk management, with DHS playing either a lead role or a major supporting role. In addition, these threats and hazards have the potential for a significant national impact on health, safety, security, the economy, the natural environ-
ment, or the continuity of governance—or some combination of these.

More specifically, the HSNRC assessment process identified 28 threats and hazards in six categories (Table 1), demonstrating how homeland security crises can stem from a variety of causes. For example, crises can result from intentional actions of people or groups, such as terrorist attacks or crimes. Other crises can result from unintentional activities, such as industrial accidents. Natural and health hazards, such as natural disasters and disease outbreaks, can also result in homeland security crises.

In addition to categorizing the variety of identified threats and hazards, the HSNRC presents the different timescales over which these threats and hazards may unfold. Some threats and hazards are associated with discrete events that cause a homeland security crisis, while others are the result of persistent phenomena. Terrorist attacks on commercial aviation, the Boston Marathon bombing in 2013, the effects of Hurricane Sandy on New York in 2012 and Hurricane Maria’s landfall in Puerto Rico in 2017, and the cyberattack on the Colonial Pipeline in the southeastern United States in 2021 exemplify discrete events that demand an immediate crisis response but vary in duration of the crisis and time required for recovery. Discrete events like these are most commonly included as scenarios in crisis response planning, although they should not be exclusively considered.

Other homeland security crises may be launched by a discrete event that occurs over an extended period, thus posing the risk of a protracted crisis. A salient example of this type of hazard is the emergence of a novel coronavirus in 2019, which developed into an ongoing pandemic. In addition, there are hazards that occur in geographic

<table>
<thead>
<tr>
<th>Category of Threat or Hazard</th>
<th>Examples of Threats and Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorist threats</td>
<td>• Attack on leadership</td>
</tr>
<tr>
<td></td>
<td>• Attack targeting critical infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Biological weapon attack</td>
</tr>
<tr>
<td></td>
<td>• Chemical weapon attack</td>
</tr>
<tr>
<td></td>
<td>• Nuclear attack</td>
</tr>
<tr>
<td></td>
<td>• Electromagnetic pulse attack</td>
</tr>
<tr>
<td></td>
<td>• Radiological attack</td>
</tr>
<tr>
<td></td>
<td>• Small arms or explosive attack on population</td>
</tr>
<tr>
<td>Cyber threats</td>
<td>• Cyberattack on critical infrastructure networks</td>
</tr>
<tr>
<td></td>
<td>• Cyberattack that steals sensitive government data</td>
</tr>
<tr>
<td></td>
<td>• Cyberattack on government networks</td>
</tr>
<tr>
<td>Illegal activities</td>
<td>• Counterfeit goods</td>
</tr>
<tr>
<td></td>
<td>• Human trafficking</td>
</tr>
<tr>
<td></td>
<td>• Illegal migration</td>
</tr>
<tr>
<td></td>
<td>• Mass migration</td>
</tr>
<tr>
<td></td>
<td>• Transnational drug trafficking</td>
</tr>
<tr>
<td>Natural hazards</td>
<td>• Drought</td>
</tr>
<tr>
<td></td>
<td>• Earthquake</td>
</tr>
<tr>
<td></td>
<td>• Flooding</td>
</tr>
<tr>
<td></td>
<td>• Hurricane</td>
</tr>
<tr>
<td></td>
<td>• Space weather</td>
</tr>
<tr>
<td></td>
<td>• Tsunami</td>
</tr>
<tr>
<td></td>
<td>• Volcano</td>
</tr>
<tr>
<td></td>
<td>• Wildfire</td>
</tr>
<tr>
<td>Health hazards</td>
<td>• Agricultural plant disease outbreak</td>
</tr>
<tr>
<td></td>
<td>• Foreign animal disease outbreak</td>
</tr>
<tr>
<td></td>
<td>• Transnational communicable disease</td>
</tr>
<tr>
<td>Infrastructure hazards</td>
<td>• Technical failure or industrial accident of critical infrastructure caused by human error or age</td>
</tr>
</tbody>
</table>

SOURCE: Adapted from Willis et al., 2018.
Threats and hazards that are characterized as persistent phenomena can also demand a crisis response if the rate at which they occur increases or they appear in geographic clusters. For example, during wildfire season in the Western United States, simultaneous fires can individually and collectively threaten populations and infrastructure and overwhelm response capabilities.

Threats and hazards that are characterized as persistent phenomena can also demand a crisis response if the rate at which they occur increases or they appear in geographic clusters. For example, the rapid increase in trafficking of synthetic opioids has spurred an epidemic in overdose fatalities, requiring a coordinated federal response. The mass migration of families and individuals from Central America seeking asylum at the southern border of the United States is another persistent phenomenon that presents a homeland security crisis, as it creates challenges for delivering the services needed to respond to asylum claims.

The HSNRC identified several impact categories that were used to describe the risks associated with homeland security threats and hazards (see Table 2). These categories of impact highlight the variety of consequences that crisis response must mitigate. Each type of impact demands different response capabilities. Effects on human health, safety, and security require capabilities to care for those affected by physical and mental injuries. Economic damages require efforts to rebuild damaged facilities and assets, reimburse costs from interrupted business, and offset changes to economic activity that result from the incidents or response to the incidents. Environmental consequences necessitate efforts to promote decontamination or the natural recovery of ecosystems. Impacts on governance demand the implementation of legal and logistical contingencies to provide for the continuity of government functions that have been disrupted. The response capabilities needed to mitigate these disparate risks during homeland security crises might be satisfied by leveraging available technologies and accumulated knowledge.

Learning from the Examples

The category, timescale, and impact dimensions for analyzing threats and hazards outlined in the HSNRC provide general insights into the causes and effects of homeland security crises, which in turn provide a foundation for examining how the science and technology communities can be leveraged for crisis response and recovery. From our review of the HSNRC, we have identified three key takeaways:
Homeland security crises stem from many causes and sources. Intentional or unintentional activities may precipitate an event that requires a coordinated federal response. The diversity in the types of events (terrorist attacks, cyberattacks, illegal activities, natural hazards, health hazards, and infrastructure hazards) that can instigate a homeland security crisis presents a variety of challenges for response and recovery efforts.

Homeland security crises occur over differing time-scales. Crises may be caused by events that vary in duration and recovery time but that demand immediate action when they reach a level of severity, magnitude, or complexity that requires a coordinated federal response. Discrete events and persistent phenomena should both be considered in crisis response planning to understand how capabilities

---

### TABLE 2
Types and Variety of Impacts Associated with Homeland Security Threats and Hazards

<table>
<thead>
<tr>
<th>Impact Category</th>
<th>Impact Type</th>
<th>Example of Low-Impact Threat or Hazard</th>
<th>Example of High-Impact Threat or Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health, safety, and security</td>
<td>Average of deaths or injuries per year</td>
<td>Space weather</td>
<td>Transnational drug trafficking</td>
</tr>
<tr>
<td></td>
<td>Maximum number of deaths or injuries in a single incident</td>
<td>Wildfire</td>
<td>Global pandemic</td>
</tr>
<tr>
<td></td>
<td>Loss of national well-being(^a)</td>
<td>Counterfeit goods trafficking</td>
<td>Small arms or explosive attack on a soft target or national political leadership</td>
</tr>
<tr>
<td>Economic</td>
<td>Average economic damages</td>
<td>Small arms or explosive attack on a soft target</td>
<td>Flooding</td>
</tr>
<tr>
<td></td>
<td>Maximum economic damages in a single incident</td>
<td>Human trafficking</td>
<td>Hurricane</td>
</tr>
<tr>
<td></td>
<td>Severe disruption to infrastructure function</td>
<td>Illegal migration</td>
<td>Cyberattack on critical infrastructure</td>
</tr>
<tr>
<td>Environmental</td>
<td>Greatest environmental damage in a single incident</td>
<td>Cyberattack that steals sensitive government data</td>
<td>Drought</td>
</tr>
<tr>
<td>Governance</td>
<td>Greatest disruption to National Essential Governance Functions in a single episode</td>
<td>Transnational drug trafficking</td>
<td>Cyberattack that steals sensitive government data</td>
</tr>
</tbody>
</table>

\(^a\) Loss of national well-being is defined as the public perception, resulting from a single incident, that government is unable to provide the desired security (Willis et al., 2018).
in the science and technology communities can be leveraged.

3. Homeland security crises affect communities in many ways. The various threats and hazards that contribute to homeland security crises affect human health, safety, and security, as well as the economy, the environment, and governance. The resulting recovery needs for each of these threats and hazards are similarly broad. However, the breadth of potential impacts creates a variety of opportunities for the science and technology communities to contribute.

**Science and Technology Community Capabilities Available for Crisis Response**

To support homeland security crisis response, the science and technology communities (including DHS’s science and technology community) have employed a variety of technical and analytical capabilities. The capabilities used vary depending on the immediacy of the crisis that is occurring; antecedents that have been considered in exercises, scenarios, or other real-world events; current data, knowledge, and capacities that are readily available; existing analytical and laboratory capabilities; and other resources that are immediately available. When existing capabilities and analytical tools are employed early in a crisis, it is likely that they will help form the basis of the response.

As responses continue to mature and broaden, new capabilities can be developed and used. This development will likely include coordination and collaboration among a variety of partners, such as industry, academia, and non-profits, and may require longer-term contracting to build new science, technology innovation, and analysis capacity within a particular field. Even these longer-term issues can be considered part of the immediate crisis response, with deliverables and requirements established that can aid in the initial crisis response and recovery. At some point, the longer-term efforts may transition out of crisis response and become new lines of business or of analytical effort. A natural transition normally occurs when the immediate crisis response transitions to the development of a longer-term set of science, technology, innovation, and analysis efforts that, in some cases, may even begin to form programs of record. Providing an exact template or framework for each possible crisis is not feasible; however, developing a broad set of guidelines that govern the employment of science, technology, innovation, and analytical capabilities is a worthwhile and necessary effort.

Employing technical support capabilities during times of crisis is not a new concept. Preparedness and response planning and exercises are based on these capabilities, which seek to incorporate scientific knowledge, technology development, innovation, and analysis to solve operational problems, inform decisions, and improve preparedness and response. We see this in the plans that are developed and the after-action reviews (and lessons learned) conducted following crises, natural disasters, and even exercises. Through these reviews, leaders and stakeholders seek to incorporate approaches, including technical support capabilities, to inform all aspects of crisis response. The Science for Disaster Reduction Interagency Coordination Group’s 2021 report—*Integrating Science and Technology with Disaster Response*—sums up the role of these technical support capabilities as providing “new collaborations and
innovative solutions [that] are needed to reduce risk” (p. 5). The report also highlights that “federal and academic science and technology (S&T) capabilities are already integrated into disaster prevention, mitigation, response, and recovery” (p. 5).5

**Historical Examples of Crisis Response**

Many of the capabilities present within the science and technology communities have been or could be applied to support homeland security crisis response. To develop a broad set of guidelines that can facilitate engagement with those capabilities, we have reviewed a selection of homeland security crises and the “technical” response to each.6 Historical examples of homeland security incidents illustrate how government departments and agencies and industry have leveraged particular capabilities. These examples can also provide the basis for enhancing contributions from the science and technology communities and identifying other ways in which their capabilities can be leveraged during a crisis.

**Post-9/11 Aviation Security**

The terrorist attacks on September 11, 2001, spurred several science, technology, innovation, and analytical capabilities that were not available prior to the attacks. While these adaptations are far too numerous to be exhaustively examined in this Perspective, the changes in aviation in the immediate aftermath of the attacks provide useful examples.

To gain control of the situation, all flights were grounded, and aircraft that were already airborne were diverted to other destinations. The leveraging of analytical capabilities began immediately. Air carriers, the Federal Aviation Administration, and law enforcement began to analyze manifests to identify other potential attacks. Commercial aviation flights were halted for several days following the 9/11 attacks (Clark, McGibany, and Myers, 2009).

When air travel resumed, the fruits of the technical response could be seen. The aviation security system, which had largely remained the same since its inception in 1973, had been transformed almost overnight. New screening techniques to look for a variety of implements that could be used as weapons were employed. The traffic patterns around airports were also rapidly modified to provide greater standoff distance from potential bombings.

A little over two months after the attacks, the Aviation and Transportation Security Act was signed into law and established the Transportation Security Administration (TSA) (Pekoske, 2021). From its inception, TSA has incorporated technical capacities to “expand field operational
testing of advanced screening technologies, increase the usage of canine resources, enhance public area security, and improve the security of passengers, cargo, cockpits, cabins, surface transportation, and foreign airports” (Pekoske, 2021). Many of these capabilities were incorporated into aviation operations during the initial crisis period of the 9/11 attacks.

This pattern of incorporating capabilities from the science and technology communities would continue in aviation security after 9/11. Although experts considered possibilities and scenarios that needed to be guarded against in the context of 9/11, it was often emerging threats or risks that led to new technical approaches. With the identification of each emerging risk, new techniques, procedures, and equipment were incorporated to harden the target and mitigate the insecurity.

The shoe bomber (2001), liquid explosive threat (2006), underwear bomber (2009), and printer bombing plot (2010) exemplify this pattern of response, as each resulted in security measures being rapidly incorporated into TSA and global screening procedures (TSA, undated; U.S. Senate, 2011). One account states,

Now, travelers often stand in long lines at security checkpoints with wait times that can exceed an hour. We take off our shoes, empty our pockets and take laptops and other devices out of carry-on bags before stepping into high-resolution, full-body scanners, while our bags go through 3D-imaging X-ray machines. And don’t forget to take your liquids of 3.4 ounces or less out of your carry-on. (Schaper, 2021)

After each of these incidents, new techniques, procedures, and equipment were incorporated into aviation security systems, in no small measure to reassure the traveling public of the safety of air travel.

The immediate efforts to mitigate threats as they emerge have also been improved by and augmented with a variety of capabilities that have been developed over time. For example, the Transportation Security Laboratory (a DHS S&T national laboratory) at the William J. Hughes Technical Center in Atlantic City, New Jersey, is responsible for certifying imaging machines to ensure that known threats can be detected, and the Center for Awareness and Localization of Explosives-Related Threats (a DHS S&T university center of excellence) conducts research on response to explosive-related threats to improve aviation security. These established capabilities, which were developed in the aftermath of the 9/11 attacks, can now support immediate crisis response in the form of data, analytical tools, and expertise that can be readily tapped in the event of a future threat or risk.
Response to Naturally Occurring and Man-Made Biological Threats and Risks

The 2001 anthrax attacks resulted in a growing awareness of the potential for bioterrorism and, more broadly, the intentional use of biological pathogens in an attack against humans, animals, and plants. In addition, the identification of severe acute respiratory syndrome (SARS) in 2002 heightened global concerns about the potential for a large-scale pandemic. The concerns about biodefense and a strategy for managing the threats and risks were codified by President George W. Bush on April 28, 2004, in Homeland Security Presidential Directive 10 (HSPD-10), “Biodefense for the 21st Century” (White House, 2004). HSPD-10 called for the development of continuity planning for pandemics and other biological risks as they began to gain new visibility. Training and exercises were developed to improve preparedness and response capabilities across federal and SLTT entities. Research into dangerous pathogens of concern continued to be conducted with an eye toward understanding the threats and risks, developing medical countermeasures and diagnostics, and developing other defensive countermeasures. HSPD-10 also codified the stockpiling of countermeasures.

Three facilities were developed in the 1950s for studying infectious disease, either naturally occurring or man-made: Plum Island Animal Disease Center (now a DHS S&T national laboratory), the U.S. Army Medical Unit (which later became the U.S. Army Medical Research Institute of Infectious Diseases), and the Centers for Disease Control and Prevention (CDC) Epidemic Intelligence Service. These organizations have traditionally had strong relationships with academic institutions that also have their own laboratories for conducting research. The U.S. Department of Energy’s national laboratories, such as Lawrence Livermore National Laboratory and Sandia National Laboratories, also supported DHS in its national biodefense mission. Later, DHS would create its own biodefense facility, the National Biodefense Analysis and Countermeasures Center (NBACC), for conducting high-containment threat characterization and forensics. The establishment of several biodefense DHS S&T centers of excellence for human and agricultural issues provided important new sources of technical support capabilities for preparedness and response, including during crises.

This early history is important because it highlights the necessity for laboratory and analytical capabilities for gaining understanding of, preparing for, and responding to biological threats and risks. It also highlights the need for interagency and international collaboration across the science and technology communities on these biodefense issues. As an example, the U.S. Department of Health and Human Services (HHS) maintains two high-containment laboratories—one at the CDC in Atlanta, Georgia, and one at the National Institute of Allergy and Infectious Diseases at Fort Detrick, Maryland—that DHS S&T collaborated with on crisis response biodefense matters (National Institute of Allergy and Infectious Diseases, 2021). International partners also bring a wealth of knowledge and capacity (including facilities where they conduct research)—as part of a normal research agenda or for crisis response—on biodefense agents and pathogens that are endemic to their countries or regions. In addition, crisis response is related directly to governmental and nongovernmental capabilities, such as public health organizations, hospitals, environmental protection agencies, and industry and international authorities (e.g., World Health Organization,
Bilateral information-sharing provides important foundations for crisis response.

Food and Agriculture Organization). During crises, these entities share technical information and findings that can be used to support leadership decisions at all levels and strategic communications with the public.

This relationship between a crisis response and its needed capabilities implies that facilities and relationships across the biodefense community must be well-developed prior to the surfacing of a biological threat and risk. For example, the 2002–2004 SARS pandemic and fears of an H5N1 highly pathogenic avian influenza becoming efficiently transmitted through the human-to-human route led to new legislation, significant planning efforts, and training and exercises to be better prepared for such a naturally occurring event. Efforts to closely monitor and report changes in the spread of H5N1 and other pathogenic diseases of concern have also been undertaken (see, for example, Sellwood, Asgari-Jirhandeh, and Salimee, 2007).

Furthermore, bilateral information-sharing provides important foundations for crisis response. Several countries have shared critical information and data on pathogens with U.S. researchers. For example, Sweden has particular expertise in the study of Francisella tularensis, the causative agent for tularemia, because it exists naturally in Sweden. Likewise, Australia conducts research on two zoonotic diseases of concern, caused by the Nipa and Hendra viruses. Canada’s work on Ebola, particularly on medical countermeasures, was also of interest to U.S. researchers. The research on these pathogens—which have different mechanisms of action (for causing disease) and different methods for prevention, treatment, response, and recovery—serves to highlight why close collaboration on biodefense between DHS S&T and international partners is essential. This collaboration should be conducted as part of biodefense preparations and during crises.

The NBACC, with specialized capabilities for understanding biological threats, supporting intelligence assessments and preparedness planning, determining pathogen properties, conducting agent fate studies, supporting countermeasure development (either pharmaceutical or nonpharmaceutical interventions), and supporting bioforensics, provides a set of unique crisis response capabilities (S&T, 2022b). The use of a master question list (MQL) to identify issues of concern and further research, track the investigation of these MQL items, and share the information with the broader biodefense community is an important aspect of support during a biological crisis (S&T, 2021b). The broader interactions with the centers of excellence that conduct research on biodefense issues also provide a ready source of collaboration during crises.

Specific outbreaks have also led to the use of science, technology, innovation, and analytical capabilities. During the H1N1 pandemic in 2009, public health authorities and government agencies, including DHS, collaborated to develop federal guidelines for screening, prevention, vaccination, and treatment; one notable example is in the case of guidance to SLTT school systems (DHS, 2009). During
the 2014 Ebola epidemic, because of scientific under-
standings developed during the crisis, U.S. Customs and
Border Protection (CBP), in coordination with the CDC,
developed screening mechanisms that included visual
observation, questioning, and notifications for all federal
inspection areas at U.S. airports, land border crossings,
and seaports (DHS, 2021a). More recently, during the
coronavirus disease (COVID-19) pandemic, DHS has
provided scientific, technology, innovation, and analysis
capabilities across a variety of activities, including screen-
ing at ports of entry and borders, protecting vital com-
munications and cybersecurity, protecting critical infra-
structure, preventing and mitigating disinformation, and
distributing vaccines (DHS, 2021b).

Response to Surge in Activity in the Rio Grande
Valley

In 2013, a surge in border crossings at the Rio Grande
Valley basin created a humanitarian crisis. The influx of
immigrants stressed the operations of many federal author-
ities engaged in the response, such as CBP, Immigration
and Customs Enforcement (ICE), and HHS. Consequently,
facilities were overwhelmed as processing times resulted in
large backlogs of immigrants at temporary facilities. The
number of people traveling across the border also over-
whelmed state and local authorities. The number of apprehen-
sions of immigrants coming from countries other than
Mexico, which had increased by 71 percent in 2013, further
exacerbated the issue. The Rio Grande Valley experienced
the largest increase in immigrant apprehensions—from
50,000 people in 2012 to almost 97,000 in 2013 (Aguilar,
2014; CBP, undated). This increased influx led to the rec-
ognition that the U.S. immigration system needed to be
reformed (Aguilar, 2014; Argueta, 2016; Martínez et al.,

An initial approach to reforming the immigration
system rested on understanding how the system was cur-
tently functioning. Although CBP was using surveillance
technologies and methods that had been used at other
border locations, there were case-specific nuances that had
to be considered. For one, immigrants were, by that point,
largely coming from Central America rather than Mexico,
indicating a changing population. In addition, there was a
lack of Mexican resources in the Rio Grande Valley com-
pared with resources at other border crossing locations.
CBP also deployed air surveillance assets to greater use in
the Rio Grande Valley, allowing the agency to better see the
border crossings as they were occurring.

In this case, CBP initiated a request for assistance in
finding ways to better manage the flows of immigrants.
An S&T team used operations analysis techniques to ana-
lyze and understand the flows of people. In this particular
analysis, the rationale for the flows was less important
than managing the overwhelming numbers of people who
were at the borders and needed to be screened, sorted
into groups for further processing, and either moved to
more-permanent locations or returned to their countries
of origin.

The S&T analytical team conducted a short initial
analysis of the situation. Following its initial research, the
team was provided with an opportunity to do “ride-alongs”
with CBP agents to gain an operational understanding of
the issues that agents faced, to identify opportunities for
improving the effectiveness and efficiency of their opera-
tions, and to develop a set of recommendations. Under-
standing the business processes by which CBP agents
operated in the field and during processing at the centers provided essential foundations for the team’s analysis. The analysis illustrated how U.S. Border Patrol agents were being consumed with the processing at the apprehension facilities. That is, the agents’ efforts were focused on apprehending immigrants, bringing them to the facilities, and processing them. This process took the agents away from their primary mission, apprehending immigrants.

Using network flow techniques, the S&T team was able to map the business process within the apprehension facilities. The team discovered that there were 21 discrete steps that needed to be accomplished as part of immigrant processing. By mapping the flows and by minimizing the number of discrete movements required for an immigrant to move between stations, Border Patrol and other government agencies could reduce the number of total stations by over half. The result was a more efficient process that reduced the time to completion by more than 24 hours.

Another important finding was that other government agencies, such as ICE and HHS, also needed to optimize their process flow.

Although the example at the Rio Grande Valley speaks to maximizing the efficiency and effectiveness of processing immigrants, the same types of analytical techniques could also be used in positioning surveillance equipment and deploying patrols. This analysis was the response to a quick reaction request, and the majority of the effort was completed within approximately six months. Several of the research team’s recommendations were employed, resulting in a decrease in processing times and greater numbers of agents available to return to the border.

Response to Hurricane Sandy

Hurricane Sandy made landfall in New Jersey and New York City on October 29, 2012. At the time, the storm spanned more than 1,100 miles and affected 24 states. The affected geographic region, combined with the size and power of the storm, set the stage to make Hurricane Sandy one of the most costly and devastating hurricanes to hit the United States. Final assessments determined that damage from Hurricane Sandy cost $80 billion.

In thinking about Hurricane Sandy preparedness and response, it is important to think of the learning and improvement of response to and recovery from natural disasters as being cumulative. In this way, we can think of improvements to prevention, protection, mitigation, response, and recovery as being based on the lessons learned from all other natural disasters. In particular, Hurricane Katrina (2005) had certainly provided ample understanding of issues that could surface with such a massive and powerful storm. Many of these lessons learned have been cataloged and analyzed using science, technology, innovation, and analytical capabilities that helped various stakeholders understand and make sense of the collected data.

For example, the Federal Emergency Management Agency (FEMA) has used experiences in other natural disasters to promote the use of early state disaster declarations well in advance of storms to allow the federal government to begin preparations for response and recovery. These preparations have included stationing response and recovery assets just outside the area that is expected to be affected so that response and recovery can begin as soon as the storm passes (Ladislaw, 2013).
Given the repetitive nature of these disasters, crisis response for the next major event is based on the science, technology, innovation, and analytical work that is done after each storm to help better prepare for and respond to future events. For example, on the third anniversary of Hurricane Sandy, the White House issued “Legacies of Hurricane Sandy: Science and Technology for a More Resilient Nation” (Dickinson and Werner, 2015). The article highlighted that the federal government had developed three “science-based products” to make communities “better prepared for and more resilient to” natural disasters: (1) “scientific research priorities for green infrastructure”; (2) “improved data-sharing among federal, state, and local officials”; and (3) “visualization of the impacts of sea-level rise” (Dickinson and Werner, 2015). It is noteworthy that one of the most important findings emphasizes the need for sustainable and resilient power. The hurricane knocked out power for 8.5 million people, a major impact on the ability to supply sustainable and resilient power. Even a week after the storm, more than 1 million people were without power. Furthermore, this lack of power hindered recovery efforts and resulted in additional damage to infrastructure (Dickinson and Werner, 2015).

Several of the key technologies and innovations that were deployed during Hurricane Sandy resulted from the actions of individual organizations that saw a need for an information source or application. For example, a New York public radio station provided information to listeners through crowdsourcing. The Sandy Coworking Crowdmap was an application that showed people where they could go to “work, recharge and reconnect” (Nanfuka, 2012). Terrain mapping with unmanned aerial systems was used to look at the “before and after” of geographic areas affected by storms (Hutson, 2017). These capabilities have proven instrumental in helping immediately assess the impact of the damage, the areas that are the most affected, and the areas where response and recovery assets are likely to be the most beneficial. One of the DHS S&T centers of excellence developed a flood assessment tool that allowed stakeholders to better understand how the flood might affect their areas (Coastal Resilience Center, undated).

Learning from the Examples

Examining past homeland security crises highlights how science, technology, innovation, and analytical capabilities have been previously leveraged during crisis response. From our review of the selected examples, we have identified several key takeaways:

1. **Crisis technical support requires a keen understanding of the operational issues to be solved.** It is imperative to understand the operational issue before embarking on analysis. Gaining this operational understanding helps to assemble the right group of
experts, bring in the proper stakeholders, and begin to collect the necessary data.

2. *There is no single framework or set of tools for supporting crises with science, technology, innovation, or analysis.* In some cases, operational analysis techniques could be sufficient to understand the issues and be able to assist operators with developing solutions, as was the case during the analysis of the Rio Grande Valley immigration issue. However, in considering the naturally occurring and human-made biological threats and risks, having access to laboratories (either directly or through collaboration) will likely be a necessity.

3. *Technical support during a crisis is enhanced by preparation, prior analysis, data, and relationship-building.* In some cases, the preparation will be extensive, as seen in the development of the NBACC. In other cases, prior analysis and an up-to-date data set might be sufficient to begin operational analysis of an issue. However, in most cases, beginning operational analysis from a “standing start” will disadvantage the research.

4. *Technical support during a crisis benefits from novel thinking, new approaches, and a diverse group of experts.* Casting a wide net, in terms of both direct SMEs and what can be best described as “outside-the-box thinkers,” can be beneficial in finding new solutions or solving complex problems. Bringing in new techniques, such as crowdsourcing, can help cast this wide net.

5. *Integrating operational solutions requires support from numerous stakeholders, including government (federal and SLTT), industry and the private sector, academia, and the public.* Developing acceptable operational solutions requires gaining buy-in, which implies being inclusive with the stakeholders who will fund, lead, and live with the operational solutions that are implemented.

---

Conceptual Framework for Employment of Science, Technology, Innovation, and Analytical Capabilities for Crisis Response

Informed by the dimensions of the threats and risks outlined in the “Homeland Security Crises” section and the lessons developed in the previous section, we have
developed a framework for thinking about crisis response support and five technical support imperatives for crisis operations.

Fusing Technical Support Capabilities with Operations

Most government organizations, large industry partners, and even nonprofits that routinely conduct business in remote locations have operations centers or command posts. Operations centers generally include a cross section of the leadership and staff elements, and they provide a capacity for gathering and sharing information, assessing the crisis, and making and communicating decisions. This collective format allows decisionmakers to have prompt access to necessary information and staff elements. Included in the staff elements are key organizations and individuals from the technical support parts of the organization. We talked to several colleagues who are SMEs on crisis response, and they spoke of the utility of their operations centers or command posts. The discussants observed that the centers were highly tailored to meet the needs of the organizations they support; however, the discussants all spoke of the utility of having their technical support elements represented within these centers.

Several U.S. partner nations have established national-level capabilities for providing this type of support. The United Kingdom employs a concept called the Scientific Advisory Group for Emergencies (SAGE), which “provides scientific and technical advice to support government decision makers during emergencies” (SAGE, undated). SAGE is chaired by the United Kingdom’s Chief Scientific Adviser. During crises, SAGE has been convened with approximately 20 participants at any given time. These participants come from several stakeholder communities, ranging from operations to academia and industry (SAGE, undated). Similarly, the government of Australia uses its Defence Science and Technology Group (DSTG) as a ready source of technical support for providing “impartial advice and innovative solutions for Defence and national security” (DSTG, undated). The DSTG is headed by the Chief Defence Scientist and “work[s] closely with industry, universities and the scientific community” (DSTG, undated).

For national responses in the United States, FEMA runs the National Response Coordination Center. This multiagency coordination center monitors incidents, supports regional and field commanders, initiates agreements and develops specialized teams, and resolves federal resource support (National Response Coordination Center, undated). Most U.S. cabinet-level departments and agencies also have functioning operations centers or command posts that support both daily operations and crisis response. Generally, these centers are lightly manned during normal operations, but they can be rapidly spun up to include key relevant organizations. Most centers will include a science and technology adviser (or equivalent position) as part of the crisis response capability. For example, the U.S. Department of Defense has the National Military Command Center, which fulfills this function and includes representatives from technical support areas.

These operations centers provide an important venue for information-sharing and collaboration. The centers employ liaison officers and have regularly scheduled video teleconferences to bring in a wide array of stakeholders and technical experts. For example, hurricanes and other weather events would routinely bring representatives
from the National Oceanic and Atmospheric Administration, U.S. Army Corps of Engineers, CDC, and U.S. Environmental Protection Agency—to name a few federal participants—into the FEMA-run National Response Coordination Center.

The Science for Disaster Reduction Interagency Coordination Group’s 2021 report highlights the science and technology capabilities that are often shared through these collaborative venues: “GIS [geographic information systems] and remote sensing, meteorological, toxicological, geological, biological, and engineering expertise, as well as social and computer sciences can be brought to bear in disaster situations to reduce both the short- and longer-term risks from these disaster events” (Science for Disaster Reduction Interagency Coordination Group, 2021, p. 6).

The same is true of subcabinet-level agencies and non-governmental organizations. The CDC, for example, can expand to more than several hundred people in times of crisis. From the CDC’s emergency operations center, the watch officer “deploys scientific experts,” “coordinates delivery of supplies and equipment to the incident site,” “monitors response activities,” and “provides resources to state and local public health departments” (CDC, 2021). Nongovernmental organizations, such as Médecins Sans Frontières (Doctors Without Borders), have operational centers that “directly manage [their] humanitarian action in the field and decide when, where, and what medical care is needed” (Médecins Sans Frontières, undated).

Because the main organizations and missions of these operational centers vary greatly, each center requires specific capabilities in support of its respective mission. An important technical support capability is having access to relevant leaders and decisionmakers during the crisis. Access to relevant models, simulations, and data is also critical—and most effective—when the data are collected and curated before a crisis. Knowing the availability of resources that could be beneficial during the crisis is also important. Given the variability of crises discussed in the “Homeland Security Crises” section, having an established network from within and across various stakeholder communities to leverage these capabilities is essential during crisis response.

The nuclear disaster in Fukushima, Japan, provides an example of how technical support capabilities can be leveraged for crisis response. In the immediate aftermath of the disaster, the U.S. National Security Council stood up a crisis action capability from across the government. Technical advisers on nuclear and radiological dispersion were brought in to provide information and judgments that would prove prescient in the U.S. response. The U.S. Department of Energy and the U.S. Department of Defense’s Defense Threat Reduction Agency ran plume models and simulations that supported decisionmakers for strategic communications, dispersal of medical countermeasures, and assessment of the severity of the incident. Representatives from HHS provided information on the effects of radiation, as well as guidance regarding evacuation strategies and the types of medical countermeasures that would be beneficial.

Overall, our research and SME engagement reinforced the importance of employing sound science, technology, innovation, and analysis to inform decisionmakers and take action. One SME underscored this point, noting that a flood model proved to be invaluable to the decisionmaking process because it provided a solid basis for making an
analytically informed decision even when the data set was not fully complete.

Framework for Technical Support Discussions

The four categories of technical support (science, technology, innovation, and analysis) included in this framework (Table 3) apply as part of the normal support that a technical agency would provide, as well as during times of crisis. The difference is that during crises, an immediacy is introduced, which is depicted in the five time frames (before the crisis, immediate, near term, mid term, and long term). The time frames are an important element of the framework because they help identify the types of activities that would be feasible and practical to implement during a crisis, as well as precrisis activities that could be important to the execution of a crisis response. Although we provide notional lengths of each time frame, these lengths can vary across different types of crises.

The technical support categories should not be considered discrete; rather, they have elements that overlap. In addition, they are not linear processes; it is possible, even likely, that elements of all four categories will be ongoing during a crisis, even in the early stages. We also note that technology is recursive and therefore builds upon earlier technologies. In this way, we acknowledge that the operational necessity caused by crises and other real-world events leads to new science, technology, innovation, and analysis that are then incorporated into future responses and events and even new ways of doing business. For example, early in a crisis response, questions can be framed, data collected, and initial study plans identified to inform the immediate response. Yet these efforts could also inform a longer-term R&D program for science and technology development. It is challenging, however, to envision how basic and applied research (as captured in the science [research] row of the framework) could be completed in the immediate term. Alternatively, the lessons learned from previous crises can serve as a basis for

<table>
<thead>
<tr>
<th>Technical Support Category</th>
<th>Before Crisis</th>
<th>During Crisis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Immediate (hours or days)</td>
</tr>
<tr>
<td>Science (research)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology (development)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Innovation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To effectively assist in responding to a current emergency and preparing for the next one, technical support personnel need direct access to science, technology, innovation, and analysis during crises.

Precrisis science, technology, innovation, and analysis that will aid in better preparation for the next emergency. Often, such data and analyses can be used to develop better understandings, even models and simulations, that can prepare decisionmakers and the stakeholder community for the future. To effectively assist in responding to a current emergency and preparing for the next one, though, technical support personnel need to have direct access to science, technology, innovation, and analysis during crises.

Getting a Seat at the Table

Gaining access to leadership was identified as imperative for providing relevant technical support during crises. This access should include connections with technical support personnel who have critical knowledge about the state of key technology areas that are likely to be important, as well as familiarity with operational knowledge gaps, for the crisis at hand. SMEs stated that gaining such access often required breaking down cultural barriers between operators and technical personnel, in addition to gaining the trust of crisis operational leadership.

SMEs highlighted the importance of technical support capabilities during a crisis. They discussed the importance of having a close affiliation with—some even stated a direct line to—leaders or decisionmakers involved in the immediate crisis. In this way, the technical support can be informed by the needs of the leadership, making it more likely to be effective in examining issues and offering relevant insights and recommendations.

One former senior leader said that they created a staff position for a full-time science and technology adviser (who also had a background in innovation and analysis) to assist in sorting through the technical support issues that
invariably arise during a crisis. The adviser’s role included providing an access point for the various stakeholders and interested parties who had developed suggestions of a technical nature. Although not all SMEs with whom we spoke had experienced a full-time member of the staff being used for technical support issues, virtually all understood the necessity of having such an individual appointed to this role. Furthermore, the discussants that had not seen such a direct role being employed noted how, in the absence of such an appointed technical individual (or point of contact), a member of the staff had to de facto step in to fulfill the role.

Several SMEs identified having prior relationships with the technical support lead and being able to demonstrate a “value add” early in the crisis as pivotal for how well technical support was incorporated into the operation. When trust had been previously established between the decision-maker and the technical support lead, the likelihood that the support would be well received was greater. These relationships might have been established during prior exercises or from previous support during crisis or non-crisis periods. If the technical support lead was able to demonstrate early “wins” by providing quick data collection, analysis, and dissemination to key leaders or by providing situational awareness or research insights, the chance of developing a successful relationship improved greatly.

Conducting Precrisis Planning and Exercises

Precrisis planning was identified by several SMEs as critical for providing technical support during a crisis. Although they mentioned that such planning does not always occur, several discussants stated that planning for crises should include tasks and requirements for the technical support capabilities that are integrated into operations plans during all operational phases. A benefit accrues for both the supported organizations and the technical support entities as they become adept at communicating on technical issues, anticipating requirements, and building key relationships.

Specifically, regarding exercises, SMEs said that the technical support leaders and organizations should be available during exercises to better inform the crisis response leadership of the types of support that could be garnered from science, technology, innovation, and analysis. Exercise participation also benefits the technical support leaders and organizations because they would likely better understand the types of support that would prove most useful.

We also heard how important the precrisis preparations could be. For example, the development of models and simulations in key areas could prove to be pivotal in the early stages of a crisis or even in preparing for an impending natural disaster, such as a hurricane. The flood prediction model developed through the DHS S&T centers of excellence program provides one such example. Either having precrisis information readily available or rapidly collecting and sharing data with operators was also cited as being important during the early stages of a crisis.

Several SMEs highlighted the importance of developing precrisis directories that contain contacts for broad cross sections of technical experts who could be called on to support the variety of possible crisis scenarios that could unfold. These experts should be identified from across the science and technology communities (i.e., interagency, industry and public sector, academic, research institute, international, and SLTT partners), as well as other key
stakeholder communities. Selection criteria for these highly qualified experts should include diversity of thought, education, and experiences. Gaining access to such organizations and individuals needs to be factored into precrisis planning; their expertise, as well as their willingness to provide support, needs to be understood before a crisis response is initiated. In some cases, contractual relationships should be established to provide flexibility for rapidly gaining the services of key technical support organizations.

Managing Data and Supporting the Development of a Common Operational Picture

All of the SMEs with whom we spoke stressed the importance of making decisions based on the available factual information and best available data. Managing the vast amount of data being collected by disparate organizations and developing a common operational picture often become key focuses of the response, and these are areas where technical support can be pivotal.

SMEs highlighted their experiences of having competing data sets or findings that were in conflict. Operational response organizations are often challenged in collecting, validating, and managing their data. The Fukushima nuclear disaster serves again as a salient example. Various global and U.S. government agencies had different data sets and plume models, which were respectively leading to different conclusions. The technical support entities embedded in the discussions were thus pivotal to gaining situational awareness of the radiological plume, as well as to developing guidance for distribution of medical countermeasures and evacuations of affected populations.

Trained data scientists from the technical communities often bring new tools and fresh perspectives that can be beneficial for aiding crisis response and recovery operations. Such experts are also trained to ask the appropriate questions to stimulate data collection and new approaches to analyzing the data. One SME highlighted how, during relief operations in Haiti, a major issue was knowledge management because keeping the data straight from all of the disparate actors was problematic. An SME who served with HHS during the COVID-19 pandemic provided another example of necessary data deconfliction for crisis response, specifically the effort to combine data from across numerous departmental and agency organizations to develop a common and accepted understanding of the crisis progression. Assisting in collecting the data, using state-of-the-art tools for storing and curating the data, and having proximity to the sources of the data provide significant benefits for the technical support organizations, as well as the crisis response organizations.

Managing the data and developing a common operational picture can also lead to the development and use of models and simulations that can be useful in managing the crisis. Several SMEs discussed the importance of such analysis. Because models and simulations are not static tools, they need to be updated with new data and insights as more is understood about a type of crisis.

Bringing in New Ways of Thinking

Employing technical support capabilities can result in new ways of thinking about operational issues encountered during crises. Several SMEs also provided insights into how technical support was incorporated into their response and recovery operations. One SME described how, during a marine accident response, existing technologies were employed in a novel way. In this case, side-scan sonar was
used to aid in the search for bodies, which proved to be an innovative solution for recovering human remains. The same individual offered that some of the response personnel had concerns about employing new technology in a real-world operation when it had never been tried during an exercise. The personnel were persuaded to give the technology a chance, and the concession was rewarded when the application proved successful.

SMEs also said that technical support (and the technical leadership) were perceived as “honest brokers,” seeking only to provide reasonable solutions. They could be part of—but not necessarily directly involved in—the response and recovery, which allowed them to have a degree of objectivity. They were able to think of the possibilities rather than be encumbered by strict adherence to doctrine or limited to only the embedded technical capabilities of the response and recovery organizations. In this way, technical support personnel could think differently about the challenges and look for nontraditional solutions to “wicked” problems.

In describing the manner in which the technical support capabilities could be most useful, the discussion participants often turned to the need for bridging the gap between the leaders and operators managing the crisis and the science and technology organizations. Here, a technologist with a broad understanding of the operational problem and the ongoing state of technology across multiple technology fields could serve as a vital translator, linking the operational problem with potential science, technology, innovative, and analytical solutions. For example, one SME shared his experiences during the Deepwater Horizon oil spill, when experts across various disciplines were asked to collaborate and share insights about possible solutions that could be used to stem the flow of oil being released into the Gulf of Mexico. Because of the nature of the crisis, industry and academic experts proved to be essential because capping the flow required new technology and innovative solutions that had to be created during the crisis. These new technologies and innovations had a near-term benefit for mitigating the Deepwater Horizon oil spill, as well as a long-term benefit that would be useful during future crises of this sort (Ewald, 2020).

**Taking Advantage of Unique Opportunities for Innovation During Crisis Support**

SMEs offered several examples of unique opportunities for providing technical support during crises: opportunities for innovation to gain situational awareness, incorporation of specialized capabilities not readily available to the broader community, and the potential for incorporating innovative solutions. The pressure to act quickly often opens doors that would not be available during normal or routine technical support efforts. People—including crisis response leadership
The intense operational requirements brought on by crises have resulted in innovations that might not have been identified without the expediency of the moment.

and first responders—are often far more willing to look for outside-the-box solutions and take chances.

SMEs highlighted the importance of gaining situational awareness early in the crisis and maintaining it throughout, emphasizing how technical support capabilities could facilitate this objective. One SME highlighted how combining various technologies in new ways (i.e., innovation) improved situational awareness. For example, a CBP P-3 aircraft was able to push pictures of Hurricane Sandy devastation over an ICE network, and the pictures were then used by the U.S. Coast Guard for assessing port damage. In addition, technology from the National Oceanic and Atmospheric Administration was used in conjunction with the U.S. Coast Guard’s systems to gain awareness of thousands of small oil spills caused by damaged vessels, which was critical for the response and recovery.

SMEs also offered that, for certain types of crises, SLTT authorities would lean heavily on the technical support capacities of the federal government. For example, plume modeling for chemical, biological, radiological, or nuclear (CBRN) events would be essential for informing responders and the public regarding these types of incidents. Federal authorities would also provide critical support and guidance in such CBRN tasks as evacuation of affected populations, treatment of casualties, and development and delivery of medical countermeasures.

The intense operational requirements brought on by crises have resulted in innovations that might not have been identified without the expediency of the moment. One SME highlighted that, during Hurricane Sandy, the U.S. Coast Guard redirected its strike teams from their usual efforts assisting with flooding relief to specifically pump out the water from New York City subway tunnels. This was the first time that this application had been tried, and it proved successful. Several SMEs highlighted the potential for innovation and technology infusion benefits from incorporating technical support capabilities. One example was the integration of counter–unmanned aircraft systems into water patrols during the United Nations General Assembly in 2019. S&T was seen as pivotal for orchestrating this support. Finally, the use of S&T to analyze the greatly increased migrant flows in the Rio Grande Valley in Texas in 2012 provides another case in which analysis provided immediate insights for streamlining the processing of migrants and the coordination between U.S. government departments and agencies. The team combined on-site assessments, interviews with Border Patrol agents, and analytical tools to identify the root cause of the growing queues of migrants.
Without the immediacy of crises and other operational necessities, it is unlikely that such innovations would have been discovered.

Considerations When Applying the Framework

Several caveats and nuances are beneficial for thinking about the four technical support categories and associated time frames (Table 3). We included the timelines as an illustration and not necessarily as a determinant of how long it would (or should) take to conduct scientific discovery, technological development, innovation, or analysis.

As highlighted in the “Homeland Security Crises” section, each crisis is unique. Even within categories of crises, such as natural disasters—or even between like crises, such as hurricanes—a unique set of circumstances and challenges will likely be encountered. For this reason, stating unequivocally that a crisis will be handled in a particular manner is not possible. Rather, the crisis response, including the technical support capabilities employed, must be tailored to meet the demands of the individual crisis. Despite these differences, fundamentals that guide crisis response (e.g., the Stafford Act or the National Response Framework) are invaluable. The same concept holds true for the technical support that can be employed. Understanding the variety of available technical support capabilities and having the means to rapidly access and employ them can provide key insights and understandings for crisis response leadership at all levels.

If precrisis lessons learned from previous crises are addressed, preparations are thorough, and existing facilities have been established for conducting research (laboratories), it is possible that scientific discovery could be done in a relatively short period rather than in years (which is generally the more likely timeline for basic and applied research). By way of example, because work has already been done on explosive detection algorithms for imaging machines, it might be possible to conduct applied research on a new threat to understand its physical properties and the detection possibilities in a shortened period, such as several months or perhaps even weeks, compared with the foundational research efforts that may have taken years. Other examples of shortened timelines for science and technology (i.e., R&D) are the Pfizer and Moderna COVID-19 messenger RNA vaccines. Through decades of R&D on DNA properties, polymerase chain reaction, genome sequencing, the Human Genome Project, RNA interference, and genome synthesis, the isolation of the target sequence for the vaccine (identified in a couple of

The crisis response, including the technical support capabilities employed, must be tailored to meet the demands of the individual crisis.
weeks) and the timelines necessary to move the vaccine into clinical trials (accomplished in a matter of months) were able to be shortened dramatically. The result was two vaccines that received U.S. Food and Drug Administration approval in about nine months rather than the decade that is traditionally required for vaccine development and approval (Garde and Saltzman, 2020).

The last two technical support categories—innovation and analysis—offer the potential for greatly improving technical support to crisis response. Innovation is about generating ideas, concepts, and processes that can offer solutions in greatly compressed time frames. The CBP P-3 example discussed previously shows what can occur at the intersection of technology and innovation. Through the combination of existing sensors and communications equipment in ways that originally had not been envisioned but were well within the technology’s operational envelope, an operational shortfall—the real-time understanding of the situation on the ground—was addressed. The establishment of Operation Warp Speed (the federal effort to support multiple COVID-19 vaccine candidates for development) can also be considered a technology support capability that was developed rapidly and with great effect, at least in terms of development of the vaccines.

The final category is analysis based on data collection, using analytical tools, and interpretation of the results. As one might expect, normally, initial findings and observations can be provided in hours and days. Of course, such short timelines would imply that initial data are either on hand or readily collected for further study and analysis. The analysis should continue throughout the crisis as new data are received.

In considering the technical support, we should recognize that the various capabilities and tools do not fit neatly into a single entry in Table 3. For example, modeling and simulations would likely be useful for conducting scientific discovery, technology development, innovation, and analysis across the precrisis period and all four of the crisis time frames. Likewise, data collection and analysis would likely be necessary during each of the time frames. Nevertheless, the framework is a useful organizing concept for thinking about and defining crisis response support and technical support imperatives for crisis operations.

The box on the next page provides some points to consider when thinking about technical support during crises.

---

**Conclusion**

With the operational need as the centerpiece of technical support efforts, science, technology, innovation, and analysis can be combined to productively address immediate crisis response technical needs. In addition, anticipating various technical support capabilities before a crisis can prove useful during it. Through the prioritization of techni-
cal support, decisionmakers will gain access to greater situ-
ational awareness and understanding of the crisis at hand.

In the previous section, we identified five impera-
tives that should be considered for providing technical
support during a crisis. Although the list is certainly not
exhaustive, these critical elements should form the basis for
providing quality technical support to operational crisis
leadership:

- getting a seat at the table
- conducting precrisis planning and exercises
- managing data and supporting the development of a
  common operational picture
- bringing in new ways of thinking
- taking advantage of unique opportunities for inno-
vation during crisis support.

To actualize these imperatives, we have developed a
concept for institutionalizing technology support for crises
(Figure 1). It begins with an examination of the categories
of threats and hazards that are included in the HSNRC,
which was reviewed in the “Homeland Security Crises”
section. The next step would be to determine a priori-
tization of the risks regarding which are most likely to occur
and for which the technical support capabilities are the
least prepared. Of course, additional criteria could be
employed so that “most likely, least prepared” would not
solely be prioritized. This step might also include a third
criterion, such as “most dangerous.”

Once the priority list has been established, the frame-
work for crisis technical support capabilities could be used
to develop a draft plan for the risk deemed to be the most
important. This process should be repeated for each of the
high-priority risks. The filled-out frameworks would serve
as initial planning documents for the various risks.

Caveats and Nuances for Thinking About
Technical Support During Crises

- DHS can improve understanding of homeland secu-
  rity threats and enhance its crisis response capa-
  bilities by leveraging technical support capabilities
  more fully.
- The science and technology communities’ capabili-
  ties should be leveraged during crisis response.
- Considering four categories of technical support
  (science, technology, innovation, and analysis) and
  five time frames (precrisis, immediate, near-term,
  mid-term, and long-term) provides a structured
  approach to technical support during crises.
- Five imperatives for consideration when providing
  technical support during a crisis are as follows: get
  a seat at the table, conduct precrisis planning and
  exercises, manage data and support the develop-
  ment of a common operational picture, bring in
  new ways of thinking, and take advantage of unique
  opportunities for innovation during crisis support.

The library of “completed” frameworks for the most
important risks should be updated as necessary. For exa-
ample, if there is an exercise or crisis, the lessons learned can
be incorporated into an updated version of the framework
for that particular crisis technical support plan.

The completed documents could also serve as oppor-
tunities to brief component heads with responsibilities for
certain risks. In this way, the methodology for technical
support capability development would help focus opera-
tional leaders on the kinds of capabilities that S&T and
the broader science and technology communities can offer
during a crisis.
FIGURE 1
Methodology for Technical Support Capability Development for Various Risk Scenarios

Update tech support frameworks after exercises or crisis

Categories of threats and hazards included in the Homeland Security National Risk Characterization

Determine “most likely, least prepared” to support

Framework for crisis technical support capabilities

<table>
<thead>
<tr>
<th>Category</th>
<th>Pre-crisis</th>
<th>During crisis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Immediate</td>
<td>Near-term</td>
</tr>
<tr>
<td></td>
<td>(hours-days)</td>
<td>(&lt;4 weeks)</td>
</tr>
<tr>
<td></td>
<td>Mid-term</td>
<td>Mid-term</td>
</tr>
<tr>
<td></td>
<td>(4 weeks to 3 months)</td>
<td>(6 weeks to 3 months)</td>
</tr>
<tr>
<td></td>
<td>Long-term</td>
<td>Long-term</td>
</tr>
<tr>
<td></td>
<td>(Beyond 3 months)</td>
<td>(Beyond 3 months)</td>
</tr>
</tbody>
</table>

Lessons learned

Update tech support frameworks after exercises or crisis

Continue to fill out the framework for all priority risks

Fill out the framework for the “most likely, least prepared”
Notes

1 We use the information shared during these discussions, although we do not attribute the information, as agreed upon with discussion participants.

2 This definition of analysis is adapted from Merriam-Webster, undated.

3 The term industrial process refers to a variety of activities, from heavy manufacturing to traditional and emerging technology areas.

4 See Willis et al., 2018, for a description of the motivation and for this assessment.

5 See also Fundamental Science Practices Advisory Committee, 2011.

6 The term technical capacity is inclusive of science, technology, innovation, and analytical capacities.

7 The information in this section was provided by Daniel M. Gerstein from his recollections of the events from his time serving as the DHS S&T Deputy Undersecretary and, later, the acting Under Secretary.

8 This value is based on the 2021 Consumer Price Index–adjusted costs (National Hurricane Center and National Centers for Environmental Information, 2022).

9 In the DHS context, the term staff elements could pertain to the DHS headquarters staff sections, liaisons from the operational components, and other stakeholder communities that have a role in the crisis response. As a result, an operations center can also be expanded to bring in representatives from other departments and agencies, industry experts, experts from advisory committees (such as the Homeland Security Advisory Council), academia, nonprofits, and, in some cases, SLTT governments, if needed.

10 Daniel M. Gerstein participated as an SME during his time in the Countering Weapons of Mass Destruction Office within the Office of the Under Secretary of Defense for Policy.

References


CBP—See U.S. Customs and Border Protection.

CDC—See Centers for Disease Control and Prevention.


Coastal Resilience Center, homepage, undated. As of April 18, 2022: https://coastalresiliencecenter.unc.edu/


DSTG—See Defence Science and Technology Group.


Médecins Sans Frontières, “How We’re Run,” webpage, undated. As of December 23, 2021: https://www.msf.org/how-we-are-run


National Institute of Allergy and Infectious Diseases, “Division of Intramural Research Laboratory Descriptions,” webpage, last reviewed November 3, 2021. As of December 23, 2021: https://www.niaid.nih.gov/research/division-intramural-research-labs

National Response Coordination Center, webpage, Federal Emergency Management Agency, undated. As of April 18, 2022: https://emilms.fema.gov/is_0101c/groups/15.html


SAGE—See Scientific Advisory Group for Emergencies.


S&T—See Science and Technology Directorate.


TSA—See Transportation Security Administration.


About the Authors

Patricia A. Stapleton is a political scientist at RAND. She uses qualitative methods and a historical institutionalist approach to examine factors affecting the development of risk regulation, and her research interests include science and technology policy; risk perception and regulation of emerging technologies; and risk assessment and communication. Stapleton holds a Ph.D. in political science.

Daniel M. Gerstein is a senior policy researcher at RAND. Previously, he served as the DHS S&T Deputy Undersecretary and, later, the acting Under Secretary. His research interests include arms proliferation and control, big data, biology and life sciences, biosurveillance, critical infrastructure protection, emerging technologies, homeland security legislation, and peacekeeping and stability operations. Gerstein holds a Ph.D. in biodefense.

Henry H. Willis is the director of the Homeland Security Operational Analysis Center’s Strategy, Policy, and Operations Program and a senior policy researcher at RAND. His recent work has involved analysis of terrorism warning indicators; border security efforts; critical infrastructure resilience; and national preparedness for chemical, biological, nuclear, and radiological attacks. Willis holds a Ph.D. in engineering and public policy.
About This Perspective

The Secretary of the U.S. Department of Homeland Security (DHS) has identified several priority challenges for DHS. Some of these are endogenous to the department, such as maturing its management and oversight functions. Others are driven by external events and threats, such as the rapid evacuation of refugees from Afghanistan. When confronted with priority challenges, the Secretary of DHS requires scientific and technical advice to identify gaps in DHS processes and operations, as well as solutions to fill these gaps now and in the future. By leveraging this advice, DHS seeks to improve understanding of the homeland security threats that it manages and its mission effectiveness.

In November 2021, the Operations and Requirements Analysis (ORA) Division of the DHS Science and Technology Directorate (S&T) engaged the Homeland Security Operational Analysis Center (HSOAC) to provide agile analytic support to the Under Secretary for DHS S&T, who serves as science adviser to the Secretary. For this effort, HSOAC identified best practices and lessons learned for leveraging science and technology communities to support homeland security crisis response. The intended audience for this Perspective includes DHS and S&T leadership and others interested in and involved with leveraging science and technology to support crisis response.

This research was sponsored by ORA and conducted within the Acquisition and Development Program of the HSOAC federally funded research and development center (FFRDC).

Acknowledgments

We would like to thank our sponsor representative, John Dargan, Director of Operations and Requirements Analysis, for his support on this task. We would also like to extend our thanks to Dan Abel, Tom Atkin, Donell Harvin, Andy Lauland, Bear McConnell, and Rob Parker from the RAND Corporation for their generosity in sharing their experiences. Finally, we would like to acknowledge the valuable contributions of Jim Bonomo and Reynold Hoover, who served as peer reviewers.